Bundeskriminalamt

HERBST-TAGUNG BKA 2013 AUTUMN CONFERENCE

Cybercrime –

Threat, intervention, defence

BKA Autumn Conference, 12 - 13 November 2013

Legal challenges in the fight against cybercrime

Abstract

Dr Wolfgang Bär

Ministerialrat, Bavarian State Ministry of Justice and Consumer Protection

Digital technologies of all kinds influence our life more and more. The Internet has already become an integral part of our every-day life. Shopping on the Net, searching for information, watching films and videos and chatting with friends has become a matter of course for many of us. The Internet affects ever more areas of life. Mobile availability through the Net and mobile access to the Internet from everywhere are becoming increasingly important.

Notwithstanding the foregoing, the Internet must not be a legal vacuum - and neither is it. The law of the analogue world is not invalidated in Cyberspace. The great challenge, however, lies in adapting it to the special features of the digital world in order to ensure its enforceability. To each of us, the Internet opens up infinite possibilities for everything imaginable. Unfortunately, also for the criminal interests of offenders. It is not surprising, therefore, that the number of the relevant cases recorded in the criminal statistics has doubled in the last five years, with the dark figure of crime being very large as many cases - such as offences with a foreign dimension - are not entered in the statistics. A characteristic of this type of crime is the tendency towards increasingly dangerous and frequent major attacks on information systems of the public and private sectors. At the same time, the methods used for these attacks are more and more sophisticated and involve criminal acts at various stages. This contribution will, therefore, address the most important problems posed to criminal law by this new digital world in order to show if all the new forms of crime are covered by substantive criminal law on the one hand, and on the other, if the law enforcement authorities have the means of detecting, and appropriately prosecuting, offences committed with these new technologies.

I. Substantive Criminal Law

The rapid technical development of modern IT systems affords offenders ever new possibilities for crime. Thus numerous new criminal modi operandi have developed in the last few years under the key words phishing, pharming, skimming, ransomware and botnet. The term cybercrime refers to all offences targeting the Internet, other data networks, IT systems or their data or committed by means of this information technology.

The legislator has responded to this new challenge at national level with the 41st Criminal Justice Amendment Act of 7 August 2007 and amended and supplemented a number of criminal offences, which had practically constituted the core area of computer criminal law since the 2nd Economic Crimes Act of 1986. This has already led to numerous amendments of criminal offences with re-

gard to the protection of data secrecy and data integrity. In addition to extending the provisions of "electronic trespass" according to section 202a of the German Penal Code, new offences have been defined under sections 202b and 202c of the German Penal Code and the previous regulations relating to data tampering (section 303a of the German Penal Code) and computer sabotage (section 303b of the German Penal Code) have been tightened at the same time.

Also against the background of the Directive on attacks against information systems adopted by the European Parliament in July 2013, which still has to be implemented in national law, there is the need for legislative action, especially with regard to three issues: First of all, legal loopholes concerning the dissemination of illegally obtained data have to be closed. To this effect, the Federal Council draft law on the creation of the new criminal offence of "Handling stolen data" under section 202d of the German Penal Code - Draft (Federal Council Journal 284/13) contains a proposal worth supporting. Secondly, it is necessary - also against the background of Art. 9, paragraph 5, of the new EU Directive on attacks against information systems - to include aggravating circumstances for dangerous and large-scale attacks against information systems and data espionage in sections 202a, 202 and 303a of the German Penal Code. For example, the creation of botnets, namely the act of establishing remote control over computer systems by infecting them with malicious software, and the hacking into the computers of large companies and critical infrastructures has the capacity to lead to a considerable threat potential and cause serious damage in individual cases. The sections 202a and 202b of the German Penal Code should also provide the possibility to impose a penalty for the attempt. And, thirdly, the definition of written material as outlined in section 11, subsection 3, of the German Penal Code, which is applicable only to data storage media so far , needs to be adapted to the new technical developments. In pornography-related criminal law, and also with regard to all other content-related offences of the German Penal Code, instead of adhering to the definition of written material, which had been developed for physical objects, all forms of providing access to media or to media contents of a punishable nature should be considered. Only in this way will it be possible to avoid the legal loopholes created by today's use of the Internet.

II. Procedural Criminal Law

Just as offences are shifting to the digital world, the tools of law enforcement also have to be transferred to virtual reality. Especially at the legislative level, this requires that law enforcement authorities be provided with the necessary legal instruments enabling them to respond appropri-

ately to the high threat potential emanating from cybercrime. To ensure effective prosecution, the necessary legal and technical means of detection must, therefore, not be withheld from the investigation authorities.

As most offences are committed by means of telecommunications, the law enforcement authorities need, above all, rights to intervene in telecommunications that are in line with the state of technology and without which it is not possible to obtain an investigative lead in many cases or clear up the case any further. An Internet user can usually only be identified through his IP address. In this context, the legislator has created new area-specific powers of intervention concerning the access to telecommunications customer data and the disclosure of personal details pertaining to a dynamic IP address, which are formulated according to the requirements of the Federal Constitutional Court in section 100j of the Code of Criminal Procedure as of 01 July 2013. However, IP addresses can be traced and telecommunications traffic data obtained only if the respective providers recover the relevant information and store it over a certain period of time. This in turn requires a legal obligation for the storage of telecommunications traffic data without direct cause. Such data retention in line with constitutional requirements is possible on the basis of the provisions of the Federal Constitutional Court if appropriate regulations are created with regard to data security, the extent of the use of data, transparency and data protection. Only with such a revision will it also be possible to meet the obligations under European Law to implement the respective EU directive and to avoid a conviction by the European Court of Justice in infringement proceedings entailing heavy penalty payments. To enable the authorities to order telecommunications intercepts also in connection with serious offences pursuant to sections 202a, 202b, 303a and 303b of the German Penal Code, the inclusion of these serious offences in the list of offences contained in section 100a of the Code of Criminal Procedure appears to be necessary - as already proposed in the draft law on the "Handling of stolen data". For the sake of clarity, specific intervention powers relating to the interception of source telecommunications as a special form of telecommunications interception should be integrated there as well.

In addition to covert technical intervention measures, covert personal investigations in social networks are becoming increasingly important. Social networks such as Facebook, Wer-kennt-wen, MySpace and Twitter are used by millions of people in all sections of the population. Due to their high attractiveness and their ever increasing use they are, therefore, an important source of information for the law enforcement authorities. Two areas are to be differentiated in this connection,

which must not be mixed up due to the nature of the activity and the underlying legal basis: the use of social networks to solve crimes on the one hand and to carry out media-assisted searches on the other. As far as investigations in social networks are concerned, their relevance to the fundamental rights needs to be considered in the individial case on the basis of the specific measure and, building up on that, an examination of the possible powers of intervention allowing the use of police officers conducting clandestine operations (sections 161 and 163 of the Code of Criminal Procedure) and of undercover investigators (sections 110a - 110c of the Code of Criminal Procedure) has to be carried out. Under the strict legal prerequisites of sections 131 - 131c of the Code of Penal Procedure, searches in social networks are also an option, provided that data protection requirements are met.

As the current legal powers of intervention for the seizure of information are based on the concept of the geographic location of data and the pertinent territoriality, the age of cloud computing calls for adjustment in this respect. Data can be moved to a different storage location in a very short period of time. The cloud computing providers themselves quite often do not know the actual physical storage location of the data. The existing powers of intervention to search and intercept telecommunications do no longer meet the requirements of these new scenarios, with the effect that obtaining relevant data which are stored in a cloud necessitates legal clarification by combining sections 100a and 102 of the Code of Penal Procedure to create a new power of intervention for gaining access to externally stored data by means of telecommunications. This should also include the possibility of access to data whose concrete storage location cannot be determined because it is outside national jurisdiction. Only by such adaptations will it be possible to meet the needs of effective law enforcement.