United Nations A/CONF.213/IE/5

Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: General
19 March 2010

Original: English

Items 8 of the provisional agenda*

Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Background documents** received from individual experts***

UPBRINGING OF MINORS IN CYBERSPACE

Prepared by

Henrik S. Spang-Hanssen

* A/CONF.213/1.

** Distribution is limited to the quantities and languages in which the paper is made available to the United Nations Office on Drugs and Crime.

*** The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

UPBRINGING OF MINORS IN CYBERSPACE

Presented to
The Twelfth UN Congress on
Crime Prevention of and Criminal Justice
Salvador, Brazil, 12-10 April 2010

by

Henrik S Spang-Hanssen,[1] *Independent Senior Researcher*
(formerly Prosecutor and Supreme Court Attorney-at-law in Denmark)

Silicon Valley, California, USA
hssph@yahoo.com
http://hssph.net

---

1. Introduction

Today's children use computers from a very early age. They use them to learn, experiment and play. Unfortunately, such "innocent" childish use can imply the violation of domestic or foreign law.

So far, international law has generally protected minors by having a minimum age. However, the only existing international treaty relating to Cyberspace stipulates no minimum age for cyber criminals. Thus, even children in diapers theoretically can, pursuant to this treaty, commit criminal acts and be sentenced as criminals.[2]

This is due to several factors. One – with which this paper will deal – is education and upbringing of children in the computer age.[3]

The following section will provide some scenarios, which are the sum of many situations that have occurred in the past or seem likely to occur in the future.

---

[1] Author of among other things: **The Future of International Law: CyberCrime** (2007)(available from the Social Science Research Network's (SSRN's) Working Paper Series at http://ssrn.com/abstract=1090876); **A Just World under Public International Law in Cyberspace: Jurisdiction** - Chapter 1 to "CYBER JURISPRUDENCE" (Icfai University Press, 2008); **Cybercrime Jurisdiction in Denmark** - Chapter 8 to: CYBERCRIME JURISDICTION: A GLOBAL SURVEY (T.M.C. Asser Press , 2006); **Public International Computer Network Law Issues** (Chapter 7 on cyber crime)(DJØF Publishing, 2006); **Cyberspace & International Law on Jurisdiction** (DJØF Publishing, 2004).

[2] However, this regime seems counter to the spirit of the Hague Convention on Jurisdiction, Applicable law, Recognition, Enforcement and Co-operation in Respect of Parental Responsibility and Measures for the Protection of Children of 19 October 1996 (entry into force 1 January 2002; ratified by 19 states as of September 2009), at www.hcch.net/index_en.php?act=conventions.pdf&cid=70 (last visited 10 March 2010).

[3] Another is when and where a cyber crime is committed – an unsolved jurisdictional question, which another paper of mine will address.

One thing appears unmistakably clear: the international community should conclude a proper treaty related to crimes involving computer use as well as to information that is required to educate children fairly and effectively in the computer age.

2. Scenarios

Peter, Louise and Ahmed are cousins – all under 15 years of age – but live with their families in different countries.

Peter and Ahmed love to play games on their computers, including with each other online. Peter lives in a country where game-betting is legal. Fancying himself as some kind of a "businessman," he suggests that Ahmed solicit bets from his school and play mates; and Peter will then, online, place the bets against a small fee. Subsequently, Ahmed sends his cousin several bets.

Ahmed is somewhat of a computer nerd and invents a software program that should be able to retrieve forgotten passwords. He tests the software on his own and his father's computers and it seem to work. He proudly informs his cousins about it and both ask him to send them the program to them via the Internet.

Peter immediately installs the program and tries to see whether he can find passwords to the local branch of an international bank. He succeeds and informs Ahmed.

Ahmed tells one of his schoolmates, Paul, about the software. Paul likes to hack into computers, just to find out whether he can bypass firewalls, etc. At the school, Paul copies the software from Ahmed's laptop while it is unattended. He then uses Ahmed's software to hack into foreign state CDONU's military's computer network. Paul has never intended to destroy or copy anything. However, in this instance he cracks some parts of the military systems, because of an unintended feature in Ahmed's software.

Louise also installs the software and tries to see whether she can find her father's password to the national television station, so she can bypass the parental protection settings to television programs. She succeeds.

She also writes an essay on religion as a school assignment. She uploads the paper on a website, which only uses the language of her country.

The bank realizes the computer break-in by Peter and the police seize his computer. While checking Peter's e-mail the police find the correspondence between the cousins.

The police in Peter's country inform the police in the countries where Louise and Ahmed live and these police forces seize Louise's and Ahmed's laptops. The police then find out about Louise's use of the software.

The police also discover that Paul has copied Ahmed's program, seize Paul's computer, and get an idea of how he has used the software.

The police notify the CDONU's military, which requires that Paul and Ahmed be extradited for prosecution.

Meanwhile, a clergyman on a foreign continent discovers Louise's paper on the website. He is able to read the foreign language, is appalled about the content, and calls for his local law enforcement agency to bring criminal charges against Louise.

Both Louise's and the clergyman's countries are parties to the CyberCrime Convention of 2001, which requires each party to prosecute or extradite violators. Neither Ahmed's nor Peter's or Paul's countries are parties to this convention.

Elsewhere, a woman belonging to a criminal gang approaches a 14-year-old girl, Tania, in a public library and asks her whether she wants to earn $100 by connecting a USB flash-drive stick to one of the public library's computers and pressing an "OK" button when it appears on the screen. The woman explains that she is not confident in using computers.

Tania accepts the offer, inserts the USB stick, and clicks "OK" on the screen, which next states that "all is well and the program will now shut down itself." What actually happens is that the clicking of the OK button initiates a program that starts copying several stores' credit card data, which is then transmitted to the criminal gang's computer in foreign country Charge.

Tania's country is not a party to the CyberCrime convention.

Ahmed's local police find that he has violated a criminal misdemeanor code by participating in Peter's betting business, because Ahmed has been soliciting his mates as customers. However, as Ahmed is under 15, he is – pursuant to the national criminal code – considered a minor; and, as he has only committed a misdemeanor, he cannot be charged.

As Ahmed only used his software on his own and his father's -- not third parties' – computers, he has not violated any computer-related national laws.

Ahmed's government rejects the request it has received to extradite him to the foreign country CDONU.

Peter, even though he has used the software and to break into the local bank's computer network and obtain passwords, is not being charged by the local police, as they find him to have had no intent to use (and, in fact, not to have used) the passwords. Only the use of a criminally-obtained password is considered a violation pursuant to the local criminal code.

As for the article on the website, Louise's work is protected by her state's constitutional free-speech provision. Her local police do find, however, that she has violated the criminal code by breaking into the national television's computer network. Yet, because Louise is under 15, she is a minor under that code and thus cannot be charged.

Louise's government decides not to prosecute the claim from the clergyman's country. But due to the CyberCrime Convention's mandatory rule of "prosecute or extradite," the government determines it must extradite Louise. Nonetheless, on appeal, the country's supreme court rules in favor of Louise's claim against extradition based on the protection in the constitution.

Paul's local police find he has violated the criminal code by stealing the software from Ahmed's computer. As Paul is under 15, he is also a minor, per the national criminal code. However, because he has committed a felony, he can be charged. The court convicts him and then sentences him, due to his age, to community service every Saturday for one year, instead of one year in prison. For the same period, he is not allowed to use a computer unattended.

As for the hacking of foreign country CDONU's military computer, Paul has not violated any national law in his own country. The foreign country CDONU nevertheless demands Paul's extradition for having violated its criminal code on national security. Paul's attorney brings the government's decision to extradite him before the courts. On appeal, the supreme court decides to allow the extradition. However, the court adds conditions to the extradition, namely that any jail sentence imposed cannot exceed the maximum limit for similar national security crimes in Paul's country (twenty years) and further that the sentence has to be handed down in total for all the offenses found by the court in CDONU.

A jury in CDONU finds Paul guilty of three charges, which verdict would normally carry a sentence of three times sixty (i.e., 180) years in jail pursuant to the CDONU criminal code, with a right to parole after two-thirds of the time has been served. However, the court in CDONU reduces the jury's sentence to twenty years due to the extradition conditions attached by Paul's country.

Tania's local police find she did not have any intent to violate any law and determine not to press any charges. However, country Charge requires that Tania be extradited and her country's government authorizes the extradition due to an existing bilateral extradition treaty. A jury in country Charge then finds Tania has violated its criminal code pursuant to which it is a crime to copy credit card information from a database. The code has a "Three Strike Rule", under which the minimum sentence of imprisonment is 25 years. The jury finds seven databases have been copied and that the Three Strike Rule should be used. Tania is sentenced to 25 years in prison.

3. Comments

The above scenarios are not exercises in paranoia, for they are not far-fetched and they accurately illustrate how different countries deal with criminal violations committed by children using computers.

Also, they show how important it is that parents, kindergartens, teachers, school officials and others involved in bringing up children teach children from a very early age to think about – step by step - the consequences of their computer use.

Perhaps children ought to be told that computers can be as dangerous as cars. We do not allow young children to drive cars because cars can be dangerous "weapons" and harm others. In the same way, giving children access to computers can be a cause of harm to themselves and to others, sometimes with disastrous results.

At the same time, governments and other entities have embraced projects like "One Laptop per Child"[4] so children from all corners of the world, and from a very young age, can use computers as a window to education.

However, it appears that there have been no real efforts to teach children about the proper use of computers/computerized information and the dangers therein.

Education is needed not only of children but also of parents and other persons involved in bringing up children. Children's perceptions of what is right and wrong are sometimes far from what is contained in applicable criminal codes. A Danish report "Rigtigt og Forkert" [Right and Wrong] of 2006[5] from Børnerådet [Danish National Council for Children] states that 8 out of 10 students surveyed in eighth grade thought it was permissible to copy music and movies; whereas only 5 percent thought it was all right to steal [a physical object].

As a result, it seems clear that children need to be taught what is right and wrong when using a computer. But their parents may often themselves know little or nothing about computers and how and for what their children are using them.

Accordingly, the international community has a great task ahead of it in terms of educating both parents and children about computer use and the possible criminal consequences of the same.

As for penalties, in many cases, the violator – whether minor or adult – has absolutely no idea of how, or in which states, they can be indicted, convicted, sentenced and imprisoned.

Meanwhile, many countries have recently been considering a special version of the Three strike rule, after which an individual can – following the third conviction – be excluded from access to the Internet for a prolonged time period. However, in today's increasingly online world this would be tantamount to excluding the individual – especially a child – from education and, ultimately – through the computer deprivation – even from full participation in society.[6]

Now, in many situations, it is still true that a minor, when asked specifically whether the effect of computer wrongdoing could occur abroad, will indeed have some realistic idea and understanding that it might – and this may be seen to be the case for Peter and Paul in the above scenarios.

However, in other cases the minor – or even an adult – will have no conception that his/her use of a computer has foreign implications,[7] as in the scenario above where Louise uploads her article to a website. Even if she did know her own national constitution/law, she would be highly unlikely to have any idea of the criminal legislation provisions existing on a different continent. In most situations, the adults bringing up Louise, that is her parents and educators, would also be surprised that her act was illegal anywhere – let alone that she could be extradited to a foreign country, tried, convicted and sentenced for it.

Consequently, it can be reasonably asserted that there really must be some serious consideration put into creating rules of public international law governing Cyberspace and the limits of national jurisdiction over it -- including, arguably: "Let it be stated by the international society that whatever is done legally in the cybernaut's own country shall not cause such individual to be charged or indicted in a foreign country or countries – except for cases of extreme harm that are reasonably foreseeable."

Without such rules, there simply can be no predictability in the international community as to where – that is in which states – the criminal computer act has been initiated and executed, which places (again, states) in which courts can exercise jurisdiction to adjudicate and enforce.

The international community must also decide upon applicable standards and norms for Cyberspace issues. For example, to what extent – if any – should "spamming" be considered a

---

[4] Originally called XO-1 or the $100 laptop, or the Children's Machine [see http://en.wikipedia.org/wiki/OLPC_XO-1], some of which have had a clamp-on crank generator as power option. A newer version will be known as the XO-3 and look like a tablet [see www.wired.com/gadgetlab/2009/12/xo-3-concept-a-crazy-thin-tablet-olpc-for-just-75 & http://laptop.org/en/laptop/hardware/xo3.shtml]

[5] Pdf download (in Danish) at http://www.boerneraadet.dk/files/Brd.dk%20Filbibliotek/PDF%20FILER/PANELRAPPORTER%20OG%20PIXIE%20(DONE)/Rigtigt%20og%20forkert/Rigtigt%20og%20forkert.pdf.

[6] The E.U. Commission has pledged to make sure the ACTA global treaty will not force countries to disconnect people for unlawfully downloading copyrighted music, movies and other material, "*Europe 'will not accept' three strikes in ACTA treaty*", ZDNET UK, 26 February 2010 at www.zdnet.co.uk/misc/print/0,1000000169,40057434-39001101c,00.htm (last visited 5 March 2010).

[7] In an American juvenile case from 2005, the minor told the judge: "Seventeen months ago, I made the worst mistake I ever made in my life. I did it out of curiosity and did not think I would cause any damage. I am sorry I created problems for people I did not even know," *US vs. An Unnamed Juvenile*, http://www.justice.gov/criminal/cybercrime/juvenileSent.htm (last visited 10 March 2010).

(cyber-)crime?[8] Then – and only then – will it be possible to delineate what cybercrime is and how to prevent it – in the end, through education of Internet users.

Finally, as for acts that are not destructive of computer networks, – a lesson could be learned from developers of the Internet Protocol (IP), who have stated: "Be liberal in what you accept, and conservative in what you send"...and who have also suggested that we "teach our children to think more deeply about what they see and hear" because "[t]hat, more than any electronic filter [and laws], will build a foundation upon which truth can stand."

4. Final Remarks

It may well be that this UN Congress should recommend all child computers have a solemn start-up warning screen similar to those used by the international film industry on DVDs. Namely, a quite harsh but accurate statement should be made that illegal use of a computer is a violation of the law and that the penalties for such use can include many years of imprisonment – possibly even in a foreign country's jail. Children could perhaps even be required to interact with such warning by clicking an "I agree" button each time they turned on/reactivated the computer – for, like it or not, repetition is often a good "teacher."

The main thing to understand to pursue here is that active efforts to teach children what is right and wrong are vital before they become "real" (continuing) criminals or determined destructive hackers ("cyber-terrorists").[9]

In conclusion, I sincerely hope this Congress will seriously consider asking the UN Commission on Crime and Criminal Justice to draft in time for the next Congress a "United Nations Internet Crime Convention," integrating United Nations Standards and Norms in Crime Prevention and Criminal Justice and at least suggesting how best to provide international computer education and training from an early age.

---

[8] The percentage of electronic spam is often similar to the percentage of unsolicited mail in a physical mailbox. Thus, spam could be held to be a "service-provider problem" (that is, not having enough copper wire/broadband for PR-commercials) rather than regarded as a crime similar to a distribution of service attack ("DoS") (that is, making a computer resource unavailable to its intended users by intentionally overwhelming it with data – "a network terrorist-attack").

[9] See "*Computer Hackers: What to Do with Them*" by D. Batchelor (Canada), A/Conf.187/13/Add.2 to the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders at https://www.asc41.com/10th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/021%20ACONF.187.13.Add.2%20Computer%20Hackers.pdf (last visited 10 March 2010).