unicri
advancing security, serving justice,
building peace

HOW APPLIED RESEARCH CAN CONTRIBUTE TO ENHANCED MANAGEMENT OF CYBER THREATS

Speech by Mr. Sandro Calvani, UNICRI Director

High Level Segment
International Telecommunication Union Council 2008
Brussels, 12 November 2008

Distinguished Colleagues,
Ladies and gentlemen,
Good morning and welcome!

It's a pleasure for me to be here today to participate, in my capacity of UNICRI Director, to the session on cybersecurity of the High-Level Segment – ITU Council 2008.

UNICRI is working on the field of cybercrime for an in-depth and better understanding of the phenomenon, in order to formulate ad hoc prevention policies, to develop security methodologies and techniques, and to strengthen the capacities of the actors involved in investigating and prosecuting cybercrime.

Effectively investigating and prosecuting cybercrime is a specialist work and there are three different challenges that the stakeholders involved in curbing cybercrime, and especially law enforcement agencies, have to face:

1) Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;

2) Legal challenges resulting from laws and legal tools needed to investigate cybercrime lagging behind technological structural, and social changes; and

3) Operational challenges to ensure the creation of a network of well-trained, well-equipped investigators and prosecutors who work together with unprecedented speed - even across national borders.

United Nations
Interregional Crime and Justice Research Institute
Viale Maestri del Lavoro,10 - 10127 Turin, Italy
Telephone: (+39) 011 653 71 11 - Telefax: (+39) 011 631 33 68
E-Mail: unicri@unicri.it - Web site: www.unicri.it

As far as technical challenges are concerned, finding an electronic criminal means that law enforcement must determine who is responsible for sending an electronic threat or initiating an electronic robbery. To accomplish this, law enforcement must in nearly every case trace the "electronic trail" leading from the victim back to the perpetrator. Tracing a criminal in the electronic age, however, can be difficult, especially if we require international cooperation, if the perpetrator attempts to hide his identity, or if technology otherwise hinders our investigation.

As networked communications and e-commerce expand around the globe, businesses and consumers become more and more vulnerable to the reach of criminals. The global nature of the Internet enables criminals to hide their identity, commit crimes remotely from anywhere in the world, and to communicate with their confederates internationally. Criminals can choose to weave their communications through service providers in a number of different countries to hide their tracks. As a result, even crimes that seem local in nature might require international assistance and cooperation.

Naturally, criminals like these, who weave communications through multiple countries, present added complexities to governments trying to find criminals. Mutual legal assistance regimes between governments anticipate sharing evidence between only two countries, that is, the victim's country and the offender's country. But when a criminal sends his communications through a third, or fourth, or fifth country, the processes for international assistance involve successive periods of time before law enforcement can reach data in those latter countries, increasing the chances the data will be unavailable or lost, and the criminal will remain free to attack again.

At the same time, the global nature of the Internet makes it easy for a criminal armed with nothing more than a computer and modem to victimize individuals and businesses anywhere in the world without ever setting foot outside his or her home.

Cybercriminals know no national boundaries, and the multi-jurisdictional nature of cybercrime requires a new multilateral approach to investigations and prosecutions.

To succeed in identifying and tracing global communications, law enforcement agencies must work across borders, not only with their counterparts throughout the world, but also with industry, to preserve critical evidence such as log files, e-mail records, and other files, and they must be able to do so quickly, before such information is altered or deleted. If they cannot get this information quickly, the investigation may grow cold.

While less sophisticated cybercriminals may leave electronic "fingerprints," more experienced criminals know how to conceal their tracks in cyberspace. With the deployment of anonymous software, it is increasingly difficult and sometimes impossible to trace cybercriminals. At the same time, other services available in some countries, such as pre-paid calling cards, lend themselves to anonymous communications. All of these technologies make identifying criminals more difficult, even though they have other benefits.

There are countless technical challenges that law enforcement agencies face, like those stemming from Internet telephony, strong encryption, and wireless and satellite communications. The technological advances in electronic commerce and communication that have led to the explosive growth of the Internet have also made it possible for international criminals to target victims in all our countries in unprecedented ways.

The second type of challenge for law enforcement agencies is in the legal arena. Deterring and punishing computer criminals require a legal structure that will support detection and successful prosecution of offenders. Yet the laws defining computer offences, and the legal tools needed to investigate criminals using the Internet, often lag behind technological and social changes, creating legal challenges to law enforcement agencies. In addition, some countries have not yet even adopted computer crime statutes.

All nations must take the threat of cybercrime seriously. Hacking and virus-writing and proliferation are not simple pranks, but injuries that have significant security and financial consequences. At a time when the number of crimes carried out through the use of computer technology is increasing at an alarming rate, it is especially important that law enforcement officials around the world demonstrate that such crimes will be punished swiftly and with an appropriate degree of severity. When one country's laws criminalize high-tech and computer-related crime and another country's laws do not, cooperation to solve a crime may not be possible. Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement.

For those countries that do have computer crime statutes, they must also have appropriate procedural laws in place to investigate crimes. We must recognize that technology is constantly changing and that procedural laws need to be updated.

In addition to technical and legal challenges, law enforcement agencies around the world face significant operational challenges. The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexity of these

technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions.

Every country should have dedicated high-tech crime units that can and will respond to a fast-breaking investigation and assist other law enforcement authorities faced with computer crimes.

Given the quickly evolving nature of computer technology, our nations must also continue to increase their computer forensic capabilities, which are so essential in computer crime investigations. Keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software.

In addition, because of the speed at which communications technologies and computers evolve, prompting rapid evolution in criminal trade craft, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases.

Capacity building and awareness-raising about information security issues of end-users are also essential to allow them to protect themselves against the menaces posed by cybercrime.

In conclusion, I wish to stress the importance of the ITU Global Cybersecurity Agenda as a tool that merges the different strategies for curbing cybercrime, namely: strengthening capacity building and international cooperation, adopting legal, technical and procedural measures and building-up organizational structures and policies on cybercrime.

Thank you for your kind attention.