Bundeskriminalamt

Perpetrators in the field of cyber-crime

A literature analysis

Part I – A phenomenological and offender typology-based analysis

Part II – Criminological explanations and scope for action

Status: 4 December 2015

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime KI 16

Jörg Bässmann

BKA

Summary

Perpetrators in cyber-crime in general and in the narrower sense are frequently referred to indiscriminately as “hackers”. As in other fields of crime, this also raises the question concerning the extent to which a differentiation of offender types might also give rise to differentiated answers by the state in dealing with such perpetrators.

In this report, German and English-language literature starting in the year 2000 on the subject of cyber-crime in the narrower sense was evaluated for offender-specific findings. Access to the media primarily was network-based via the Internet, Extrapol as well as the BKA Intranet. One of the difficulties faced with this work is that hardly any criminological studies in conformity with high scientific standards have ever been carried out in this field.

In phenomenological terms, the report shows that typical hackers are pupils, apprentices or students who have frequently acquired their knowledge of information technology by autodidactic means. Today this is simpler than in the past, seeing as many young hackers have meanwhile grown up as so-called “digital natives”, fully familiar with computers and the Internet as an information platform. Most hackers spend their leisure time especially with computers and work a great deal on their own without being “socially conspicuous”[1] in the process. They tend to maintain informal contacts evidently derived from momentary experiences rather than from solid integration into social structures and groups. Contacts are maintained especially via chats, cliques or also as individual friendships in the real world.

For the actions of hackers, individual motives appear to be less decisive than aggregations of motives. Things of particular relevance are the fact that hacking is fun, followed by curiosity and entertainment aspects as well as the exciting thrill of doing something that is prohibited. Striving to become part of a group of persons with shared interests and to acquire respect, recognition and status in a person’s own group or community likewise are relevant motives, as is the apparent acquisition of power due to the ability to control extraneous systems. In addition, monetary and political reasons should not be ignored as incentives for hackers, just as striving for destruction or revenge may be a conceivable motive. In connection with the intrinsic motivation to engage in hacking, there are manifestations of flow experiences of the kind known from high-risk sports, especially for qualified hackers.

In order to successfully gain access to others’ computers and networks, a high level of IT expertise and skills is no longer imperative. Offerings available on the web, such as “crime as a service” or “malware as a service” also enable offenders with less practice to carry out attacks on computers and networks. In this context, the targets are many and various. Depending in particular on the motivation in each case, attacks are launched on companies of any size, on websites of governments and administrations, pornographic pages, ethnic or religious websites, banking systems and also on web pages of private individuals.

Extremely few cybercriminals appear to have already come into contact with the criminal justice system. Possible forms or punishment or also imprisonment are practically without any deterring effect, seeing as the expertise and resources of the criminal prosecution authorities are not assessed as particularly high. The possibility of embarking on a successful career in the IT sector thanks to the qualifications acquired (even though illegality was involved) also plays a role, as a number of hacker legends have shown in the past.

[1] Translator’s note: A term in German that can mean, *inter alia*, being maladjusted, non-conformist or lacking in social skills

Considering the core mandate of identifying possibilities for creating offender profiles, the report shows that in the past 25 years, hackers have predominantly been typified according to their level of skills, the purpose of and/or motivation behind their actions and, more recently, also according to their occupational origins and/or principals or employers. A number of such factors are simultaneously taken into account on a regular basis. Hardly any indications were available in literature concerning the methodical approach used in developing offender types in the field of hacking. A more profound methodical analysis of type manifestations amongst hackers thus was not possible within the scope of this literature study.

Nevertheless, not only does the work performed provide a chronological overview of type characterisations amongst hackers; it also facilitates an overview in a certain bandwidth ranging from rather rough differentiations according to the level of skills all the way through to complex type differentiations, in particular also according to motivational aspects. Incidentally, both aspects played a part in most typifying systems. Moreover, new typifying activities refer to the origin and/or institutional "classification" of hackers, as illustrated by the example of typifying activities of the Dutch National Cyber Security Centre. Based on a model of hacker types derived from literature, in annual situation reports a type-specific danger is described as the starting point for national state counterstrategies, *inter alia* to reinforce the resilience in many and various fields.

In criminological terms, the study deals with the criminological theories mentioned most frequently in connection with cyber-crime and their applicability. In detail, the report deals with such topics as attachment and control theories, learning theories, the neutralisation theory, the theory of rational selection as well as the routine activity theory, the theory of criminality as "forbidden fruit", the flow theory and, as a new theory to explain cyber-crime, the "space transition theory". Even if the theories alone cannot provide any explanations for cyber-crime in the narrower sense that can be applied in isolation, they certainly are of substantial significance above and beyond the various theories, not only for preventive work.

In terms of practical police work, the literature analysis has been used in order to obtain ideas for offender-related interventions and/or preventive measures. A promising approach could be to concentrate repression above all on the relatively small group of highly qualified hackers rather than focusing on a broad mass of "script kiddies" or hackers with rudimentary training who essentially use prefabricated tools. The concentration of public prosecution on well-versed hackers is also likely to be beneficial as they are not the developers of an ever new range of attack tools alone but simultaneously represent key nodes in offender-related cooperation and key supports in providing know-how to hackers with less expertise.

With regard to the "script kiddies", it cannot be ruled out that we are merely confronted with a new phenomenon of juvenile delinquency. For this reason too, it appears to be sensible to rely on social prevention approaches that – to name but one – include also police-related deterrent measures towards potential offenders such as warning visits or letters.

Moreover, in preventive terms the findings of the literature analysis argue in favour of applying situation-related preventive approaches whose effectiveness is adequately documented in rather classical fields of criminal investigation. As a rule, situation-related measures are not suitable to deter highly professional and highly motivated offenders from committing their criminal acts. However, they are an effective tool for the mass of opportunistic perpetrators or those offenders who simply take advantage of any opportunities

to commit a crime. In relation to the subject of hacking, these would be those frequently juvenile offenders who use prefabricated tools for attacks because they themselves have too little expertise and too limited (financial) resources to develop complex attack tools themselves. In this context, situation-related approaches do not only refer to measures of basic IT security on the user side but can also be deployed towards offenders so as to prevent possibilities of guilt being neutralised.

Finally, the report also documents the shortfall in research – particular in German – that exists on the subject from the perspective of criminalist and criminological research.