AWARD NOTIFICATION

Congratulations your identity has been sold!

All our lauded technological progress -- our very civilization -
is like the axe in the hand of the pathological criminal.
(Albert Einstein)

Over the last years we have witnessed changes as we analyzed criminal trends and elaborated new strategies to confront crime. New scenarios have emerged, which have obliged us to improve knowledge and to rethink strategies. These changes are the direct consequences of a wired world driven by global markets where

frontiers are abolished mainly in the name of economics. This new world, dominated by new information and communication technologies, has also redefined the criminals' profile and their modus operandi.

Most of the criminal phenomena we are fighting today are transnational. The network woven by organized crime has also become part of our daily life, it has infiltrated the new information and communication technologies (ICT) and, the more we depend on these, the more we are potential victims. ICTs have expanded our possibilities, but they have also enabled a wide spectrum of offences, and the magnitude of these violations can reach impressive levels through the Internet.

Nowadays, security is no longer just an issue in the real world: it is a virtual matter as well. Therefore, trying to be on the safe side today also means having a good firewall, a strong program to detect viruses, avoid answering messages from unknown senders or sharing sensitive information on unprotected channels, and so on.

As it turns out, the likelihood of suffering from a real crime, like being robbed in the street, is actually smaller than the possibility of suffering a virtual crime, such as an on-line identity theft or a credit card fraud. Committing cybercrimes is much more profitable, significantly less risky and strictly linked to market logic and trends. Moreover, many of them no longer require a high level of expertise or sophisticated techniques.

Internet abuses may originate anywhere in the world, no matter where the target happens to be. How we defend ourselves from crime has changed, but we should consider that organized crime is becoming faster and more aggressive in exploiting new technologies and in sharing their know-how with the hacker community.

However, none of us can deny that the impressive changes that information technology has brought to our societies have also allowed for the development of countries and democracies, and for the improvement of people's life standards.

According to the International Telecommunication Union (ITU), in 2009 an estimated 26 percent of the world's population (or 1.7 billion people) were using Internet. This means that one out of four persons has opened a window to the rest of the world: they can avail themselves of the amazing opportunities offered by the Internet, but, at the same time, they can also become a victim of cybercrime.

We can now exchange data, information and know-how from one side of the world to another in just a few seconds. The accessibility of information combined with the fact that all aspects of our life are electronically stored are the two aspects that contribute to our socio-economic development, our possibility to enjoy the freedom of a world simultaneously connected to us, but also to our vulnerability to cybercrime. The Internet breakthrough and its widespread accessibility are the technical factors that have allowed the emergence of cybercrime: phishing, pharming, credit card fraud, identity theft, computer espionage, hacking, the elaboration and diffusion of viruses and worms, just to mention a few, are now part of our common dictionary.

Think about it. One of the articles here included mentions that, considering 1995 as "year 0" (the last year before the Internet boom erupted in many countries), Interpol knew of only 4,000 child abuse images; today it totals around 1,000,000, and the number of children abused to make them runs in the tens of thousands. And this is but one of the many facets of crime in the Internet Era. A bot herder can remotely control thousands of victim computers at once, including yours, and launch a systematic and widespread attack with just the click of a mouse. The UN estimates that identity theft alone can account for around 1.5 million victims, with an estimated annual value of 1 billion USD.

Furthermore, we are speaking about a world that right now is still only partially connected. Africa: is going to be the latest Internet-connected continent, also thanks to the recent FIFA World Cup, which this year has doubled the continent's Internet links capacities. In a region where the hardware platforms and the operating systems are outdated, security issues, mass-worms and botnets could spread through Africa. This could mean a new wave of targeted attacks that may have a serious impact on African financial institutions and

national critical infrastructures, such as oil and gas pipelines.

In this landscape, cybercrime represents a real challenge to governments' security: militaries have been working for years on issues like cyber espionage and cyber war scenarios, just to mention few. Let's imagine the consequences of a cyber attack to a crucial infrastructure: the outbreaks of violence, looting, plunder and destruction that occurred during the 1977 blackout in New York would fade in comparison.

From the evolution of cybercrimes, to terrorist use of information technology, to the main offences committed through the Internet, this issue of the Magazine aims to improve our knowledge of phenomena that could potentially affect or are already having an effect on each of us: cybercrime. This issue includes several perspectives on cybercrimes and suggestions to reduce our vulnerability and on how to prevent them.

The fight against cybercrime is not a journey towards the unknown (although it is almost impossible to identify the offenders): it is actually a matter of creating a collective strategy to avoid criminals from taking advantage of the weakest links of the chain (lack of legislation, of technical expertise and statistics, poor coordination across borders and sectors) and to exploit to its utmost the global market opportunities driven by new technologies.

The world we know today is not capable of surviving a collapse of the system of information technology. But, on the other side of the coin, our increased vulnerability should not be neglected.

Doris Buddenberg, Officer-in-Charge of UNICRI