United Nations

A/CONF.187/13/Add.2

Tenth
United Nations Congress
on the Prevention of Crime
and the Treatment of
Offenders

Distr.: General
10 April 2000

English only

Vienna, 10 – 17 April 2000

Agenda item 5

Effective crime prevention: keeping pace with new Developments

Computer Hackers: what to do with them, by D. Batchelor (Canada)

Statements submitted by experts[*]

Note by the Secretariat

1. In its resolution 53/110 of 9 December 1998, the General Assembly emphasized the importance of the workshops to be held within the framework of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and invited Member States, non-governmental organizations and other relevant entities to support financially, organizationally and technically the preparations for the workshops, including the preparation and circulation of relevant background material.

2. In its resolution 54/125 of 17 December 1999, the General Assembly encouraged Governments to make preparations for the Tenth Congress, including by establishing national preparatory committees, with a view to contributing to a focused and productive discussion of the topics and to participating actively in the organization of and follow-up to the workshops, the submission of national position papers on different agenda items and the encouragement of contributions from the academic community and relevant scientific institutions. In the same resolution, the Assembly called upon the specialized agencies and other relevant United Nations bodies and institutes and other intergovernmental and non-governmental organizations to participate effectively in the Tenth Congress and to contribute to the formulation of regional and international measures aimed at preventing crime and ensuring justice.

3. Pursuant to rule 60 of the provisional rules of procedure for United Nations congresses on the prevention of crime and the treatment of offenders (A/CONF.187/2), written statements related to the work of the Congress submitted by the designated representatives, individual experts or observers are to be distributed by the secretariat to all delegations in the quantities and in the languages in which the statements are made available to the secretariat for distribution, provided that a statement submitted on behalf of a non-governmental organization is on a subject in which it has a special competence.

[*] 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.

COMPUTER HACKERS: What to do with them.

A paper prepared for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders by Dahn Batchelor *criminologist*

There is a lake on the eastern edge of the Sacramento Valley and the western edge of the Sierra Nevada Mountains in the state of California called Oroville. It is 22 kilometers in length and its shoreline is 241 kilometers as the lake splits off into its various finger-like extensions protruding in many directions. Its depth is 213 meters and its volume is enormous. At the western end of one of those protrusions is the Oroville Dam. It controls water for the thousands of farms in the huge valley and more importantly, it supplies a great deal of the hydroelectric power for California.

During spring thaws, the engineers discharge excess water through eight gates in the middle of the dam. These gates are ten meters high and 5 meters wide and if they were opened to their fullest, as much as one hundred and fifty thousand cubic feet of water per second could cascade down the river leading towards the small city of Oroville, six kilometers away.

Opening all these gates at the same time while the river is already at its high point would cause a huge onslaught of water roaring down the river and wipe out the small city below it, drowning thousands of people in minutes and then head into the valley and flood hundreds of thousands of acres of farmland. The cost of this would be in the billions of US dollars.

Naturally, there are safe guards against this kind of catastrophe happening. In a facility south of the dam, the engineers use computers to monitor water flows. The valves in the powerhouse and the heavy steel gates in the middle of the dam are controlled by these monitors.

Dedicated phone lines connect the dam's computer system to a server in Sacramento, the state's capital, allowing the State Water Bureau to order releases of water electronically. Dozens of dams and sluices are connected by computer to Sacramento thereby allowing the authorities to oversee the water flow throughout the state.

A twelve-year-old boy, a boy of exceptional intelligence, living in city of London, UK who has more than the basic knowledge of computer hacking (much of what he picked up on the Internet) could link up his cheap computer with two or three supercomputers in the United States for the purpose of breaking through the firewall of the computer system in California or decoding the computer's password. The supercomputers would, through their brute force, match every letter, number, punctuation, and even the control symbols (characters made by pushing the control key at the same time as another key) until a thousand quadrilllion unique passwords have been browsed through and the password the boy is searching for, is finally found.

Then one spring night in the city of Oroville, where thousands of its inhabitants are asleep, as are many thousands more in the farms in the valley below the dam, the twelve year-old boy after having finished eating his lunch, is looking at his computer screen and realizes that he has the power to control the steel gates in the middle of the Oroville dam which is holding back the enormous amount of spring runoff water behind them.

He follows the instructions the computer in California gives him to open the gates and all that is left for him to do is for him to press, ENTER. He thinks that by doing that, he will open one of the gates part way and not really cause any harm at all. He doesn't realize that he didn't follow the California computer's instructions properly. He presses ENTER and in doing so, he opens all of the gates at the same time and as such, he has condemned thousands of people to death.

Millions of tons of water cascade down the river, hundreds of feet in height, like a tidal wave, destroying everything in its path. As the boy looks at the screen of his computer and marvels at how he, a twelve-year-old boy can lift a heavy steel gate, a gate weighing hundreds of tons, upwards, a gate that is half way around the world at that, he is completely oblivious to the fact that while he is patting himself on his back, thousands of innocent victims are drowning in the deluge hitting them. While he is thinking about what he is going to watch on TV that night, the electrical system of most of California is now down, causing millions upon millions of people to do without their phones, their lights, their heat and a great deal of the emergency measures that might have been available to them. While he is later having his supper, the surviving farmers and their families in the Sacramento Valley are seeing the dawn of the new day as the rising sun is reflected off the surface of the water that has flooded their farmlands and drowned members of their families and their friends.

This is the result of thoughtless computer hacking but this scenario pales when compared to what could really happen if a number of computer hackers decided to destroy an entire nation.

Computer hackers can get into any computer system if they take the time to break into them. For example, one would think that the American Central Intelligence Agency, the CIA, would be protected by encrypted codes, secret passwords and fire walls that would keep anyone out of their computer systems. Not so. One day a hacker got in and changed the wording of the CIA's home page so that visitors to the CIA's home page read, "Welcome to the Central Stupidity Agency." In that instance, no real harm had been done but it was a powerful wakeup call for the CIA and the American government.

During the Gulf War, Dutch hackers stole information about the U.S. troop movements from U.S. Defense Department computers and tried to sell it to the Iraqis. In March 1997, a 15-year-old Croatian youth penetrated computers at a U.S. Air Force base in Guam. In 1997 and 1998, an Israeli youth calling himself "The Analyzer" hacked into Pentagon computers with help from California teen-agers.

Ten computer hackers who might spend several months making their preparations for the purpose of closing down most of the computers in any country or destroying the information programmed into the computers and when the precise moment arrived, they, acting in unison, could cripple an entire country as large as the United States, within 30 seconds. If the country's main computer's programs were destroyed at the same time, it could put that nation back into the dark ages for several years.

We can spend billions trying to improve the security of our computers but when a twelve-year-old can get into the most sophisticated system, and wreak havoc upon thousands upon thousands of innocent victims half way across the world, then we have to try something else.

There are four types of computer hackers around the world. The first is the hacker who illegally slips into computers to change the data to meet his intentions, such as committing a fraud, altering facts or obtaining information he's not entitled to. The second is the hacker who does it because, and I will quote that famous mountain climber, Mallory, "Because it is there." He likes the challenge and although he doesn't want to do any harm, he can unintentionally cause harm. The third kind of hacker is the amateur cyber-terrorist. He is the kind of person who illegally goes into computers for the purpose of destroying data, altering data that will have an effect on others, shutting down computer networks that can end up causing great havoc in any or in all parts of the world. He has no conscious. He simply doesn't give a tinker's dam who he hurts. He is addicted to one thing. Power. He gets it by acting as a cyber-terrorist. He is a nobody, who through his own efforts alone, can make his existence have meaning to him because his existence can have an effect on the lives of millions of people around the world. And finally there is the professional cyber-terrorist. He is the hacker who is hired to destroy whatever he can to wreak havoc on a nation.

We must be mindful that access to the information highway is no different than having access to our highways and streets around the world. To drive on those highways and streets is a privilege, not a right. We are licenced as motorists and if we do something wrong, we can be traced and when found, punished and our privilege to drive on our highways and streets can be suspended and even revoked.

Since cellular phones are licenced, why shouldn't computers be licenced also? Perhaps all persons who want the right to use the Internet should have their computers licenced. And if the owners or their friends do harm to other computers, they too, like the careless or dangerous motorist, can be tracked down and taken off of our information highways and where appropriate, punished with imprisonment for what they have done.

In the case of *United States v. Morris*, this man's conviction in 1991 and sentence of only three years' probation and a $10,000 fine were upheld by the United States Supreme Court.

Today, in the U.S., the most likely avenue of prosecution is the Federal Computer Abuse Act of 1994. The Act outlaws the "transmission of a program, information, code, or command" that "causes damage to a computer, computer system, network, information, data or program." For those who intentionally cause damage by transmitting a virus, the punishment can amount to ten years in federal prison, plus a fine. For those who transmit a virus with only "reckless disregard" to the damage it will cause, the maximum penalty
stops at a fine and a year in prison.

The trouble I have with a penalty of only one year for those who illegally hack into other computers with reckless disregard for the harm they can cause is that these people can bring about unnecessary deaths because of their actions.

I believe that cyber terrorists who are first-time offenders should be sentenced to a minimum of ten years in prison. Second time offenders should serve twenty years and third-time offenders should serve forty years. And if these convicted cyber-terrorists are convicted of other offences related to their cyber-terroristic acts, then the ten, twenty and forty-year sentences should be served consecutively to the other sentences.

These proposed sentences should be world-wide so that no matter where the cyber-terrorists operate, their sentences upon conviction in their own country can be the same as they would be in the victim countries.

The measures we take to protect ourselves from cyber-terrorists is not the same as that which we take to protect ourselves from burglars who break through our doors and windows of our homes at night. At present, our computer programs are housed in tents made of gauze in which a teen-age vandal with a match can burn down in an instant. We must take extreme measures to protect our computer programs from cyber-terrorists. If we don't, then the only way our computer programs will be safe from the hackers is to disconnect all of our computers, place them is titanium-lined vaults and have well-paid guards standing watch over them. When that happens, computers would become a thing of the past.