Bundeskriminalamt

6th Research Conference on Organised Crime

Organised Crime and the Internet

in Niedernhausen on 25 – 26 September 2013

Transborder investigations in cybercrime cases: New challenges for law enforcement

Rainer Franosch

The General Public Prosecutor's Office of the State of Hesse – Central Department for Combating Cybercrime, Frankfurt am Main

Curriculum vitae

1968	Born in Marburg (Germany)
1987 - 1989	Active military service, reserve officer (1990 - present), lieutenant colonel (2008)
1989 - 1995	Studies of law at the university of Marburg
1995	First state exam
1995 - 1998	Legal preparatory service, part-time work in a law firm
1998	Second state exam
1998 - 2001	Public prosecutor in Frankfurt am Main
1999	One of the first specialized cybercrime prosecutors in Germany
2001 - 2009	Public prosecutor in Marburg (cybercrime and economic crime department)
2003	Three months of military exercise in Bosnia and Herzegovina as a legal advisor for the commander of the German Stabilization Force (SFOR) contingent, cooperation with the International Criminal Tribunal for the former Yugoslavia (ICTY)
2010 - present	Senior public prosecutor at the office of the General Public Prosecutor of the State of Hesse, one of two leaders of the Central Department for Combating Cybercrime (CDCC)
2011/2012	Legal expert for the German parliament's enquete commission „Internet and digital society“
1999 - present	Training supervisor for police officers, public prosecutors, judges and other law enforcement agency members (cybercrime and economic crime), German armed forces (military and international law), training of employees of private entities in the framework of public-private partnerships (cybercrime and economic crime)

Abstract

In cybercrime prosecutions, it is more and more frequently the case that the relevant data for local preliminary investigations and criminal proceedings are stored on foreign servers or that the physical place of storage is unknown.
Traditional ways of international cooperation in those criminal cases are often too slow, which leads to the loss of evidence data. For investigations involving the Internet, the time factor plays a decisive role due to the lack of data retention in several states.
Cybercriminals know about these advantages and exploit them for their own purposes, deliberately using several networked intermediary systems in different countries.

The presentation intents to show the growing professionalism of cyber criminals in exploiting loopholes and side effects of new technologies. On the other hand, it will point out to the already ongoing legal discussion about possible solutions for the problem of the „loss of location“ of stored computer data on the internet.