



Bundeskriminalamt



**Crime Scene Internet –
A Global Challenge for Internal Security**

BKA-Autumn Conference, 20 – 22 November 2007

Criminal Law in the Digital World

Summarised presentation

Dr. Wolfgang Bär

Judge at a Higher Regional Court in Bamberg

The introduction of personal computers in all areas of the economy and private life and the increasing networking of computer systems along with the rapid growth of the Internet have also given rise to a large variety of new risks and opportunities of misuse where computer data and systems - in terms of quality and quantity - increasingly become the instruments or targets of crime which nowadays may paralyse entire areas of the economy and, above all, may also generate high losses. I would, therefore, like to address and further discuss new important legal issues arising from both substantive law and procedural criminal law.

1. Are phishing, pharming, spamming, port scanning, wardriving or DoS attacks and other new modi operandi covered by the criminal law in force? As far as substantive criminal law is concerned, the legislators amended and supplemented a number of criminal offences - practically constituting the core area of computer criminal law since the 2nd Economic Crimes Act of 1986 - on the basis of the 41st Criminal Justice Amendment Act of 7 August 2007. Section 202a of the German Criminal Code, “electronic trespass“, the new section 202b and the particularly controversial section 202c of the German Criminal Code close confidentiality gaps identified during data transmission (“sniffing“) as well as in advance (“hacking tools“). Simultaneously, previous provisions governing data alteration (section 303a of the German Criminal Code) and computer sabotage (section 303b of the German Criminal Code) have been tightened also in view of denial-of-service attacks. There are, however, no separate provisions governing cases of phishing which have now resulted in extremely high damage. In this context, we have to differentiate between fraudulently obtaining confidential data which may only be covered by section 269 of the German Criminal Code and their subsequent use (predominantly section 263a of the German Criminal Code). Where wardrivers move in unsecured Wireless Local Area Networks, criminal liability may be assumed in exceptional cases only. The criminal justice authorities focus more and more on file sharing networks used to down-load and offer large bulks of digital material of any kind on the Internet in violation of sections 106 and 108a of the German Copyright Act.

2. Can necessary evidence be secured and an investigation be conducted successfully? In addition to the classical measures of investigation such as searches, confiscation and interception of telecommunications, the use of all modern forms of communication raises new crucial legal issues. What, above all, is controversial in this connection is the appropriate choice of the legal grounds justifying access to email communication during intermediate storage at the provider. As far as section 100a of the German Code of Criminal Procedure applies in this case, “electronic mail” may only be monitored where a listed offence is involved. Where sections 103, 94 and 99 of the German Code of Criminal Procedure serve as the legal basis, these restrictions do not apply. In this

connection, the IP address is also growing in importance as an identification in network communications. The disclosure of personal details pertaining to a known IP address pursuant to section 113 of the Telecommunications Act and/or section 100g of the Code of Criminal Procedure is handled in very different ways. The decision taken by the Federal Court of Justice on 31 January 2007 also confronts us with the question as to whether the use of new technical means - ranging from key-loggers to Trojans and online searches - is admissible under the existing powers of intervention laid down in sections 100a, 100f and 102 of the Code of Criminal Procedure. Particular difficulties arise from cross-border investigations when the location of the computer is to be determined and legally relevant data stored on any computer around the world is to be accessed. Last but not least, the use of illegal file sharing networks also raises new questions regarding the practical aspects of dealing with mass complaints. The draft act aimed at reforming the interception of telecommunications and other covert measures of investigation which is being debated in Parliament (German Bundestag publication BT-Drs. 16/5846 as of 26 June 2007) hardly provides any proper solutions to these legal issues.