Cybercrime Convention – Is there a chance to stop it?

Cornelia Sollfrank talks to Andy Müller-Maguhn, spokesman of the German hackers' association CCC (Chaos Computer Club) about the upcoming Cybercrime Convention.

12 August 2001

Cornelia Sollfrank: What exactly is the Cybercrime Convention?

Andy Müller-Maguhn: The Cybercrime Convention is a collection of laws which will prohibit direct attacks on computers, but also, an this is an extension, the possession and the dissemination of tools for attacks will generally be criminalized. It will be forbidden by law that a hacker writes a program to automatically test system weaknesses. But such tools are essential for system administrators in order to check the stability of their systems.

The Cybercrime Convention goes even further by listing criminal offences where computers and the internet only play the part of a medium for distribution. I am talking about childpornography or let's say political material which is illegal in one of the participating countries. Regarding that aspect the legal situation differs in many countries.

The ideas of the proceedings of the Convention plan that in preliminary proceedings the accused is obliged to hand out the encryption key for data on his computer to the police if they think they would find evidence there. In case he does not, he will be sentenced not for what he was originally accused of, but for refusing access to evidence.

But this is just a few examples from the meanwhile 80 page document. An other interesting point is the law enfrocement treaty which says that criminal offences can also be sued from another country than that where the accused lives, even when his act is not illegal in his own country. The preliminary proceedings have to be allowed by the country, in which the accused lives, and then appropriate measures can be taken, like surveillance of telecommunication. All this is possible although, acoording to the law of his own country, the person didn't do anything illegal.

C.S.: What countries have contributed to the preparation of the Cybercrime Convention?

M.-M.: The Cybercrime Convention is a document of the Council of Europe–not to confuse with the European Union–which is an intergovernmental organisation of representatives from the 43 member states. Besides the 15 European states also Russia

and the states of former Yugoslawia are involved and work on regulatives for higher social and political problems, which in a next step, will be implemented as national law.

One really problematic aspect of the Cybercrime Convention is that politicians who have to sign it mostly are not very well-informed. They have learned about viruses and DoS (Denial of Service) attacks from the media, but have not the slightest clue how these things work technically. That is also the reason why they are unable to develop reasonable counter-strategies. Suddenly they have to sign a document which is the product of a highly intransparent process and all the security problems ostensibly will be solved. Putting it exaggerated, one could say that the Cybercrime Convention better serves to justify surveillance measures than guaranteeing computer security.

C.S.: You consider the politicians who are supposed to sign the convention as incompetent, at the same time, you are stating a tendency towards a police state. Who is it then exerting an influence? Who follows what interests?

M.-M.: Banning the tools for attacks in electronic networks is a highly doubtful act. It may make sense to forbid conventional weapons, but even there it is questionable, if a ban of weapons protects from bank robbery. But in terms of computer networks it is a completely different story. Here, tools for attacks are the same tools as tools for security.

C.S.: I am still interested in the question what interests shall be put through by the Convention.

M.-M.: In large parts the Cybercrime Convention reads as the DMCA and the authorization of NIPC (National Infrastructure Protection Committee), which means US-american ideas of how to guarantee computer security. That is securing systems not at a technical level, but by governmental surveillance. The main tendency of NIPC which has been founded to protect the national information highways from “cyberterrorism” goes into this direction. It is not about helping the operators of networked computer systems by handing out security tools, which would be the right way in my opinion, but about surveillance in order to be able to react to attacks. This won’t work, and only justifies a police state but not computer security.

C.S.: The Cybercrime Convention should be signed after the summer break mid September. Is there any plans to take action against the signing?

M.-M.: Here at HAL we have been dealing with the history and the characteristics of the document, together with my British colleague Gus Hosein from GILC (Global Internet Liberty Campaign) who is much more familiar with it than me, and in a little workshop,

we discussed strategies how to react to this for hackers highly alarming legislation. It is not yet decided if there will be a common resolution, or how we can address and educate our national politicians, and offer an interface for politics. One advantage hackers have in comparison to other organisations is that we do not only know how things work at a technical level, but we are dealing with it in an open way. We don't try to provide security by secrecy, but instead by merciless revelation. This is the only way to analyze the actual problems and to develop reasonable solutions.

European Council: http://www.coe.int

GILC - Global Internet Library Campaign: http://www.gilc.org

NIPC - National Infrastructure Protection Committee: http://nipc.gov

Published in: mute Magazine, Critical Information Services, issue 21, September 2001