How can we combat cyber crime?

A group of researchers are aiming to shed new light on how legislation can be used to stop these criminals.

Computer technology pervades almost every area of society and social sphere. Our pre-Internet way of life is now consigned to the history books – no one born after the early 1990s has experienced a world without the Internet.

However, advances in computer technology are also enabling criminals to commit crimes. They can steal your identity, dupe you into disclosing sensitive information, and distribute information about your children and pictures of them. These crimes are in principle the same as the “classic” crimes, such as theft, forgery, fraud and illegal gambling.

The villains of the piece, however, are no longer masked gunmen, but organizations consisting of invisible and anonymous computer experts who operate in cyberspace. And the investigator – the modern-day Sherlock Holmes – is not a man with an impeccable logic and exceptional powers of deduction, but a network of computer systems and highly qualified technologists.

Who is winning the race?

Two uncompromising sides are pitted against each other: advanced organizations of expert cyber criminals on the one hand, and international institutions with highly competent researchers, including legal professionals and technologists, on the other. The technology is the same, but it is the use and misuse of the technology that separates the good intentions from the sinister ones.

Investigating cybercrime is a process riddled with challenges, in which computer experts hunt down other computer experts.

The work is extremely resource intensive, and even with competent investigators, a lack of resources can lead to unfruitful police investigations. There is no telling how and when the race will end, but both the scale and speed of the race appear to be intensifying.

Haven for criminals

“Combatting cybercrime presents a number of legal challenges. For example, applying existing legal rules to cybercrime can prove difficult when the terminology used in the rules does not keep pace with technological advances,” asserts Lee Bygrave, who is a Professor in Law and heads the research project SIGNAL.

The four-year project started in January 2016 and aims to “examine changes in the legal framework for network security by focusing on established, new and proposed security requirements aimed at critical Internet infrastructure and cloud computing”.

New times, new dimensions

Computer-savvy criminals are well versed in exploiting the benefits of a world where physical and virtual boundaries are much more diffuse than before. Using computer technology, a small group of cyber experts can perform criminal acts on a colossal scale. They can threaten a nation’s security, wreak financial havoc, organize terrorist activities or paralyze vital national networks. However, even crimes of smaller proportions, such as identity theft, bullying and the distribution of child pornography can cause a great deal of harm.

“The extent of cybercrime is anyone’s guess; it is the big unknown in the field. According to a survey conducted by the Norwegian Business and Industry Security Council (NSR), a total of 23,500 instances of hacking or unauthorized modification or deletion of data were carried out in 2010, but the number reported during the corresponding period and in the same categories was just 218. Underreporting and reluctance to report cybercrime seems to be a trend. One of the reasons may be low expectations of the police’s ability to deal with such cases,” suggests Bygrave.

Phishing expedition

One example of cyber fraud is Internet banking fraud, which is carried out using sophisticated computer programs. The acts are carried out by teams whose members specialize in different areas of the operation. Some develop and update malware, while some produce and spread viruses, and others are responsible for recruiting money collectors.

Another example that most of us are exposed to is identity theft. The main characteristic of this type of crime is that someone pretends to be someone else. It is not uncommon to see an e-mail where the sender is supposedly a reputable bank needing to verify customers’ personal details. In cyber jargon, this is known as “phishing”, and criminals often succeed in obtaining the information they want. They can then use a false identity and take control of the victim’s bank accounts.

Evading prosecution

One of the main challenges is the disparities between national rules on cybercrime. Despite greater harmonization of various countries’ legislation in the field, significant differences remain on a global scale.

This makes it more difficult to crack down on criminal acts that are committed across national borders.

Ever greater numbers of criminals are moving their operations to countries where the laws are less stringent and where it is easier to evade prosecution. Cybercrime law is very weak, and more or less non-existent in countries such as the Philippines. Criminals can operate with impunity in such countries, because even if they are found out, they are not extradited to countries with stricter laws.

Legal measures to combat cybercrime

Legislation determines what actions are deemed cybercrimes, how such actions should be investigated and what penal measures should be taken. International conventions and other intergovernmental agreements are an important way of coordinating the various sets of rules. They are also essential to facilitating cooperation between the police and prosecuting authorities in different countries.

The most important international convention in this field is the Council of Europe’s Convention on Cybercrime, adopted in 2001. T
The Convention establishes a comprehensive set of rules for the formulation of national regulatory policies on cybercrime in relation to substantive and procedural law.

“But in today’s Internet age, the convention is now outdated, and its viability in relation to technological developments is constantly being questioned. There are also concerns about whether the convention is maintaining a suitable balance between the interest in combating cybercrime on the one hand and the protection of fundamental human rights and freedoms on the other. These questions are two examples of the issues that we will examine in the SIGNAL research project,” says Bygrave.