THEORY OF LAW AND COMPUTER CRIMES

TEORIA DO DIREITO E CRIMES INFORMÁTICOS

Agata C. Amato Mangiameli[1]
Universidade de Roma – Tor Vergata

Abstract
This paper aims investigate the general theory and the elements of the computer crimes as well it social engineering, because as technology advances, more and more people use it according to their needs.
Keywords
Computer crimes. Elements. Dogmatic.

Resumo
Este artigo visa investigar a teoria geral e os elementos dos crimes informáticos, bem como engenharia social, porque à medida que a tecnologia avança, mais e mais pessoas usam de acordo com suas necessidades.
Palavras-chave
Crimes Informáticos. Elementos. Dogmática.

Introduction

As technology advances, more and more people use it according to their personal inclinations and desires. Remedies and risks - security and cybercrime - seem to be connected, as they grow and feed each other. For example: post-password recognition systems use behavioral authentication. More exactly, they help identify invisible fingerprints - we also refer to them as e-Dna (Electronic Defined Natural Attributes). It has been said that an algorithm is capable of identifying hundreds of unique identifiers such as the speed with which a person types on the keyboard or the way he holds his smartphone. However, it seems that e-Dna also depends on the activity the individ-

[1] Professora Catedrática da Universidade de Roma – Tor Vergata

ual had carried out previously. It changes when the individual is under the influence of drugs or if he is at risk of infarction.
For this reason, post-password technology may have more far-reaching implications than mere computer security: e-Dna may be useful in preventing certain diseases. It could become an important tool in asserting and protecting human rights. On the other hand, e-Dna could help industries and governments to develop new and more effective espionage activities.
Moving from similar considerations, in this report I intend to present the main threats to digital security, analyzing the challenges that they pose for legal scholars as well as the personality of the cybercriminal.

1. A general theory of computer crimes.

Cybercrime has to do with a wide range of behaviors and unlawful uses of the new technologies. There are many different forms of computer crimes, depending on the techniques used as well as on the goals the offender intends to reach.
As a matter of fact, the so called 'computer crimes' are both illicit activities in which the computer is just a means for committing crimes, and activities where the computer is the object of an illegal conduct. Computer crimes can hence be broken down into two categories: crimes where electronic devices and programs are used as a mere means to other ends - harass, extort, blackmail, etc. - and those where electronic devices and programs are the real targets - as occurs, for example, in the case of spreading viruses and damaging computers.
A large number of other activities belong to the category of crimes - such as harassment, child molestation, extortion, blackmail, manipulation of financial markets, espionage, terrorism - which involve repeated interactions with

a chosen individual. Obviously, there are many different procedures. It can happen, for example, that the victim is contacted in a chat-room or a public forum. Generally, these activities are carried out without the use of complex programs.

The rich variety of computer crimes also includes crimes such as theft or manipulation of data, identity theft or bank fraud. It also includes the offenses having the following characteristics: the illicit activity is facilitated by the use of a malicious software - such as keyloggers, Trojan horses, viruses, etc. -; they take advantage of system vulnerabilities; the victim unknowingly downloads an infected file or he unknowingly connects to a hostile site.

1.1 The subjective element.

Concepts as intent and guilt, as well as manslaughter, are affected by the advent of the new media and of virtual reality. As a matter of fact, no one can be punished for an action or omission if he has not acted with awareness and will. Moreover, no one may be punished for an act envisaged by law as a crime if he did not act intentionally, except in cases of premeditated murder or manslaughter as expressly provided for by the law (Art. 42 Penal Code). The Penal Code thus distinguishes between crimes committed fraudulently and crimes that are "beyond intention". In the former case the crime is committed with intention, namely the harmful event or danger, which is the result of an action or omission, was expected and wanted by the perpetrator - manslaughter. The crime is "beyond intention" when the results of the action or omission are not exactly what the subject wanted or expected - therefore it occurs against their intention - the event was not wanted by the agent and is the result of negligence, imprudence or inexperience (Art. 43 PC).

However, it is complicated to determine subjective intent in cases of computer crimes. Traditional parameters do

not seem to be sufficient, especially if we consider that many sophisticated programs perfectly simulate reality. The confusion and overlapping of planes (virtual/real) could prompt in the user the belief that what he does - or writes - in cyberspace is not real and is not important. It is as if in cyberspace the law cannot be broken nor can people's rights and interests be damaged. In addition, highly sophisticated programs often operate in an unpredictable manner so that their effects may not be intentional and may go beyond the user's intentions.

In some cases, the individual does not seem to be aware of his conduct. This lack of awareness does not depend on the fact that some people - like traditional or revolutionary hackers - do not perceive the illegal value of their actions. It depends mainly on the fact that criminal law was late in regulating software and the Internet. It might be said that the digital era was born and flourished in - and maybe "because of" - a lack of legal rules.

Moreover, the motivation of an illegal conduct is taken into consideration by the judge when he has to establish the quantum of the penalty. He has to judge the reasons of the crime, the ability to commit it and the severity of the offense.

So judges have a particularly delicate task. For example, the hacker's ludic purposes could be considered in favor of the accused, hence a reduction of the penalty, or, on the contrary, it could be considered against him, hence an increase in the punishment. If he acted for important purposes, such as freedom or equality, he may be judged more leniently since the reasons for this type of conduct may be seen to have a moral or social value as considered in Art. 62 (1) Penal Code. On the other hand, the same considerations may induce the judge to issue a more severe sentence.

1.2 The legal asset.

The commodity most usually damaged by cybercrime is information. It may be the aim of the offender, or it could be merely the means enabling the criminal to achieve his real goals.

Information has specific characteristics and the measures adopted to protect information must take them into account. For example, let's consider the classical economic theory: it is based on the postulate that commodities are rare, on the irreversible nature of economic processes (such as consumption) and on the exclusive nature of the commodity (deprivation). All these characteristics do not concern information: it is never lost, nor can it be destroyed by using it.

Consider the intangible nature of software. Software is a non-rival good - we can give away a copy and we can still go on using our own. It is fully reproducible without incurring high costs. Furthermore, informatics knowledge is cumulative and modular: new components can be easily added to upgrade a previous version.

As a consequence, the general theory of criminal law has to deal with the peculiar characteristics of information.

At this point, it may be useful to refer to the concept of legal interest. This notion is the result of a longstanding debate in the literature and it embraces all those items (and / or interests) that are considered important for society, hence worthy of protection. It is a very broad category which includes physical integrity and honor, but also life, property, public faith, intellectual property, etc. All the latter are elements whose protection comes under the purview of penal law - when the offense or danger is severe - or to civil law - when the damage suffered by the victim is not very severe.

Among the typical aspects of legal interest there is, definitely, a certain *dynamism*, dictated by the need to accommodate new and ever changing social needs. With the ad-

vent of the so-called digital society, cybercrime - and, in particular, the items it endangers or compromises - deserves very special attention.
Thus, after an initial phase characterized by doctrinal debate, many European States have decided to equip themselves with specific criminal legislation in order to regulate dangerous behaviors, such as those related to the spread and use of the new technologies.

1.3 A (non)locus commissi delicti.
Deterritorialization is a typical dimension of cyberspace. As a matter of fact, the activities that are carried out inside the network can not be easily located. In other words: the network knows no boundaries, and even less so those which delimit legal systems.
And yet, the network could be a (non-) *locus commissi delicti* - that is why issues of jurisdiction and competence are of great importance. The non-territorial and communicative nature of the network is well expressed by its vocabulary with expressions taken from sea-faring activities such as "surfing the net" or "being aware of pirates".

2. Malware, Viruses and Worms.
In recent years, we have been witnessing a rapid evolution of dangerous programs - the so-called 'malware'. I'm referring to hardware and software capable of obtaining user data for advertising purposes or for commercial activities. These programs can damage or alter the operation of a computer in order to take control of it and operate against other computers. The list is not only particularly long, but it is constantly growing. Let us consider some examples.

Adware is a program that independently opens windows of the browser in order to promote merchandising and services. This program presents some risks. Some adware

can slow down your computer, others can change the html of the pages you are browsing, just to include links and advertisements. In addition, many types of adware communicate your browsing habits to remote servers, thus violating your privacy.

Backdoor is a program that allows unauthorized access into your system, even without knowing your username and password. This program may represent a means for gaining emergency access to the system. The 'backdoor' is often installed by the system operators in order to allow recovery of a forgotten password. However, it could also be used by a computer expert who intends to unlawfully access the system.

Dialer is a program which disconnects the computer from the usual provider and connects it to a premium-rate number. The method usually followed by criminals is the free offer of an item, such as logos or ringtones for your smartphone, songs and mp3, pornography and so on, provided that a certain program is installed. Hidden software is often a dialer.

Keylogger is a hardware or a software that is capable of recording every letter the user types on his keyboard - as, for example, passwords, his chat conversations or the addresses of the web sites he has been browsing. A keylogger hardware may be installed in the cable which links the keyboard to the PC, or it can be hidden inside the keyboard itself. Software keyloggers could be installed on a computer directly or via remote access. They can also be delivered by a Trojan horse or a worm.

Trojan horse is a seemingly harmless program that hides dangerous commands for the computer. Typically, a Trojan horse is used to send spam or steal personal data. In any case, it is a program which aims at taking control of a computer. It does not have the capacity of self-replication - so it requires the direct intervention of the aggressor in

order to be spread. It can be concealed in the operating system folders.
Virus is a program that can reproduce and spread itself, infecting files, networks, and other computers. A virus usually damages only the software of the computer, but it can also indirectly damage the hardware. Nowadays, their favorite vehicle of infection is represented by e-mails and peer-to-peer networks.
Worm is a software which modifies the host operating system, in order to replicate itself. The worm usually searches for the address book stored in a computer and sends a copy of itself as an attachment to all, or part, of the addresses it finds. Often, the criminal who sends worms, uses social engineering techniques to induce his target to open the attachment. Some worms exploit the flaws - bugs - of the system to run automatically when the user views his e-mail. Quite often, they serve as a tool for the automatic installation - on as many computers as possible - of another malware like the mentioned backdoors and keyloggers.

And again, Hijacker is a program that launches undesirable web pages, logic bombs that 'explodes' when the pc reaches a certain state or the user performs a certain action. They can change or delete files, lock the system, or delete the entire contents of a disk; Rabbit is a software which uses all of the computer's resources to create copies of itself at great speed; Scareware is a program that notifies non-existent problems prompting the user to install a malware pretending it is an anti-virus - as, for example, the known rogue anti-spyware; the Spyware program is designed to steal information such as the surfing habits, the passwords or cryptographic keys of a user; Zip Bomb is made up of files that, when opened, expand until they occupy about four petabytes in size, using up all the hard drive storage space.

The spread of such techniques and programs facilitate - and perhaps even encourage - criminal activities. Moreover, there is a black market linked to these programs. In addition, you can purchase or use sensitive data for personal purposes and without the knowledge of the legitimate owners, or even a certain amount of remotely controlled computers via Backdoor.
To quote former US financial adviser, Frank William Abagnale: *today it is much easier to do what I used to do during my youth. Technology helps crime!*

3. From cybersquatting to phishing: the main criminal conducts.

Just a few examples of activities which endanger the rights and safety of individuals, groups and nations.

Cyberlaundering: is a money laundering technique that takes any of many forms: the most classical form starts with the transfer of money obtained through illegal activities to 'clean' accounts. But recycling techniques in the digital era are extremely varied. For example, to clean up money and evade financial rules, some organizations use parallel banking systems. An illegal system that, in the Chinese case, has taken the name of *fei chien* (flying money).
Moreover, on the world's largest digital black market, named Silk Road 3.0 - which is not indexed by search engines and only accessible through Tor - you can purchase not only drugs, weapons, do-it-yourself kits for making bombs, etc., but you can also launder the proceeds from criminal activities. In fact, transactions do not occur in common currencies, but in Bit-Coins: an electronic currency that ensures on-line trading anonymity. It is no coincidence that Ross Ulbricht - the founder of Silk Road -

is currently on trial. He has been charged with several offences which include software piracy and money laundering. If his defense fails to prove that he abandoned the administration of the portal immediately after it was founded, he will have to face a sentence from a minimum of 20 years to life.
In Italy, the legal framework against money laundering is represented by Legislative Decree no 231 of 21.11.2007 and its implementing regulations issued by the Minister of the Economy and Finance.

Cybersquatting: Cybersquatters register web domains belonging to well-known trademarks or public personalities and hold them for ransom money. They may also register a web domain when it reaches its expiry date, which is usually one year from the date of purchase and require payment of a fee for renewal. For this purpose, cybersquatters have created programs that browse the net and examine web logs, looking for expiring domains.
In the United States, where such cases are not rare, cybersquatting is sanctioned by a law - The Anticybersquatting Consumer Protection Act approved by Congress in 1999 - which envisages heavy penalties for those who register web domains or trademarks with the mere intention of selling those domains back to the owner.
In Italy, domain names are subject to the regulations governing the right to names (as guaranteed by Articles 6, 7, 8 and 9 of the Civil Code), to the rules on trademarks and logos of the Civil Code (Section 2569 et seq.), and to the industrial property code. Referring to the Civil Code, this means that Tizio (Tom) can sue Caio (Dick) if the latter opens a website with the domain name tizio(tom).it, damaging the real Tizio (Tom). Regarding the regulation of trade marks and brands (Civil code and Industrial Property Code) domain names have their own distinctive value as

they also play a branding function as do other commercial signs and marks.

Defacing is an activity aimed at modifying the home page of a web site, or at changing one, several or all the internal pages. This is an act of vandalism by unauthorized crackers.
The reasons to deface a site are heterogeneous: the defacing may represent a kind of warning, pointing out the vulnerabilities of the site to the webmaster; it may be a funny joke or an indirect act of propaganda carried out in order to damage and disqualify rivals; blackmailing, namely, the threat to carry out repeated defacings or a fraud perpetrated by a cracker.
In Italy, defacing can be part of three types of crimes listed in the Penal Code, namely unauthorized access to a computer system (Art. 615 *ter*), digital damage (Art. 635 *bis*) and defamation (Art. 595).

Pharming is a technique that is often used to gain access to personal or confidential information. This technique relies on the fact that the address of a web page is automatically translated by the host into a numeric IP address. This type of attack may be addressed to the DNS server of the Internet Service provider or to the victim's PC. In the first case, the cracker changes the combination of the domain and its IP address. All the users who try to connect to that provider, type the right URL address, but are redirected to a dedicated server. In the second case, a cracker alters the computer system of the victim by using a software or by gaining direct access.
Pharming may supplement a computer fraud crime as stated by Art. 640 of the Penal Code which punishes an individual who, by altering in anyway the structure of an electronic system or by changing without authorization, in any way, the data, information or programs stored in a

computer, obtains unjust profit, for himself or for others to the detriment of a third party.

Phishing is a technique that aims at obtaining confidential information, by addressing the victims directly. For example, in an e-mail, seemingly signed by a lending institution, a user is asked to enter his personal information under the guise of a security check. By using this information, the offender enters the victim's account and, carries out various operations.
This criminal activity is based on the techniques called social engineering. In addition to random emails, phishing can also be carried out by telephone or by sending text messages.
Usually, the email asks the user to click on a link in the message to avoid a charge and/or to regularize his position with an institution or company.
Sometimes, the e-mail contains an offer of working opportunities, for example, positions as financial operator. By providing their bank details, users will receive a credit. This has a lot to do with recycling activities – cyberlaundering, money-laundering, is particularly important for phishers. By dispersing stolen money in many current accounts and spreading them in different countries, it becomes extremely difficult to discover the criminals' identities.
In Italy, the Milan Court - in its judgment of 10.12.2007 (confirmed by the Supreme Court in 2011) - condemned the members of a transnational organization dedicated to phishing; the judgment of 29.10.2008 sentenced for laundering all the individuals who, like a financial manager, had collected and re-transferred abroad the money of Italian holders.

Sniffing is the interception of data transiting in a network. It may have legitimate purposes as, for example, the analy-

sis of communication problems and/or the detection of intrusion attempts, but it can also have illicit purposes - such as fraudulent interception of passwords or other sensitive information.

Sniffers use different models depending on the network (ethernet-switched or not), and various techniques such as intercepting, storing, sorting and filtering data, etc. Moreover, sniffing creates privacy problems for users. On the other hand, it could be used to defend copyright. In this case, the sniffer accesses a computer or a network in order to fight against the spreading of copyright software, pictures and movies. This activity requires a mandate from the judicial authorities. It must be pointed out that in this kind of investigation, the data provided by the Internet Service Provider does not clearly identify the person who downloaded a file protected by copyright, but the person who pays the telephone bill. The difficulty in identifying the person who has physically committed the act, excludes the penal causal link with the copyright infringement. In any case, there is not sufficient evidence for criminal effects since criminal intelligence requires the unequivocal identification of the person and of his/her responsibilities.

Among the first sentences on this subject, it is worth mentioning the judgment of the Court of Rome - March 17, 2008 - regarding the Peppermint vs Techland case. As is known, the German record company and producer of Polish video games had asked a Swiss company specialized in intercepting peer-to-peer networks, to detect the Ip addresses of those who shared music files and games. The company obtained their names from the Italian providers in order to get compensation for the economic damages it suffered. The Court of Rome rejected the request to proceed, claiming that the company had no right to access the personal data of those who had been intercepted. Therefore, the collected names had no probative value, and could not be used in the judgment.

Spoofing is about sending a message which contains a request for help. The recipients of the message are usually friends and acquaintances of the victim whose identity has been stolen. The Spoofer finds their addresses in the mailing list of another user.

As already mentioned, digital identity theft was introduced by Law no. 119/2014, which amended Article 640 *ter* of the Penal Code, with the inclusion of a third paragraph that envisages the penalty of imprisonment from two to six years and a fine from € 600.00 to € 3,000.00 in case the offense was committed by means of theft or improper use of a digital identity.

There are different types of spoofing, but what they have in common is the fact that they trick the victim: the false information may refer to a MAC address, an IP address, and much more, including spoofing techniques to strike the protocols of the application, and web spoofing.

Being intuitive, this latter definition has to do with the web. It occurs when a user is persuaded to link up with a safe server rather than with the malicious one. The technique used is usually the following: the cracker builds a fake server (also called shadow server), which may contain a copy of the real server (pages are copied locally onto the shadow server), or he falsifies the association between the web address and the IP address.

In the case of Transport Layer Security - an encryption protocol used in the web to secure communication and exchange information between two network nodes (usually between client and server) - the so-called Pirates generate a fake server certificate, totally equal to the real one. When a user clicks for acceptance, the attacker connects him to the real server, acting as an intermediary and intercepts the communications.

DNS Spoofing is a cyberattack that allows a criminal to redirect a web domain name to an IP address other than the original one; *Eavesdropping* refers to listening activities (e-mail, instant messaging, etc.) without being authorized; *Man in the middle attack*, in which the attacker is able to read, enter or modify at his own will, messages between two users; *Spamming* is a very well known and widespread phenomenon that consists in indiscriminately sending unsolicited messages; *SQL injection* is the use of an abnormal query that - if not properly filtered - allows the attacker to gain administrative privileges, or to access the site without possessing the right credentials; *Tampering* is an alteration of activity and tampering of information, of programs and systems.

3.1 Crimes on the border between network and real life.

Cyber-bullying are acts of harassment, usually among minors on-line, such as sending messages, photos or videos, which are false, offensive and/or threatening.

Just like bullying in the real world, cyber-bullying may constitute a violation of the Civil Code, of the Penal Code and a violation of the Privacy Code. The motivations and purposes are the same as bullying in the real world: bullies target anyone they see as being different for their appearance, sexual orientation, language or conduct, etc. and they do so in order to isolate and exclude them from a specific social group.

Cyber-bullying is characterized by the anonymity of the harasser and by the difficulties that the victims have to face - mainly because they are exposed to the large number of people who have access to the forum or social network. Moreover, there is a structural ethical aspect that needs to be emphasized: when you are on the Internet you can pretend you are someone else. On the Internet you can say and do things you would not normally say or do in

real life. The victims are exposed at all times and everywhere because of the absence of space and time which characterize the digital world. The cyber bully can send violent, vulgar online messages, they can start and fuel verbal battles in a forum (flaming), or denigrate and marginalize someone from an online group, or simply instill fear. The cyber-bully can also glean information from the friends or family members of the victim by gaining their trust and then publish and share the confidential information they have received.

Beyond all the different techniques and purposes, cyberbullying normally involves pre-teens and teens. A research by the "teenagers Observatory" - presented by Telefono Azzurro and DoxaKids in November 2014, conducted on over 1,500 students of Italian schools aged between 11 and 19 years - states that cyber-bullying is a phenomenon that is well known to teenagers, given that 80.3% of respondents have heard about it, 2 out of 3 know someone who has been a victim, one out of 10 was the victim of an act of violence (10.8% of respondents; 9.1% boys and 12.6% girls). The same research also showed that children who have been victims of online harassment incur relationship failures more frequently than those who have not been harassed.

Cyber-stalking is the use of the new technological means with the intention of laying siege, defame, stalk, threaten, oppress, harass a person or a group of persons.

Just like 'real' stalking, cyber-stalking consists in a continuous series of actions that invade the personal, social and professional life of the victim. Moreover, it is the obsessive, constant repetition of these acts that characterizes stalking and cyber-stalking. That is why the chosen victim feels like she/he is always at risk.

As occurs in case of stalking, the cyber-stalker often tries to defame his victim. Thus, for example, he publishes false

information, creates web pages or blogs in order to damage his/her reputation; he spreads disparaging statements in news groups, chat rooms, forums, social networks, etc.; he makes false and disparaging statements on public pages - such as wikipedia and in other similar places. While defaming, he penetrates the cyber environment of the victim, collecting information and prompting other users to join in the activity of stalking his chosen victim.

Both, stalkers and cyber-stalkers, claim - beyond all evidence - that they were provoked by the victim. On the other hand, they try in every way to meet and / or establish a relationship of complicity with the victim. As a matter of fact, cyber-stalkers use all the new tools and programs available in the digital arena. They can spread computer viruses, abort their victim's connections, eliminate or suspend his/her profile, provoke material and moral damage or intercept the communications between the victim and his/her friends. And again, cyber-stalkers can use the data of the victim to make online purchases on his/her behalf. They may also use the data of the victim to activate spamming services.

Sometimes, cyber-stalkers meet their needs by simply writing on online forums, chat rooms, etc. They spread slanderous information about their victim or victims in order to establish a relationship, or better in order to transform a virtual relationship into a real one. Considering the contents of the messages, given the style of the actions and the conditions of the victim, it might be said that cyber-stalkers develop a conduct that is similar to all forms of non-consensual relationship - such as, for example, rape. Indeed, cyber-stalkers often seek to cross the line between virtual to real life. The harasser discovers the places frequented by his victim and follows him/her. Consequences can be easily understood. This explains also why, in many jurisdictions, stalking, whatever its form, is prosecuted and

punished as a form of violence, usually perpetrated by men against women.
In this connection, it should be remembered that Article 612 bis of the Italian Penal Code, in the event of repeated threats and harassment which may cause a continuing and serious state of anxiety and fear in the victim, such as to force her to change her life habits, provides that the penalty be increased if the offense is committed by a spouse - even if separated or divorced - or a person who is, or has been, involved in an emotional relationship with the victim. The penalty is also increased if the act is committed through computers or electronic tools.
The reasons for this punishment lies in the fact that not only the is the Internet - in its own right – 'real life' - but it is also a (non-) place in which aggression, insult, mockery, and / or their incitement, can become gradually more and more pervasive - and for this reason even more violent. It should be added that in real life you can get a warning or an expulsion order from public places. While in (non-)virtual places this becomes more difficult and, not infrequently, even impossible.

Cyber-terrorism is the use that terrorist organizations make of the Internet, mostly for propaganda and recruitment purposes. In fact, terrorist groups use the Internet to denigrate and delegitimize the policy of States, as well as spread fear. At the same time, they promise their franchisees eternal rewards.
Perhaps, cyber-terrorists are more interested in the social and political effects of their intrusions and threats, rather than in attacking the digital infrastructure. Yet cyber-terrorism is becoming very common, as evidenced by some recent episodes. False affiliates of the caliphate of Abu Bakr al Baghdadi entered the Twitter profile of the American daily Albuquerque Journal, posting a threatening message: "We are already here, in your PCs and in

your homes". Even the homepage of Malaysia Airlines was violated posting the message: "404 - Plane Not Found. Isis will win". Not to mention the attack against the Twitter and Facebook accounts of the Central Command of US troops in Tampa - in that case, terrorists wrote messages like "the Islamic State is chasing you" or "watch your back".
In such cases - just as in the intrusion of the so-called Cyber Caliphate in the Twitter account of Central Command of the US Department of Defense - what actually matters is that terrorists use the Internet to spread fear, they know how to knock out the critical structures or processes which ensure national security.

Cyber-spying, or cyber-espionage is a set of activities that exploit the network in favor of one or more governments, to ensure their economic and/or strategic superiority over another person, organization or State.
As one might expect, governmental activities in this field are particularly intense and developed, also for the large amount of information that can be - and indeed is - collected by computer systems. In the United States the amount of data collected by the computer network is increasing and is currently equal to 2 petabytes per hour, almost 2.1 million gigabytes (the equivalent of hundreds of millions of pages of text).

Cyber-warfare is the set of military activities and operations connected to keyword 'information'. This means that the States are trying to gain information on their front, and, at the same time, they art trying to change and destroy the communication systems of their enemy. This kind of war is often fought by systematically dismantling the opponent's critical barriers or by disrupting and deactivating his strategic communications networks. It goes without saying that these activities are hard to trace - ex-

cept through appropriate protective shields. That is what they constitute the best way to wage war.
Just one example among many is Flame (and more exactly Worm.Win32.Flame) which is a particularly advanced program capable of illicitly obtaining a wide array of data - the content displayed on the screen and the information systems, files of contacts and audio conversations. This malware is so complex and sophisticated that it remained undetected for over two years. It seems that the creation of this malware happened totally by chance while security experts were working on the identification of another malicious program, called Wiper. It has been said that Flame - a digital weapon capable of performing targeted attacks in several countries and that has the ability to reproduce on a local network using different methods - was created in 2012 by the United States and Israel, and has been used against Iran.

3.2 Social Engineering

With increasing frequency, hackers and crackers use social engineering techniques. That is to say they analyze individual behavior in order to steal information.
This increase is related to the evolution of software itself: the more computer systems are free from errors (bugs), the more it becomes difficult, if not impossible, to attack their defenses technologically. The so-called social engineer, whose essential arts - in the words of Kevin Mitnick - are deception, and intrusion, is an expert liar in the first phase, called footprinting, when he gathers all the information he needs for the real attack. He then verifies information and only when this is done does he launch the attack.
Unlike other computer crimes, social engineering is based on apparently simple methods that are clearly described on multiple sites. One such method, for example, is neuro-linguistic programming. This technique is used for

therapeutic purposes but it can be used to manipulate people.

In any case, there are no doubts that in the case of fraud - also computer fraud - the mental patterns of the victims are very important. The social engineer takes into account the victim's needs, fears and emotions that are the basis of communication and of interpersonal relationships. The trust we place in others may be motivated by the respect we have towards authority - we have confidence in the police, in doctors, etc., it may depend on social pressure; on the attention we pay when judging others, or on our deep feelings and desires. So the social engineer takes advantage of the victim's good faith and/or ignorance, inventing a credible story and requesting an immediate reaction. It does not take much to prepare a social engineering attack: all that is required is knowledge of the characteristic traits of human behavior and some information published by the victim on Facebook, Twitter, Foursquare, or simply a wish list on Amazon!

4. Some final consideration

Sometimes hackers are animated by a creative spirit, they do what they do out of curiosity or for the sake of playing. Other times, the aims pursued are not legal. In this case, it would be more appropriate to define them 'crackers'. It is clear that the boundary between these figures is not always clear. Not surprisingly, common language frequently confuses these two terms, and more or less consciously proposes an incorrect analogy between hackers and criminals.

As a matter of fact, hacking indicates the set of techniques that are used to break through the defensive barriers of a hardware or software system. Normally, it is a legal activity. Not infrequently it is carried out by people who professionally manage computer systems.

For example, this activity may be aimed involve at increasing the performance of the hardware. Similarly, hacking activities may include adding functions to a program.
In other cases, the set of techniques and hacking operations can be are adopted as a defensive measure to ward off attacks by pirates.
The positive meaning of the term hacker derives from the particular culture described by Levy in the 80's in the book *Hackers. The heroes of the computer revolution*. In that book he wrote that the hacker culture was based on five key principles: sharing, openness, decentralization, free access to information technologies and progress of humanity. It is no coincidence that modern hackers - among them, Richard Stallman - are staunch supporters of free software and open source as against proprietary software.

As we can read in the Hacker Manifesto written in 1986 by Loyd Blankenship:

"This is our world now [...] the world of the electron and the switch, the beauty of the gang. We run a service that already exists [...] run by greedy gluttons, and you call us criminals. We explore [...] and you call us criminals. We seek after knowledge [...] and you call us criminals. We exist without skin color, without nationality, without religious bias [...] and you call us criminals. You build atomic bombs, you provoke wars, you murder, cheat, and lie and try to make us believe it's for our own good, yet we're the criminals. Yes, I'm a criminal. My crime is that of curiosity. My crime is to judge people by what they say and think, not for their appearance. My crime was pointing out your errors and weakness, that's why I will never be forgiven. I am a hacker, and this is my manifesto. You may stop this individual, but you can not stop us all [...] After all, we are all equal"

On the other hand, digital criminals can be involved in many different activities. For example, they try to bypass the purchase of licenses or to access other user's systems in order to steal confidential data or damage them. If they alter the structure of a program, this phenomenon is called cracking. It is cracking whenever the author acts in violation of technological protection measures (DRM) that have been developed by the manufacturer of the program. Other cracking activities consist in gaining access to the public communications network or using it without being accredited, as well as the unauthorized use of a computer network.

Not infrequently, crackers use reverse engineering namely, a technique whereby you can understand the structure of a software analyzing the answers it provides to given inputs. This process is usually used to create and distribute material, mainly software, for copyright infringement.

And that's not all! In the midst of violations and looting - including cheating and damage - crackers form teams (the so-called 'cracking crews') and challenge each other, very often driven by the prospect of financial gain, or by the need to be approved within a specific group of crackers.

Finally, many studies have shown that the cyber-criminal has a medium-high education, large capacity of intent, organization and programming. He can access secure computer networks, and in particular, he is able to access a system and adapt it to his needs. His computer skills are very advanced, but often accompanied by a reduced perception of the illegal character of his conduct.

As a matter of fact, the network has blurred the line between professional criminals and 'normal people'. In many cases, a computer crime is committed by individuals who before the digital revolution would never have committed a crime - or at least, by people who were included in the category of the so-called 'unsuspected' individuals. Considering this same issue from another perspective, we can

however say that cyber-criminals play in a thug 'first league'. Generally, cyber-criminals work in solitude, and while they spread their malware – like Evgeniy Bogachev, magician of botnets - they increase their confidence in playing a game that they consider not only exciting, but also extremely profitable.

This is why the suppression of cybercrime has required, and still requires, a specialization of the judicial police. Police must now take into account the profound changes in human relationships and habits provoked by the digital era. For example, nowadays a *crime scene* can also be a web site or a computer; the attenuation in the perception of crime caused by the replacement of the old face-to-face with the new interface; the inclusion in the criminal category of people who, before the information revolution, were completely strangers to the world of criminals.

The foregoing considerations are of particular importance for the so called psychological elements - subjective elements - of a criminal conduct. According to Italian law: intent, guilt and beyond the intention.

The fact of acting from a considerable distance, makes the victim invisible, incorporeal, just like everything else in cyberspace. And all this facilitates the agent - who does not immediately see the effects of his conduct. Similarly, the fact of living in a virtual reality induces the criminal to be bolder and more decisive. In both cases, we wonder whether all of these aspects should be assessed during the investigation of guilt, and, in any case, to what extent and how it should be evaluated.

It should also be considered that an individual usually commits a crime after using a computer for mere entertainment purposes. Indeed, he often reproduces objectives and the dynamics of a game. It is no coincidence that in this field youth crime is widespread. Moreover, videogames were one of the channels for the dissemination of this kind of knowledge. As occurs with videogames,

> sometimes users develop a psychological addiction, such as the Internet Addiction Disorder Related Psychopathology. All these elements can be important for the rules that establish who is to be considered less responsible, for example for psychic immaturity (minors: Articles. 97 and 98 PC); for mental disorders (arts. 88 and 89 of the Penal Code). Or for the fact that they acted under the negative effects of drugs and alcohol (arts. 91 et seq. cp). In this latter case, if the individual has been voluntary taking drugs his punishment will be more severe. The latter reference is not a coincidence, because nowadays we often speak of 'abuse' and 'detoxification' from the Internet, or even of e-LSD and drug-apps.

Finally, a specific form of protest and struggle characterize the activity of the group that goes under the name of Anonymous. The members of this group are usually recruited from chat-rooms and forums. They coordinate and act in order to achieve concrete political goals. Or to avenge the violation of human rights. For example, the first action of Anonymus was carried out against the social network Habbo Hotel following the news that in Alabama a minor affected by AIDS was not allowed to use the swimming pool of a playground. Even more, let's think of their current stance against Isis. Anonymous has targeted thousands of Twitter accounts, Facebook and Instagram, intercepting as many e-mails and blocking hundreds of jihadist propaganda sites.