Bundeskriminalamt

HERBST-TAGUNG BKA AUTUMN CONFERENCE 2013

Cybercrime –

threat, intervention, defence

BKA Autumn Conference, 12 - 13 November 2013

Cyberterrorism, cyberespionage and cyberwar – a current threat assessment from the perspective of science

Abstract

Dr. Sandro Gaycken

Researcher in technology and security at the Freie Universität Berlin

Strategically important cyberespionage and cyberwar are no longer theoretical concepts.

There is evidence in support of this. China, for example, was caught in 2012 when a military cyberwar group committed very sophisticated industrial espionage. The attacker called “APT-1“ systematically spied out high-technology companies to make Chinese companies the leaders of global high-technology markets, as has meanwhile emerged from China. This goal seems to be strategically important enough to avoid the immediate cutback of APT-1 activities even in case of detection. The campaign is still ongoing, but operating from Africa and targeting Europe. Other states, too, have become more transparent. Edward Snowden unveiled interesting facts about the United States Cyber Command, for example. A particularly alarming piece of information has only recently been published by the information technology media. The Command carried out 231 offensive operations in 2011 and invested 652 million US Dollars in high-tech backdoors in the IT ecosystem. These figures are quite significant. The 231 offensive operations such as Stuxnet and Flame in the year 2011 targeted more than 18,000 computers and networks, some of which were heavily secured, and not a single operation has been unearthed in its most basic form and disclosed - an enormously important observation on the systematic deficiencies of our ideas of IT security and on the apparent efficiency of our CERTs and SOCs, our detection and awareness. After all, a backdoor investment of 652 million US Dollars is game-changing in itself. Given a strategic installation of the backdoors "early on“ in the production process and "bottom up“ in the stack, we can assume in view of this figure that a significant part of our IT environment has persistently been infected at hardware level and via operating systems – again absolutely undetected until today.

Other countries are even more difficult to monitor, but will hardly be more reserved in their efforts. Indicative of this are activities and budgets of the British GCHQ, the epidemic growth of cyber-mercenary companies offering high-tech exploits on the international market or the inclusion of the subject "cyber“ in the curriculum of the School of Economic Warfare in Paris.

The rapid evolution and commercialisation of offensive cyber activities make control of the multiplying cyber arms more and more difficult. Yet, we have no sustainable concepts of protection in response to this type of player. So what should be our idea of cyber security in future? The development of maximum security IT would be an option, and even one we could well establish especially in Germany. Our industrial basis, our cautious security policy in the field of offensive cyber

activities and our focus on a high level of security whilst at the same time taking into account civil liberties and privacies make us an ideal player for this new type of computer. However, we would have to overcome a number of initial difficulties to achieve this. Information technology marked by a high degree of security requires us to leave the path of "IT business as usual". Otherwise, we will, in any case, not be able to continue. The failure of "IT security business as usual“ becomes more and more tangible every day and urgently needs to be made public and politically acknowledged and addressed.