DEUTSCHER PRÄVENTIONSTAG

International Cybercrime: Results from the Annual International Forum

by

JÜRGEN STOCK

From: Marc Coester and Erich Marks (Eds.):
International Perspectives of Crime Prevention 4
Contributions from the 4th and the 5th Annual International Forum 2010
and 2011 within the German Congress on Crime Prevention
Forum Verlag Godesberg GmbH 2012, Page 129-136

ISBN 978-3-942865-00-5

Jürgen Stock

International Cybercrime: Results from the Annual International Forum[1]

The objective of this contribution is to give account of the findings and results achieved during the 5th Annual International Forum under the title "International Cybercrime Occurrence, Development and Prevention" held within the framework of the 16th German Congress on Crime Prevention in Oldenburg. The two-day forum was characterized by highly topical, interesting presentations and discussions as well as by an intense exchange between the experts attending the meeting.

Altogether six presentations given in the course of the two-day forum provided initial responses to the following questions:

1. What is the current situation with regard to the cybercrime phenomenon?
2. What trends and developments may be expected?
3. What countermeasures have to be taken in order to effectively combat cybercrime?

As the cybercrime phenomenon is very multifaceted, it was approached from equally different angles. The experts managed to highlight socio-scientific, legal, economic and criminological aspects.

The perspective of the German security authorities was illustrated by two officers of the *Bundeskriminalamt*, Helmut Ujen and Mirko Manske. They gave an outline of the criminological phenomenology, as far as it is perceived by the *Bundeskriminalamt*.

Frank Ackermann, representative of the *Eco-Verband der Deutschen Internetindustrie* (Association of the German Internet Industry), reported on interesting crime suppression approaches pursued by the economy and the cooperation between the economy and security authorities. Media consultant Frank Tentler informed the audience on the structures and the functioning of social networks, possible dangers and on the developments that are to be expected in this area.

From the perspective of the European Commission, the political level, Marc Arno Hartwig described possible measures against the dangers outlined. Finally, Cornelia Schild of the *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Information Security) and Sven Karge of the *Eco-Verband* (Association of the German Internet Industry) supplied information about a public-private partnership successfully launched in the field of combating botnets.

---

[1] Slightly revised version of the presentation given in Oldenburg on 31 May 2011.

"Using the Internet is like skating on natural ice: Sometimes you do not know how thick or thin the ice is. In some places, the ice is thin and skating is dangerous. Nevertheless skating is great fun." This is how a participant very aptly described the attractions and risks of the Internet.

The Internet gives impetus to social and economic development. It is a medium used for networking, accelerating and simplifying. It has become indispensable for a large number of daily activities. At the same time, we have to be aware of the threats posed by malfunctions and cybercrime. The growing possibilities of the digital world also imply an increase in the dangers involved.

1 Situation

1.1 Positive Aspects of the Internet – Social and Economic Potentials

The Internet offers enormous potential for social and economic developments at national and international level. More and more people in Germany have Internet access, with not only younger people having a share in this development but also older ones, i.e. almost 40 per cent of the people aged over 60 regularly use the Internet.[2]

There is no doubt that the Internet is an important element of today's society: To imagine not only the world of work, the education, trade and services sectors, but also social contacts, especially social networks, without the Internet is impossible. We all use the Internet for procedures like online banking, the tax declaration, which is submitted to the tax office preferably via the Internet, the registration of vehicles and so forth. Due to the mobility of the devices necessary to that end, not least due to the increasing dissemination of smart phones, the Internet can be used in nearly all places at any time. This means that the World Wide Web can be accessed from everywhere; people do no longer depend on fixed business hours, for example.

Nowadays, it is quite simple to establish new forms of communication; making and maintaining contacts is becoming easier, at least in technical terms. These developments are global trends. All of you know charts that show the share of Internet users in the populations of the individual countries in the world. Europe and the USA have an eye-catching appearance; the use of the Internet is widespread in these countries. But also on the African continent the number of Internet users is significantly increasing.

This is the "bright side" of the Internet, the facet that simplifies our lives and that is fun.

---

[2] *Bundesverband Digitale Wirtschaft* (Federal Association of the Digital Economy): In the third quarter of 2010, 73.4 per cent of the German-speaking resident population in Germany aged over 14 used the Internet. Almost all 14 to 39-year-olds (well over 90 per cent) are present in the Internet, the 40 to 49-year-olds have a share of 86.3 per cent, the 50 to 59-year-olds of 73.2 per cent. Still more than one third of the persons aged over 60 (36.2 per cent) use the Internet.

1.2 The Dangers of the Internet – The Law Enforcement Situation

The focus of the discussions at the forum, however, was on the "dark side" of the Internet, which one participant defined as the "portals of threat". Danger lurks in all areas: social media, online banking, geodata, e-commerce. The lecturers stated that in many cases IT security is not included in the original programme architecture, but has to be added later on in a complex and costly procedure.

Cybercrime in part includes conventional forms of crime, which duplicate merely on the Internet. Therefore, the Internet on the one hand is a new instrument of crime. On the other hand, we are facing new types of crime phenomena which were previously non-existent in this form. The experts complained in particular about the lacking overview of these new phenomena.

In this connection, according to the experts, it is questionable to what extent the figures shown in the police crime statistics are valid. Might it be that business enterprises with their specific interests are behind the figures? What is the estimated number of undetected cases? The experts participating in the forum voiced doubts as regards the usability of these crime statistical data.

The police crime statistics show that cybercrime is one of the growth sectors of delinquency. A decrease is noted with regard to many other types of crime and case numbers in total. In contrast, the number of cybercrime cases recorded alone between 2009 and 2010 rose by approximately 20 per cent. Also with respect to the damage caused by cybercrime, increases by up to 50 or 60 per cent are noted. These figures are a matter of concern.

However, the figures mentioned above refer to recorded crimes only. How many offences are not reported to the law enforcement agencies, for example because private victims have no clue about their computers being part of a globally operating botnet? How many enterprises become aware of an attack but refrain from reporting it to the law enforcement agencies for fear of damage to their image?

One thing is for certain: The offenders 2.0 come from all traditional fields of crime known to the police and the judicial authorities. These offences involve organized crime, terrorism, child pornography, industrial espionage, fraud and also offences against state security and corruption offences. All this can be found on the Internet - there are, however, some new facets that also gave the participants of the forum food for thought. Phenomena such as the theft of digital identities, which the offenders use for shopping sprees on the World Wide Web, thus being able to cause considerable damage, are something to be seriously concerned about. Moreover, the possibility to create digital clones or - in other words - parallel identities, bears an enormous damage potential.

This is also true for the developments in the field of phishing. You all know this phenomenon, many of you received so-called phishing mails at some time or another: What was very clumsy when it started some years ago has meanwhile become more professional through corresponding social engineering applied by the offenders. Nowadays, you catch Trojans through so-called "drive-by infections". A supposedly non-compromised website, for example the website of the *Bundeskriminalamt* or the *Bundesamt für Sicherheit in der Informationstechnik*, might be a forged website that can hardly be distinguished from the genuine one and that infects your computer with a Trojan when website contents are retrieved.

Also classical forms of crime such as extortion, protection racketeering and extortion for ransom nowadays take place on the Internet. If we stick to the term, there is a mafia 2.0, which no longer robs banks somewhere but uses the opportunities provided by the Internet to approach enterprises and to threaten them with spam attacks. If the enterprises menaced in such a way do not take the threats seriously, their servers get flooded. The fact that enterprises are unavailable because their servers are being flooded may cause considerable losses. Corresponding cases have shown that the threat is associated with an actual damage that may cause significant problems for an enterprise, in some cases even for smaller countries.

One topic of the future, as was expressly emphasized by the experts, are mobile terminals. Many people already have such mobile terminals, which combine more and more functions. The consequence is that in the future mobile terminals will become the target of an increasing number of attacks, for example by botnets. This is certainly an issue that, under the aspect of prevention, should be in the focus of attention in the future.

In the meantime, an underground economy, a wide range of criminal products offered on the Internet, has developed. Digital identities, credit card data, Trojans or complete botnets can be acquired at relatively low cost, and on that basis considerable damage can be caused with relatively limited IT skills.

"That has been our depression day" - this is how one participant aptly described the first day of the 5th Annual International Forum. What action can or must be taken in the field of prevention? Are the instruments we have effective? What can we do when realizing that our own computers pose a potential threat? These were the questions we faced at the beginning of the second day.

2 Countermeasures – Players and Methods

The discussions on those involved in counteraction and on the methods used in this context focused on the following questions: What preventive countermeasures can we offer? What players and methods have been involved so far? Nearly all lecturers felt that, on the one hand, we are lucky to have a large number of different initiatives

at national and international level - which in my opinion is an important message emanating from this year's Congress on Crime Prevention. Many actors are strongly committed to developing measures against cybercrime. However, according to the experts, there are some areas still requiring considerable effort to catch up. For example, with regard to "awareness", i.e. the technological and consciousness-related IT security, we have to take countermeasures as soon as ever possible. The gap between what is happening in the field of cybercrime and what we are doing to counter it must not widen.

2.1 Security Authorities

Since March this year, the Federal Government has pursued a common cyber security strategy. In this connection, the security authorities fulfil their traditional tasks involving law enforcement and aversion of danger. Employees from different fields of work, such as scientists, technicians, police officers and other experts work together in the security authorities every day. In the field of traditional police repression, the police and judicial authorities, among other things, face the challenge to find solutions to the question of how to secure traces on the Internet in such a way that they may be used as evidence in court later on. A further challenge is posed by the large data volumes that have to be analysed in connection with investigative proceedings.

The experts participating in the forum pointed to the need to intensely deal with future developments. Due to the dynamics inherent in cybercrime we are well-advised to use procedures such as scenario planning for identifying probable future developments. This also involves a monitoring system that functions properly. Instead of trying to catch up with developments, a situation we complained about, we must be acting with an eye to the future. Examples of recent developments are modern payment systems such as WebMoney or Ukash. Moreover, the experts addressed issues that (still) appear futuristic, e.g. "digital camouflage", which is currently under development and can be used for covering up criminal activity.

2.2 Economy and Associations

Representatives of the economic sector and the associations pointed to the different platforms and forms of cooperation that have so far been established for preventive purposes. These include, on the one hand, activities by the economic sector in its specific spheres of activity. On the other hand, examples were given in which prevention programmes carried out by other actors, such as schools especially at local level, are supported by commercial enterprises and associations.

2.3 Users

It is also the users who are required to act accordingly and who have to consider themselves to be central elements of the security structure. The awareness of and sensitivity for the dangers of the Internet, have to be strengthened. In view of the fact that

even antivirus software installed on the computer cannot provide complete protection and is able to identify only a part of the viruses currently on the market, the users have a special responsibility.

2.4 Public-Private Partnership

The issue of public-private partnership was presented on the basis of a current example, the Anti-Botnet Consultancy Centre. The Anti-Botnet Consultancy Centre is a cooperation project between the *Bundesamt für Sicherheit in der Informationstechnik* and the *Verband der deutschen Internetwirtschaft*. Internet service providers and providers of anti-virus software are also involved in this close cooperation. It is remarkable that this cooperation project does not restrict itself to being just a strategic advisory body but that concrete advice is offered to enterprises or individual persons affected by a botnet attack. The experts asserted that, if necessary, call centre employees would go through a work plan item by item together with the caller in order to ultimately remove the Trojan responsible for integrating the computer into the botnet from the computer.

3 Conclusions

As indicated several times before, many aspects remain yet to be settled in the dynamic field of cybercrime. The knowledge of the phenomenon is in part not very profound. Awareness of the impending threats has to be strengthened. What conclusions can be drawn from the lectures and discussions especially in terms of prevention?

3.1 Extension of Existing Cooperations

Many players have already been active in the field of cybercrime prevention. Existing cooperations have to be extended and strengthened. Especially in the field of prevention there still is potential for optimisation.

3.2 Keeping up with the Dynamics of Development

According to the experts, the developmental dynamics of the Internet and hence also of cybercrime will not diminish. Professor Potja appropriately stated that in the past those involved in technological innovation had still had much time to think about solutions to problems. The experts at the forum were unanimous that this time is no longer available. We must react more quickly and intensify our preventive effort.

3.3 Strengthening Research Activities

Cybercrime-related research activities must be pushed ahead. The phenomenological knowledge on what is happening on the Internet is to be improved. It is a task area of classical criminology to learn more about the manifestations and the quantitative dimension of cybercrime. Furthermore, clearing up undetected crimes also counts among the classical social science research and is an area that has to be tackled. On the other hand, it is necessary to improve technological research with a view to pre-

venting opportunities to commit offences on the Internet and especially with a view to stepping up IT security. This is the only way we can obtain more information on risks as well as on crime, victim and offender structures.

3.4 Suppression of Cybercrime as a Task for the Whole of Society

The fight against cybercrime is a task to be tackled by the whole of society. The experts' lectures made clear that cybercrime is a classical cross-sectoral issue. As a consequence, this means that we have to develop strategies at interdepartmental level. We all must assume our share of obligation in the preventive value chain from private users to enterprises and state actors.

3.5 Intensification of the Social Discourse

In the opinion of the experts, the social discourse on what should take place on the Internet and what not, has to be intensified.

"Don't be stupid", that is the simple formula for prevention. But is this sufficient or do we need more regimentation? What level of freedom should there be on the Internet? What role do the individual actors play? Are pure Internet ethics sufficient, which the users themselves develop for all intents and purposes, or do we need more state regulation? The World Wide Web is, one the one hand, global. However, a glance at the European countries alone shows that they in part have very different views regarding the extent to which the state should intervene. The discussion on the Act to Impede Access to Child Pornography Content in Communication Networks, which was introduced in Germany and repealed afterwards, is a good example for illustrating the problem.

3.6 Strengthening Media Competence

For the purpose of making a universal prevention approach, media competence must be broadened and promoted in all areas of society. Information and preventive work in respect of children must start as soon as they touch a device connected with the Internet for the first time. At this point, specific education and awareness production must begin.

3.7 New Forms of Cooperation between Private and Public Actors

We must try out new forms of cooperation between private and public actors, both at national and international level. There are many existing or developing forms of cooperation on a local, national and international scale. These have to be tested further and expanded. As far as possible, they have to be scientifically supported in some cases in order to enable us to assess how these networks can be organized in an effective manner.

3.8 Extension of Individual Offers of Assistance

In the opinion of the experts, the individual offers of assistance are to be expanded. The Anti-Botnet Consultancy Centre, jointly run by a public authority and an association, is a good example. Forum attendants compared it with the burglary prevention advice services provided by the police. This means that, according to the experts, traditional areas of crime, for which the police have established an ample advice system, have to be extended to cybercrime. A government agency is required which people can call for advice.

3.9 Adaptation of Prevention Methods

Our prevention methods have to be adapted. The prevention actors need a new specific social engineering, they need to know how to reach the respective target groups. "Listen, Learn and Lead", these catchwords describe how actors in the end assume leading roles in terms of prevention activities. Thus, we have somewhat called into question one point of Wiebke Steffen's presentation yesterday: Are the methods of the analog world transferable to the digital world? Taking into account the results of our forum this is questionable, which consequently means that specific instruments will have to be developed.

3.10 Provision of Resources

Sufficient resources are to be made available for countermeasures and prevention. This is not surprising. In the final analysis, one of the pleasant side effects of public-private partnership is that the economic sector bears part of the costs and that cooperations are set up, by means of which training measures can be financed.

These are the essential findings of the 5th Annual International Forum at the 16thGerman Congress on Crime Prevention.

I would like to take this opportunity to thank all lecturers for their excellent presentations and the participants in the discussions for their contributions. Thank you very much for an informative and goal-oriented forum.

Content