Prospective Analysis on Trends in Cybercrime from 2011 to 2020

PREFACE

Those who attempt to predict the future run the risk of being wrong. But those who overlook the importance of conducting a prospective analysis adopt a passive attitude that weakens them against the dictatorship of events. Anticipating societal changes prepares us to weather the storm.

The pioneers of the Internet, including the recently deceased Paul Baran, certainly never imagined that the Internet would connect more than two billion subscribers half a century later.

Who could have predicted it? The boom in digital technology is changing the foundation of our society. Who would have imagined its impact on telecommunications, social relationships, the economy, industrial processes, home automation, politics, and countless other areas?

Some compare the digital revolution to Gutenberg's invention of the printing press. Surely, the change has even greater magnitude, because it touches all human activities. Each and every day, we bear witness to a true reconfiguration that affects individuals, businesses, and institutions.

Cyberspace is a place of freedom, creativity, and growth, with "exponential" prospects. It is a chance for humanity. Yet all progress has its downside. The perverse effects manifest themselves as well, as predators immediately exploit vulnerabilities in order to gain profits, destroying or neutralising anything that stands in the way of expanding their criminal enterprise.

Cyberspace promises opportunities, but it is also grounds for power and conflict. It's war!

We can imagine a future based on certainty. Cyberspace will link more and more people together, in developed countries and even more so in emerging countries, particularly China. This expansion can also be seen in third-world countries, which now have access to new technologies, by making a quantum leap that blurs stinging differences.

New technologies will also enrich daily life down to the finest detail. That is another certainty. The notion of power will have to be examined in a new light, and the expression of democracy will break free from the schedule of electoral consultations. Public and private institutions will have to adapt to this new citizens and consumers behaviour. Organizational methods will shift toward a more complex matrix system.

Those in charge must identify the things that will remain the same and also detect potential breakthroughs in changing technologies. Hence the importance of scientific monitoring.

The future also depends on uncertainties. Will countries, whose legitimacy resides primarily in defence and security, be able to maintain such a monopoly when faced with multiple daily threats or attacks that may come without warning and from various sources?

Will international cooperation be able to overcome the contradiction between an inherent globalization of networks and the maintenance of political, legal and military borders?

Can the measures that need to be taken for defence and security receive funding during the prolonged economic crisis, measures that are needed to supplement – not replace – those that are already needed in order to guarantee peace in the air and at sea? Will "*black*" countries, mafias, criminal organizations, and terrorist movements reap the benefits of free actions and resources that may be lacking among those who seek to prevent their empire from growing?

Building awareness is paramount if we want to avoid chaos. Governments are committed to this today with resolution. France's recent creation of the Agence Nationale de Sécurité des

Systèmes d'Information (ANSSI) is the visible and highly symbolic representation of a proactive policy that requires discretion so as not to reveal all of its components.

Businesses are also steadily moving forward, knowing that their human, tangible, and intangible potential could be affected or destroyed if they are not vigilant.

But awareness must also be shared among all citizens. This is why we need instruction to be integrated very quickly into our schools and university programs, sowing the seeds today in order to reap the benefits tomorrow.

Beyond this, the key question among forecasters relates to the role of us humans in cyberspace. What lies at stake is the preservation of our identity, our image rights, our privacy, our freedom of opinion, and our access to unbiased information. Humanity must prevail over cyberspace, not become enslaved to it particularly through the intrusiveness and traceability of digital technologies.

As the product of twenty two experts, this prospective analysis on trends in cybercrime is the culmination of different experiences.

It deserves a great deal of credit for highlighting the human dimension of issues involved in "*21st century crime*".

This seminal work provides solid answers to today's questions, without which tomorrow would have no future.

General of the Army Marc WATIN-AUGOUARD
General inspector of the Armies – Gendarmerie

FOREWORD

Cybercrime is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately.

At the end of the 2010 International Forum on Cybercrime (FIC 2010), event organizers officially endorsed the plan presented by Daniel GUINIER to reiterate a prospective study on cybercrime led by Philippe ROSÉ in 1991[1]. The result of this group discussion for the next decade was to be presented as part of FIC 2011, which was since cancelled.

This prospective study on the next decade brought together a panel of experts from the public and private sectors. The approach chosen is based on the Delphi method, an iterative process of discussion based on a questionnaire developed by a scientific committee, with interim summaries drawn up by an *ad hoc* committee. The paperless discussion method was effective while allowing participant responses to remain anonymous, which also levelled the playing field. The 22 experts who contributed to this study underwent three rounds of individual interviews, allowing them to express their opinions and reformulate their responses in comparison against the results of the group discussions. Without excluding the possibility of a major technological breakthrough, the combination of their analyses, along with their respective professional experience, made it possible to identify their differing opinions while maintaining the rich contribution of their individual expertise and to spot typical criminal trends of the 21st century. The delicate maturity process has taken one year[2] before presenting the results in the form of this summary.

The result of this work is not an end in itself, but rather a tool to encourage discussion among policy makers, business leaders, and representatives of civil society regarding their strategies to be implemented in order to maintain the best possible control in a digital world without borders.

This prospective study[3] being published is the reward for these experts who made a personal contribution to the development of a collective vision.

The appendix provides detailed information on the method, the list of those who participated in the study, and the questionnaire that was submitted to them.

[1] Rosé P. (1992) on Computer crime by 2005, and Guinier D. (1995) on the development of criminology focusing on Information Technology.

[2] From the presentation of the project to FIC organizers in April 2010 until March 2011.

[3] **Copyright Notice:** Being a collective work distributed at the initiative of the French National Gendarmerie, it is understood that the readers and producers of this work, *including identified committee members and consulted experts*, are allowed to use parts of it, provided that they fully cite the source: *"Prospective Analysis on Trends in Cybercrime from 2011 to 2020"*, © 2011 National Gendarmerie. However, any publication of this work must be expressly approved by the National Gendarmerie, as the beneficiary of all ownership rights, like the "*Guide pratique du chef d'entreprise face au risque numérique*" (A practical guide to digital risk for business leaders), whose second version dated 31 March 2010 was presented at FIC 2010 in Lille, France.

TABLE OF CONTENTS

INTRODUCTION

Definition and Aspects of Cybercrime

This section presents the results of defining the term "cybercrime" in light of the various paths it is expected by experts to take during the decade from 2011 to 2020[4].

Etymologically, *"cybercrime"* combines the term *"crime"* with the root *"cyber"* from the word *"cybernetic"*, from the Greek, "*kubernân*", which means to lead or govern. The *"cyber"* environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "*computer crime*" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity.

Criminal Aspect of Cybercrime

From a criminal dimension**,** some experts say that there is no need to change or redefine this term, but rather a need to clarify what it encompasses, using the Council of Europe's **Convention on Cybercrime**[5]. They emphasise the coexistence of common law offenses from the real world with other offenses that are more related to the virtual world or even more specific, *such as online identity theft*. The proportions of the various types of offenses committed or seen in light of public sensitivities are subject to change. The next ten years will certainly bring the development of **the financial aspect** – *including money laundering, despite it already being easy to circumvent the traditional banking system using the Internet* – **involving organized crime groups**, often on an international level, and the importance of keeping personal data secure.

Others, however, prefer the term *"**digital technology crime**"*, which includes offenses and lawsuits that involve digital technology. Others still point out that **the term *"cybercrime"* rather oversimplifies matters**, given the distribution of damage caused, mainly related to causes outside of computing, and the various procedures involved, far beyond what is covered by Art. 323 of the French Criminal Code (Code penal), which now includes content, services, and infrastructures.

Technological Aspect of Cybercrime

From a technological dimension, other experts point out **the need for a comprehensive term, such as *"electronic crime"* or *"e-crime"***, thanks to the convergence of ICT[6], including mobile technology, telephony, memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included[7].

[4] According to question Q01: How would you redefine or clarify the areas of illegal activities and redefine the term *"cybercrime"* for the next decade?

[5] Also known as: "Budapest Convention on Cybercrime of 21 November 2011".

[6] Information and Communication Technologies.

[7] Simply using one or other means of communication is not enough to qualify a criminal act. As an example, a phishing message qualifies as cybercrime because the message itself contains the proof of using a fake name or characteristic within the definition of fraud. However, an appointment

Anthropological Aspect of Cybercrime

From an anthropological aspect, cybercrime originates from various populations and exhibits socio-educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. The maladjustment of the education system may contribute to the development of new forms of cybercrime or deviant practices and behaviour with various levels of severity, including cheating and reputational damage, which can be related to frustrations and the redefinition of material and citizen values, inconsistent with what is expected when approaching and leading an adult life. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including *theft, child pornography, and calls for uprisings, violence, and hatred*. With regard to techno-ideological factors, one must consider sites and networks aimed at propaganda, destabilisation, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

Strategic Aspect of Cybercrime

From a strategic aspect, cybercrime is seen as an offense to cyber-security, namely attacks to digital networks for the purpose of seizing control, paralysing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

Amplification and Diversification of Cybercrime

Experts agree that **illegal or criminal activities are expanding and will continue to expand**. The definitions of acts and processes of conducting them are already and will be modified by the use of ICT in various usual and innovative areas, including *financial transactions, privacy, identity theft, reputational damage, damage to critical systems, terrorism*, and more. **Emerging issues** call for the classification of offenses with regard to new and future technologies, as well as an understanding of the motivations driving those behind such crimes. They will have to take into account the relays involving **poorly structured, yet well-orchestrated social networks**, the presence of more or less discrete **highly-structured organizations** acting at an international level, and the extent of the consequences, in view of terrorism, information warfare, and cyber warfare that would affect strategic socio-economic systems and infrastructures, with risks of major outages and the unavailability of entire networks and systems.

References:

CE (2001): Convention on Cybercrime (STE no. 181), Budapest, 23/11/01, Council of Europe.

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France). Édition 2010.

FIC2010 (2010): Guide pratique du chef d'entreprise face au risque numérique version 2010: risques identifiés et solutions proposées en 13 fiches, recommandations (A practical guide to digital risk for business leaders, 2010 edition: Thirteen identified risks and proposed solutions), 90 pages.

Filiol E., Richard P. (2006) Cybercriminalité (Cybercrime). Enquête sur les mafias qui envahissent le Web (Survey on mafia groups invading the Web), Dunod, 212 pages.

made over a landline or mobile phone to carry out an illegal sale does not contain the proof that a direct offense was committed, but evidence of a meeting during which such an offense could be committed.

[10] According to question Q02: What place will cybercrime have and how will it be related to other forms of crimes and offenses, including *counterfeiting, financial and economic crimes, child pornography, drug trafficking, human trafficking, terrorism, and other crimes?*

Guinier D. (1995): Développement d'une criminalité spécifique liée aux technologies de l'information – *en rapport avec l'informatique, les réseaux et les autoroutes électroniques* (Development of targeted crime related to information technology – *including computers, networks, and information superhighways*). Proc. 7th CITSS Symposium, Ottawa, pp. 21-45.
Krone, T., 2005. *High Tech Crime Brief.* Australian Institute of Criminology. Canberra, Australia. ISSN 1832-3413. 2005.
Quéméner M. (2008): Cybermenaces, entreprises et internautes (Cyberthreats: businesses and users). Economica, 264 pages.
Quéméner M. Yves Charpenel (2010): Cybercriminalité, droit pénal appliqué (Cybercrime: applied criminal law), Economica, 273 pages.
PWC, Coopers (2009): IT Governance Global Status Report.
Rosé P. (1992): La criminalité informatique à l'horizon 2005 – Analyse prospective (Computer crime by 2005 – Prospective analysis). IHESI and Harmattan, 165 pages.
Tisserand I. (2000): Nouvelles populations, nouvelles addictions: l'exemple des hackers (New populations, new addictions: hackers), Annales de médecine interne (Annals of internal medicine), Masson, vol. 151, pp. B49-B52.
Tisserand I. (2002): Hacking à cœur: les enfants du numérique (Born to hack: the digital generation), e-dite, Paris, 136 pages

http://blog.crimenumerique.fr/2008/10/30/faire-face-nouveaux-defis-delinquance-numerique
http://europa.eu/scadplus/leg/fr/lvb/114560.htm
http://ftp.jrc.es/EURdoc/JRC58484.pdf
http://lesrapports.ladocumentationfrancaise.fr/BRP/044000076/0000.pdf
http://re.jrc.ec.europa.eu/refsys/pdf/Snapshots_EUR_2010i.pdf
www.aucc.ca/publications/media/2010/banting_postdocs_07_06_f.html
www.ccl-cca.ca/CCL/Reports/LessonsInLearning/LinL20100707AcademicDishonesty-2.html
www.cio-online.com/contributions/lire-le-traitement-des-risques-humains-en-milieux-professionnels-strategiques-logique-ou-modernite-en-ssi-101.html
www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_aseger_247cp.pdf
www.eea.europa.eu/publications/the-territorial-dimension-of-environmental-sustainability/at_download/file
www.enisa.europa.eu/about-enisa/activities/programmes-reports/general-report-2009
www.fedpol.admin.ch/content/dam/data/kriminalitaet/diverse_berichte/cybercrime_sab_200110f.pdf
www.huyghe.fr/dyndoc_actu/495a33359efe6.pdf
www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite
www.nap.edu/openbook.php?record_id=1581&page=283
www.operationspaix.net/sites/politiquessociales.net/IMG/pdf/CP_suivi_tableau_de_bord_pauvrete.pdf
www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved Report_16Oct2009.pdf
www.voltage.com/pdf/Voltage-Data-Breach-Incident-Analysis.pdf

Cybercrime’s Place

This covers the place of cybercrime and how it will relate to other forms of crime during the 2011 to 2020 decade[10]*.*

Expansion and Growth of Cybercrime

Given that modern technology has radically changed how we live, traditional crimes and offenses will rely on this by **crossing criminal borders**. Digital networks indeed make it easier to commit such acts, with a number of added benefits, including *discretion, anonymity, fewer offenses, an international character, and the fleeting nature of evidence*.

Cybercrime’s place is growing due to the exponential development of connections, increased subject knowledge, cultural awareness, and programmable onboard electronics, which increase the number of potential targets. Compared to other crimes and offenses, it generally requires a smaller investment and can be carried out in various locations, without any geographical constraints, with no consideration to borders.

Predominance of Cybercrime

Everyone agrees that **cybercrime will hold a prominent place and cover the spectrum of conventional crime**. The argument is based on common points and connections between cybercrime and conventional forms of crime, and on examples provided by ICT and Internet which show the potential impact. Due to its accessibility, the appearance of impunity, and its potential, the Internet and ICT make some crimes and offenses easier to commit, including *counterfeiting, economic crimes, money laundering, child pornography, sexual exploitation, drug trafficking, human trafficking, terrorism, fraud, and other crimes*. These forms, particularly financial and economic organized crime and money laundering, will undoubtedly become more involved in *"cybercrime"*.

Terrorism could also benefit from the fragility of some systems and infrastructures, including *airports, air traffic control, transportation, financial transaction, power distribution and stations, data centres, and surveillance centres*, developing new methods of attack with significant impact. We should expect to see the arrival of a generation of individuals who are skilled in computer technology and communication, wanting to influence the world from the comfort of their computer screen. The ability to fully or partially operate remotely and with impunity will be a powerful incentive to act.

New risks will emerge, with the development of bioinformatics and bio-electronic implants that can be embedded into the human body, vastly expanding the realm of possible attacks, especially those that can be carried out remotely[11]. Developments in home automation and communication devices will also open gateways for cybercriminals to breach our privacy.

Subtleties of Cybercrime

For some, **cybercrime will dominate** since most criminal financial gain will be carried out on networks, using increasingly complex schemes and hard-to-dismantle money laundering systems, taking advantage of legal complexities between countries and the lack of defence mechanisms in place. Some experts already believe that cybercrime has become dominant. In 2009, for the first time ever, fraudulent money transfers exceeded physical theft in bank branches in the United States.

[11] Such as changing the settings on pacemakers or other vital implants.

For others, **cybercrime will remain behind** financial and economic crime in all its forms. However, the economic impact of cybercrime remains difficult to estimate, even more so in comparison to economic crime and drug trafficking.

References:

Guidère M. (2010): Les nouveaux terroristes (The new terrorists), Editions Autrement, 156 pages.

http://forms.cybersource.com/forms/FraudReport2010NAANETwww2010
http://krebsonsecurity.com/2010/03/page/3/
www.globalsecuritymag.fr/Vigil-nce-Pacemaker-multiples,20091109,13745.html
www.interieur.gouv.fr/sections/a_votre_service/statistiques/criminalite/2009
www.mcafee.com/us/local_content/white_papers/cybercrime_20100315_en.pdf

Overall Impact of Cybercrime

This section presents the results concerning the overall impact of technological change and breakthroughs of dominance – or rather, of the increase – of cybercrime during the 2011 to 2020 decade[12]*.*

Perception of the Overall Impact of Cybercrime

The overall impact of cybercrime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap between lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. However, its use can be described as negative or positive.

This is especially true in cryptography, used for securing transactions and data interchange as well as to secure communications covering illegal activities and the establishment of evidence. History shows that new technologies, rarely regulated and not fully complete, are both used for good and bad.

The next ten years will be marked by mobility, with the need for availability, real-time communication, connectivity, and a dependence on digital identity equipment and risk. This decade will also include monitoring automata systems and increasingly new risks.

Negative Developments with regard to Cybercrime

Expected developments, which may have a negative impact on cybercrime, render little distinction between work life and private life, using for example the difficulty of locating information for a company and Web applications with cloud computing, targeted stealth malware, and more generally, the massive use of new technologies, including mobile and wireless technologies, and a careless exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past.

We must emphasise **the volatile nature of finding data as evidence and the difficulty of reporting offenses** to the sources, with no legal means, because cybercriminals are adapting alongside new technologies.

[12] According to question Q03: What will be the overall impact of technological changes and breakthroughs, including *cloud computing, virtual systems, mobile systems, cryptology, steganography, and malware, on the control – or rather on the rise – of this phenomenon*?

In general, the anonymity of the Internet and the global breadth and depth of networks support the impunity of the criminals, and cloud computing will make it even more difficult to look for and record evidence. Criminal groups also have the financial means to acquire R&D services to develop tools to use in their attacks or to commission criminal acts or criminals themselves, leading to a form of professionalism.

Positive Developments with regard to Cybercrime

In contrast, **security measures based on these same technologies could have a positive impact.** Security is central to the problem and must be based on policies and be strictly enforced. It will be a major challenge with cloud computing, due to the complexity of where data is stored and the numerous jurisdictions involved, major risks associated with governance and territoriality. The effective level of quality security will be a key factor in the acceptance of these new services.

References:

Guinier D. (2010): L'informatique dématérialisée en nuages – *Ontologie et sécurité du "cloud computing"* (Cloud computing – *Ontology and security of cloud computing*). *Expertises,* no. 351, October, pp. 335-344.

www.gartner.com/it/page.jsp?id=1422314
www.klb-group.com/fr/upload/larticle_du_mois/liens/cost_killing__mai_2010.pdf

1. THREATS

1.1. Emerging Threats: Expected Targets and Forms

This section presents the study results regarding emerging threats and expected new forms of cybercrime, along with their level of sophistication, during the 2011 to 2020 decade[13].

Expected Targets

Emerging threats include not only online transactions and applications – *including nowadays gambling and betting* – but also industrial control systems, robotics, home automation, and onboard systems, with the development of Internet connectivity and the increasingly strong dependence on digital devices. SCADA[14] systems for remote monitoring, remote control, real-time remote technical management, and satellite systems may be targeted in particular. On-demand cloud computing services will further promote malware targeting users.

New threats are likely to target technologies that are not necessarily state-of-the-art, but rather technologies that are currently or soon-to-be deployed on a larger scale. To reduce the financial impact of such technologies, installation times are shorter, and so too is the time devoted to providing security. Therefore, attacks that were once possible but not carried out due to a lack of financial interest will become more lucrative due to their mass impact. An example of this are premium telephone numbers and telephone switchboard fraud[15]. Such an operation, however, is sophisticated only in its setup, which requires many calls to be generated to one or more countries and an adequate structure in a tax haven to deposit the resulting profits[16].

There will also be attacks conducted against critical infrastructures and strategic financial, socio-economic, and other services, using of vulnerable relays or active groups in order to disrupt and paralyse systems, blacking out communications or power grids, especially at times of conflict.

Expected Forms

All technical innovations are open to attack, since products often come with design or operating bugs, **and new products often experience** "**feature creep**", which also becomes a source of potential malware. Changes in social networks, along with an increasing interest among users in electronic communication, will certainly generate threats against individuals, businesses, public organizations, and governments. Possibilities for blackmail and extortion[17] directed at businesses and governments could use such networks to discredit, *such as by combining the potential of WikiLeaks and Facebook.* The decade will certainly be an increase

[13] According to question Q11: What are the emerging threats and the new expected forms of cybercrime, along with their level of sophistication?

[14] For Supervisory Control And Data Acquisition. This includes the remote monitoring and remote technical management of buildings and facilities, including air conditioning, heating, alarm system, lighting, access, and other aspects.

[15] PABX switchboards, for example: This technology supports as many mini-switchboards as there are configured terminals. Each has a function to forward calls to a remote number. To save time, the password used for protecting this configuration is rarely changed. Hackers test lists of telephone numbers, and when they detect a company with such a switchboard, they configure the call forwarding to generate a mass amount of calls to a premium-rate number.

[16] Perhaps using "mules" to collect and transfer the money in exchange for compensation.

[17] *"Racketeering"* or *"bullying"*.

in scams and fraud, involving digital identity and banking information thefts[18], with fraudulent use of personal data, violation of privacy, and social engineering attacks. **Bioinformatics risk**, targeting personal medical information to cause harm for criminal purposes, is also to be considered.

Related Causes

On the one hand, the level of complexity of the threat will not be directly related to the complexity of the technology. **On the other hand**, we have to expect that threats will become more innovative and sophisticated. They will improve at locating and exploiting new or uncorrected vulnerabilities in *wireless networks, Web applications*, and other technologies for massive data theft, despite existing measures and vigilance. Furthermore, social engineering methods will become more subtle, targeting users in a more personalized way.

For some experts, the increase in the number of occurrences of the various threats presents a major problem, with lawless tools and regions, along with the multiplication of some minor offenses that circumvent the legal system. **For others still**, it is the increasing threat of hijacking information, during a time of crisis or economic warfare, and the increased competition between businesses, both globally and locally (ex. APT for *"Advanced Persistent Threats"*).

References:

Laïdi A. (2010): Les États en guerre économique (Countries in economic war), Seuil.
Metzger M. (2010): Letting the Air out of tire pressure monitoring systems, Defcon Conference.
Rosé P., Loitier P., Guichardaz P. (1998): L'infoguerre, stratégie de contre-intelligence économique pour les entreprises (Cyberwar: a financial counterintelligence strategy for businesses), Dunod.

http://blog.crimenumerique.fr/
http://laurentgentil.wordpress.com/
http://maghrebinfo.actu-monde.com/archives/article7622.html
www.enisa.europa.eu
www.forrester.com; *The value of Corporate Secrets, Forrester Research, March 2010.*
www.gao.gov/new.items/d07737.pdf
www.idtheft.gov/reports/IDTReport2008.pdf
www.infoguerre.fr
www.lemondeinformatique.fr/actualites/lire-motorola-poursuit-huawei-pour-espionnage-industriel-31269.html
www.mcafee.com/us/local_content/reports/7985rpt_labs_threat-predict_0110_fr_fnl_lores.pdf

[18] By all means, particularly using the vulnerabilities of new techniques, such as *multiple contactless cards, RFID, etc.*

1.2. Threats to Organizations

This section presents the study results on threats to public and private organizations during the 2011 to 2020decade[19]*.*

For this question, we present a qualitative summary of citations, stating that the threats vary *according to the business sector, the type of community, and the type of government concerned*.

More Serious Threats

The three most commonly cited threats are common to businesses, communities, and government. They are:

- **Unavailability:** *denial of service, sabotage, blocked access, paralysis*
- **Damage to data:** *strategic, personal, confidential, sensitive*
- **Damage to image:** *misinformation, defamation, compromise*

From a cognitive and social sciences point of view, **difficulties in managing crises can lead to the partial or total paralysis of networks and information systems** necessary for critical activities and major needs. **Despite the true dependence on such systems, they are afforded little consideration.**

The following tables show the number of times the following threats were mentioned, in descending order.

Number	Most Commonly Cited Serious Threats to Businesses
9	Denial of service / blocked access / paralysis / unavailability
8	Loss or theft of strategic data / unfair competition
7	Misinformation / defamation / damaged image
5	Intrusions / economic fraud / embezzlement
4	Cyber-extortion / demand for ransom
3	Theft of personal data managed by the business
2	Threats to vital infrastructures
2	Propagation of malware through social networks / Web navigation
1	Misuse
1	Falsification of documents

Number	Most Commonly Cited Serious Threats to Communities
8	Loss or theft of personal and confidential data
7	Misinformation / political actions / damaged image
6	Denial of service / blocked access / paralysis / unavailability
3	Fraud / embezzlement
3	Threats to technical, security, or monitoring facilities
3	Cyber-extortion / demand for ransom / blackmail
2	Sabotage / threats to vital infrastructures
1	Propagation of malware through social networks / Web navigation
1	Falsification of documents / damage to the integrity of personal information

[19] According to question Q12: What will be the most serious threats to organizations, such as businesses, communities, and government services? *Three threats per category of organization.*

Number	Most Commonly Cited Serious Threats to Governments
9	Loss or theft of data / interception of or access to sensitive data
7	Denial of service / blocked access / attack to e-administration sites
4	Compromised individuals / damaged image
3	Cyber-extortion / demand for ransom: cyber-terrorism
3	Threats to the security / identity of individuals
3	Fraud, particularly relating to official documents
2	Damage to data integrity / falsification of documents
2	Threats to vital infrastructures
1	Propagation of malware through social networks / Web navigation

References:

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France).
Monnet B, Véry P, (2010): Les nouveaux pirates de l'entreprise, Mafias et terrorisme (New enterprise hackers: Mafias and terrorism), CNRS Editions, 250 pages.
Pons N. (2006): Cols blancs et mains sales (White collars and dirty hands), Odile Jacob.
Pierrat J. (2008): Mafias gangs et cartels: la criminalité internationale en France (Mafias, gangs, and cartels: international crime in France), Denoêl.

http://datalossdb.org/
http://securityblog.verizonbusiness.com/category/2010dbir/
http://solutions-logiciels.com/actualites.php?titre=La-securite-des-systemes-SCADA-de-plus-en-plus-vulnerables&actu=4715
www.lecercle.biz
www.les-assises-de-la-securite.com*; 2006-2010 blue books and appendices*

1.3. Threats to Individuals

This section presents the study results on threats to personal assets and data during the 2011 to 2020 decade[20]*.*

For this question, we present a qualitative summary of citations, *stating that the threats vary by the level of widespread use in the presence of vulnerabilities*.

It is emphasised that these threats are expected to increase due to:

- The existence and development of prosperous illegal businesses,
- Security flaws, especially in transactions, databases, personal computing, etc.,
- The use of mobile devices, especially smartphones, and online payments, which are common today.

The following tables show, in descending order, the number of times the threats were mentioned.

Number	Threats to Personal Assets
6	Scams / stolen data
2	Theft of mobile devices: GPS, telephones, smartphones, etc.
1	Physical intrusions or burglaries*, related to home automation or alarm systems*

[20] According to question Q13: How will threats to personal assets and information develop?

Number	Threats to Personal Information
8	Digital identity theft / spoofing / RFID data theft
6	Intrusions / theft / fraudulent use of personal data
5	Mass theft of banking, financial, or card details
4	Invasion of privacy / stolen resources / geographical location
2	Blackmail / disclosure of compromising information

References:

Clusif (2009): Panorama cybercriminalité 2009 (Cybercrime Parorama 2009); *"Réseaux sociaux: menaces, opportunités et convergence" ("Social networks: threats, opportunities, and convergence"), "Web 2.0, le cinquième pouvoir?" ("Web 2.0: the fifth power?")*

Desgens-Pasanau G., Freyssinet E. (2009): L'identité à l'ère numérique (Identity in the digital age), Dalloz.

Katenbach L, Joux A., Les nouvelles frontières du Net: qui se cache derrière Internet? (New frontiers of the Net: who is hiding behind the Internet?, First Société, 2010, p.227-255.

Pinte J.-P. (2010): Pour protéger notre vie privée (Protecting our privacy), Défense no. 14, Special on cybercrimes, threats, and responses, p.38-39, Sept-Oct.

Pinte J.-P. (2010): Gérer son e-réputation sur le Net (Managing your online e-reputation), Quarterly review of the Gendarmerie Nationale, p.35-40.

http://213.139.102.176/gendarmerie/content/download/179227/1532551/file/p35-40%20Dossier%20Net%20PINTE.pdf
www.huffingtonpost.com/richard-barrington/foreclosure-documentation_b_774154.html
www.lefigaro.fr/hightech/2006/09/26/01007-20060926ARTWWW90414-internet_en_le_futur_trouble.php

1.4. Threats to Security Properties

This section presents the study results on threats relating to key security properties during the 2011 to 2020 decade[21]*.*

For this, the four basic properties of security (Co In Av - Ac) and their dependencies must first be defined, along with the threats and barriers to information and systems[22].

These definitions are summarised as follows:

Confidentiality **Co**	Symbolic **property** of keeping a secret, with access only to authorised entities. **Threats** include illegal access or interception, disclosure, removal, and loss. **Barriers** include access to sensitive or classified information by unauthorized third parties, or also voluntary or accidental disclosure. **Dependency** with integrity (In).

[21] According to question Q14: What changes can be expected in the distribution of threats to the confidentiality, integrity, availability, and accountability of *information and systems*?

[22] Recall that the term "object" applies to information and to systems. Additionally, sensitive objects relate to confidentiality and integrity (*ex. personal data, classified information, research and development, etc*.). Vital objects relate to availability and integrity (*ex. management systems, control data and systems, etc*.). Also, "sensitive" or "vital" are preferred to the more ambiguous terms "strategic" or "critical". These four properties (Co In Av - Ac) are essential, and it is important to emphasise three of them concern integrity, which is fundamental.

Integrity **In**	Symbolic **property** of storing data and components without corruption in space and time. **Threats** mainly include modification. **Barriers** include modification by an unauthorised third party or following an incident or mistakes made by an authorized individual. **Dependency** with confidentiality (Co).

Availability **Av**	Symbolic **property** of proper delivery under the stated terms regarding times, deadlines, and performance. **Threats** include disruption or interruption, destruction, removal, or loss. **Barriers** include the accessibility of data and continuity of services by providing sufficient resources, by authorized individuals. **Dependency** with integrity (In).

Accountability **Ac**	Supplementary **property** related to monitoring assignments and duties performed, without possible repudiation. **Threats** include modification, destruction, removal, or loss. **Barriers** include access to a control system and also unauthorised or accidental manipulations to the system or to test data. **Dependencies** with integrity (In) and availability (Av).

All Properties

The threats are mainly due to a tougher competitive environment and the potential to profit from sensitive information. They result from the difficulty of controlling information due to mobile employees and cloud computing, exposing generated data in transit and stored outside the company. Overall, **for some experts**, the increase will affect all properties equally. **For others**, confidentiality will be the most threatened property because it involves the most sensitive units. Availability will also be highly affected by distributed attacks, service shutdowns, or sabotaged infrastructures affecting vital targets. **For a minority of experts**, criminals will be most concerned with accountability.

Confidentiality

There is likely to be a major increase in threats, particularly with a resurgence of malware. The fear is the constantly growing interest in personal and professional data that is highly vulnerable in terms of confidentiality and integrity.

Integrity

The amplification of threats related to malware, mainly affecting intangibles, and accidental causes or human error is expected to stabilise. Attackers are likely to take advantage of mistakes made by potential victims in order to remotely commit an intrusion or install malware to compromise integrity, mainly for the purpose of collecting useful information.

Availability

There may be a decrease in accidental causes, offset by an increase in maliciousness, ultimately compromising availability. In fact, the increasing occurrence of attacks against servers and infrastructures and denial of service attacks suggests that availability will be affected even more, despite lower risks due to redundancy and cloud computing.

Accountability

Accidental causes are expected to remain stable, despite the focus on traceability under the mounting pressure of regulations, but malicious causes are expected to increase, with more sophisticated attacks and attempts to conceal one's tracks. Business logic often conflicts with the needs of traceability and logging traces. Cybercrime close to home (such as internal cybercrime) could also increase the threat. A minority of experts feel that, because of progress made in the field of security and the skill of specialised investigators and judges, the primary focus among criminals may be to compromise accountability.

References:

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France), Report, 102 pages.

http://news.netcraft.com/archives/2010/04/15/april_2010_web_server_survey.html
www.huyghe.fr/actu_747.htm
www.cloudsecurityalliance.org/
www.arbornetworks.com
www.ponemon.org/research-studies-white-papers
www.cert.org/
www.memoireonline.com/04/09/2033/m_La-Cybercriminalite-nouveaux-enjeux-de-la-protection-des-donnees3.html

2. ATTACKS

2.1. Types of Attacks

This section presents the study results concerning the distribution of attacks, in terms of both number and severity, given the cited offenses, during the 2011 to 2020 decade[23]*.*

It is very difficult to accurately measure the different type of attacks, in number and in severity, as **it is already difficult to predict general trends in conventional crime**. There is still a problem in the existence and relevance of tools used to measure these changes. Several attempts have been made to solve this problem within the profession by sharing appropriate security indicators and developing related documents on the existing technology. Moreover, victim surveys[24] are not always satisfactory with regard to the perception of risks among those who respond to the questions. Overall, however, there is expected to be an increase in attacks due to a major increase in connectivity among individuals, businesses, and governments.

The following potential attack trends were identified:

Attacks to Electronic Identity

Electronic **identity theft**, resulting from acts of interception and data theft, will increase, particularly through social engineering, currently carried out in cybercrime using malware tools and powerful methods, such as phishing and spamming. Personal data will continue to be intercepted from personal systems, businesses, and communities over time, given their increasingly high tech nature, for financial gain and other motivations.

Attacks on Minors

Child pornography is expected to remain steady in terms of physical concurrent acts. This form of crime relies on "*human material*", with children victimised by acts of paedophilia or made to participate in carrying out offenses. This is still risky for criminals due to legal enforcement. What will change in this area is the way in which images and videos will be exchanged, with greater availability and concealment. *Child pornographers often argue that they are not doing anything wrong, instead believing themselves to be merely "voyeurs"*.

Attacks on Infrastructures

Critical infrastructures will be targeted by cyberterrorism for various reasons. Power distribution networks, transportation networks, and communication networks are expected to undergo attacks intended to paralyse a nation by depriving it of its vital services. Such attacks could cause unprecedented crises on many levels, including *the economy, safety, health, sanitation, civil peace, and more*. In addition, hackers and other cybercriminals (even governments themselves) could further target their opponents. They may include attempts to attack informational sites, with a growing number of counterattacks by some governments or resistance groups (*ex. exiled Tibetan dissidents*).

[23] According to question Q21: How will the distribution of attacks change, both in terms of number and severity, given the offense, including fraud, interception, data theft, intellectual property violations, identity theft, child pornography, e-reputation, etc.? *Distinguish between individuals and public and private organizations, specifically noting whether the attacks to critical infrastructures (ex. telecoms, power networks, etc.) may become a major risk.*

[24] Such as the surveys conducted by CLUSIF in France each year.

Attacks to Reputations

Reputational attacks[25] are expected to increase, mainly in terms of severity, to the point of becoming a significant – or even definitive – cause of an attack to a company or an individual's image.

Attacks to Intellectual Property

Intellectual property theft and other forms of counterfeiting will become more dominant, mainly in terms of number, for some sectors (ex. R&D, innovation, and high tech). Intellectual property will never truly be respected and protected. Outside of artistic works, many online documents are freely plagiarised by other users.

Attacks on Assets

"Nigerian" **scams**, based on a request for charity, the lure of monetary gain, and hypothetical encounters, originating in certain countries[26] and targeting more developed countries, will increase with a rise in Internet penetration, facilitated by the weakness of existing networks. This goes hand-in-hand with payment fraud following the theft and exploitation of banking details.

2.2. Aggravating Factors

This section presents the results of the analysis of the aggravating factors involved in committing the cited offenses, during the 2011 to 2020 decade[27].

The following main aggravating factors were identified:

Mobility and Virtualization

Mobility and mobile employees naturally are better able to transfer malware and to retrieve sensitive data. Computer systems are growing weaker due to the popularity of remote access and local file storage, making them more sensitive to threats such as data loss or theft[28]. Also, with the advent of cloud computing, businesses and individuals become physically separated from their data.

Crises and Social Inequality

A crisis makes users less attentive and increases their chances of being duped by ever more imaginative crooks. Economic and social crises are a breeding ground for cybercrime because they increase the number of outside players, in addition to company employees seeking recognition. Actions are also more frequent, due to the diverted attention of

[25] Or "*e-reputation*". This is primarily an attack against the image of known individuals, institutions, or other public or private organization.

[26] For the French, these especially come from French-speaking African countries. They seek to extract large sums of money from gullible people, called *"mugus"* or *"mougous",* via fraudsters, often by means of a Western Union office for the payment of a percentage or commission to the agent. With this phenomenon growing, the amounts of money involved are sufficient to provide a good standard of living for an entire family or even a neighbourhood, sometimes more, thereby providing protections.

[27] According to question Q22: What will the aggravating factors be: dependency, crises, mobility, cloud computing, etc.?

[28] This is especially true when data is stored on portable media devices, such as *notebook PCs, smartphones, memory keys, and other devices*.

businesses[29]. Crises make it easier for criminal groups to recruit skilled computer scientists who are lured in by the prospect of financial gain. There is an ever-increasing gap between those with access to these means of communication, information, and new forms of socialisation and those who are excluded from them. Moreover, the loss of social or moral values can lead individuals to be more vulnerable to contacts over the Internet, favouring a boom in partisan businesses. Finally, some public announcements[30] by organizations may lead to acts of retaliation, including boycotts and denial of service attacks, intended to be justified and righteous, creating the possibility of being copied in a number of ways, not always controlled.

Trends in Computer Systems

Technology seems to be changing in a way that reflects increased security in cyberspace, thanks to the popularity of mobile interfaces, *with smartphones, tablets, onboard computing, and connectivity, automobiles embedded equipments,* as well as the virtualisation of storage systems. This is because of the very rare implementation of secure architectures. There is also an opinion that cloud computing architectures blur the boundaries between what is physical and what is digital, to the point where no one knows where the data is stored, nor who manages and uses it, etc. Furthermore, the commercial availability of SCADA[31] remote management systems, designed for the remote monitoring and acquisition of data, has shifted toward equipment that uses the same technologies, protocols, and operating systems as the general public, including *TCP/IP, Ethernet, operating systems, etc*., thereby increasing their vulnerability. The complex nature of the global Internet means that attacks against critical networks can become more common and more dispersed.

Dependence on Technology

According to the 2010 survey by CLUSIF, 73% of companies in all sectors combined *(regardless of their size)* consider an outage lasting fewer than 24 hours to have serious consequences. The dependency on computer systems is already a debilitating factor that increases with the development of cloud computing, virtualisation, and mobility. Individuals, organizations and businesses rarely consider the risk involved with interconnecting their systems. Backup systems for working locally after an attack are rare, inexistent, or even ineffective in response to a disaster. All public and private services, including *public finances, town halls, hospitals, public transports*, and more, could be disrupted or shut down in order to cause serious problems to health, safety, and the public order.

The increasing dependency of businesses, the lack of diversity, the overabundance of interconnected systems, the complexity of adequate security needed for cloud computing, especially offshore, and the concentration of data in mega-centres will all be aggravating factors.

Everyday Use of Electronic Banking Services

The everyday use of virtual and/or electronic money: This money is subdivided into two categories: "trust" money and "precious metal" money. The first is based on the trust between the buyer and the seller. It has no legal tender; its value exists only for the individuals and businesses that use it (*ex. WebMoney, WMZ* and *UKASH*). The second, backed by precious metals, uses the value of gold to establish its conversion rate for electronic money (*ex. eGold* and *Pecunix*). Once the money is converted, the funds and the

[29] The growing use of foreign outsources, mainly for monetary reasons, increases the risk of lost skills and mastery.

[30] Anonymous, Greenpeace, WikiLeaks, etc.

[31] Supervisory Control And Data Acquisition.

account are often impossible to trace. Used increasingly more frequently, cybercriminals will be more eager to get their hands on it, as it is difficult for victims to justify their claim. Criminal networks will also use it to conceal their transactions or launder the money from their activities. They will also use it for themselves. Of the electronic currencies mentioned above, criminals gravitate toward those that provide the greatest anonymity and the least traceability. On the websites and forums they frequent, *eGold, WebMoney* and *Western Union* are often preferred. In France, unlike notaries and banks approved by the banking commission, they are not required to file statements of suspicion to TRACFIN[32] when there is a suspicion or when a transaction exceeds a certain amount.

Penetration of Equipment in our Daily Lives

The gradual disappearance of the separation between **private life and professional life** with the use of domestic digital equipment[33] will result in problems like mismatched equipment, while the growth in the number of connected devices also represents open doors to privacy in the home, opportunities for cybercriminals.

References:

www.clusif.asso.fr
www.ponemon.org*, "Business Risk of a Lost Laptop", Ponemon Institute, April 2009*

2.3. Main Goals

This section presents the results of the analysis of the main goals involved in committing the cited offenses, during the 2011 to 2020 decade[34].

Profitability

Fundamentally, **the primary goal** of crime has never changed. It seeks to **maximise financial profits** by minimising risks, analysed from its own point of view. This is true of all criminal communities, regardless of the initial motivations and their geographical areas of activity. Damage to privacy is only one of many ways to achieve this same result. Attempts at disorganization or instability, if they can be recognised at first as ideological approaches, are often tied to a financial risk. Because **competition** is increasingly more exacerbated, disruption activities will increase with regard to companies. Attacks will continue to build competitiveness through regular mass penetration attempts and a looting of intellectual property, sometimes supported at a government level.

Search for Power

The second goal will certainly be the **search for power** through the control or destruction of information. That is, although greed is still a top goal among cybercriminals, actions to destabilise vital centres are expected to also increase in the coming years. In fact, the use of digital networks is a strategy that requires little investment, particularly for emerging countries that are facing major economic difficulty. In a society where information is a weapon, being able to search it, store it, and control it constitutes an obvious power up to federal level. We

[32] For *Traitement du Renseignement et Action contre les Circuits Financiers Clandestins* (Information Processing and Action Against Clandestine Financial Networks).

[33] Associated with the well-known BYOD concept, for "Bring Your Own Devices".

[34] According to question Q23: What will be the main goal: financial gains or losses, damaged privacy, instability, disorganization, misinformation, destruction, terror, etc.?

should also expect some spectacular actions targeting resources and infrastructures for ideological reasons.

Invasions of privacy will prevail in order to continue obtaining and exploiting personal data. These intrusions will have the ultimate goal of **seeking financial profit**, with financial, banking, or advertising data or in **search of power**, with social networks, recruitment by terrorist organizations, etc.

It is also considered that, with the emergence of various **markets of cybercriminal services**, a competitive commercial sector will become established. It will be frequented by diverse criminals with various motivations, who take advantage on their geographical location and their organizational and technical skills, and are seeking to achieve their criminal goals, whatever they may be, by profiting from opportunities in cyberspace.

References:

Verizon (2011) : 2010 Data Breach Investigations Report, Verizon/US Secret Services.

http://gocsi.com/

2.4. Ability to Compromise Countries

This section presents the results of the analysis on possibly creating government instability through the behaviours cited, during the 2011 to 2020 decade[35].

Opinions are quite divided on this question, but governments are already aware of it as we can see by the setup of prevention and detection devices in the United States – *with the "Perfect Citizen" program that is designed to monitor infrastructures that are deemed to be critical to national security* – and in Switzerland, *with its annual report by the Swiss Confederation Intelligence Service (SRC).*

Countries vulnerability

The relationship between cybercriminals, rogue countries, and transnational non-governmental entities seems to be in line. Rumours of computer attacks conducted by or encouraged by nationalist, corrupt, or authoritarian regimes are becoming more precise. While the concept of cyberwar is no longer reserved to science fiction, it is not unlikely that unstable regimes, rival countries, and terrorist or radical – *such as eco-terrorism* – movements may turn to methods of cybercrime. After nuclear weapons, cybercrime weapons appear to be dangerous, and particularly "*clean*", with little direct damage to human lives.

Countries stability could certainly be compromised, and this will undoubtedly be the goal in some cases of mass attacks directed against vital infrastructures and networks needed for the economic and social activity of a country to function properly. Concerted, or orchestrated, misinformation could achieve a socio-political destabilisation or retaliation by means of an economic or commercial boycott of a country. European governments already take this type of threat seriously and simulate major incidents in order to observe, coordinate, and improve the implementation of countermeasures among all national structures in order to reduce the impact of a cyberattack or to attempt to resolve it and restore stability. The effectiveness of the means for responding and coordinating industrialised countries remains to be seen.

[35] According to question Q24: Would it be possible to compromise the stability of countries?

Sensitive infrastructures may be a target for blackmail demanding a ransom or by terrorist organizations. Their "*conversion*" to ever-present standard systems (*ex. Windows*), the abandonment of closed systems, and the indirect opening of these networks to the Internet through management systems, will increase both the number of people who are potentially at harm and the number of weaknesses.

Governments stability is clearly threatened, or otherwise compromised, by the emergence of a resilient market of criminal services focused on the illegal use of Internet technologies. Such a phenomenon would make it possible to commission a number of offenses that attack country's stability, an attractive alternative to undervalued advanced skills. This would include everything from corruption to money laundering.

Factors Limiting the Countries Weakness

Industrialised societies are certainly the most dependent, and therefore the most vulnerable in the event of a serious attack. However, their governments possess intellectual and material resources for dealing with this, even if we cannot exclude serious failures.

Although it would be difficult to compromise a country's stability, the following situations are possible:

- **Acts of retaliation** against a country by militias or anti-state organizations in order to defend a cause, targeting the availability of infrastructural networks or e-services
- **Acts of deterrence** or warning against a government regarding a policy that is considered to be contrary to certain interests, targeting the availability of the computer systems of some government services
- **Acts of terrorism**, targeting the availability or integrity of institutional websites of sensitive government services

Although **weaker countries** appear to be less dependent on computer technologies, and therefore less vulnerable, we cannot exclude the fact that they are among the collateral victims, for example, of a crisis triggered by computer manipulations to stock markets or attacks on public infrastructures, *including power grids, telecoms, transportation, administration, and more*.

Governments as the Initiators of Attacks

Until now, governments have always denied their involvement in this type of attack. It may not be long before we see undeniable proof of their participation. Since it is impossible to isolate these chaotic places to keep them from implementing such actions, some democratic countries may be tempted to use these same methods for purposes they deem to be worthwhile in order to respond to or even launch pre-emptive attacks. The consequences of such an action, under the guise of protecting our democracies, could be catastrophic.

References:

Guinier D. (2010): L'informatique dématérialisée en nuages – *Ontologie et sécurité du "cloud computing"* (Cloud computing – *Ontology and security of cloud computing*). *Expertises,* no. 351, October, pp. 335-344.
Goldstein G.-P. (2010): Babel Minute Zero, Thriller, Denoël., 723 pages

http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html?mod=WSJ_Tech_LEFTTopNews
www.lemonde.fr/technologies/article/2010/07/08/citoyen-parfait-le-big-brother-a-l-americaine_1385055_651865.html
www.news.admin.ch/NSBSubscriber/message/attachments/19841.pdf

3. THE AUTHORS

3.1. The Origin of Threat Agents

This section presents the analysis of the prospective description of the origin of threats, during the 2011 to 2020 decade[36]*.*

Difficulties in Evaluating the Origin

Changes to the origin (internal, external, and mixed) of threats are hard to estimate, due to various factors and contradictions that appear in the studies and particularly because the facts are not always completely known. Also, we must properly distinguish between the number of incidents and the total damage caused. We must note **that in addition to changes in cybercrime**, there will be losses due to failures, malfunctions, neglect, or even human error. The estimate is generally that 80% are internal threats and 20% are external threats, but these figures are not based on a reliable source and prove to be contradictory in terms of occurrence and impact.

Therefore, **the experts are divided**, based on their sensitivity to changes and underlying factors. The argument is based on tracking changes in past years for an understanding of the phenomenon. **Some experts** point out an increase in the distribution of internal threats, while **others** (representing the majority) cite an increase in external threats. Finally, **a third group** believes that there will be a **balance between internal and external threats**: *the source of which is mixed and divided, with increasing variation from country to country*. **Externally**, most experts believe that there is a growing risk associated with transnational organized crime, which will continue to grow as it benefits from loopholes.

Increase in Internal Threats

The argument in favour of an increase in internal threats is mainly based on the following trends:

- The easy nature of carrying out targeted threats
- The deteriorating internal social climate of public and private organizations
- The impact of internal insufficiencies and negligence, etc.
- The difficulty of carrying out external threats due to increasing security levels

Increase in External Threats

The argument in favour of an increase in external threats is mainly based on the following trends:

- The number of users who are trained in new technologies
- The mix of the planet, high speed, context, and international conflicts
- Incidents related to partners and agencies located in other countries, etc.
- The development of mass crime linked to the development of the Internet in emerging countries
- Very broadly interconnected systems, with easy access to company data and personal data, and individuals who are always connected, etc.

[36] According to question Q31: What changes will there be in the origin of threats (internal, external and mixed)? *Provide the distribution in terms of percentages in 2010, 2015 and 2020*.

- Transnational organized crime, which is difficult to counter with technological improvement, will continue to grow thanks to perpetual loopholes in international cooperation.

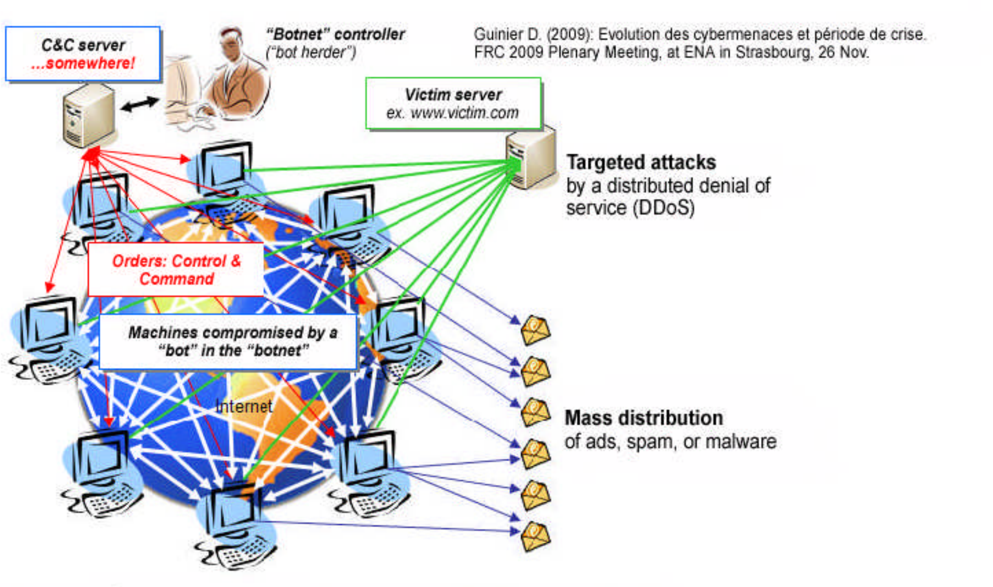
Increase in Mixed Threats

The argument in favour of an increase in mixed threats is mainly based on the following trends:

- The difficulty of attacks without any knowledge from the outside
- The use of subtle means of social engineering
- Shared profits with external third parties during crisis periods, etc.

Evolution of Threats Sharing in the Medium / Long Term

Some experts believe that it will not be possible to determine a clear trend over the next five years. Very few of them established percentages, but the general trend shows a significant increase in external threats over time. **In the short term**, there are threats relating to increased deviant behaviour and the use of botnets as **effective attack mechanisms**. **In the medium term**, there is the compromise and/or partial or full destruction of cyberspace and its instruments, including space satellites. On this point, some experts anticipate the possibility of a major political-ideological and energy catastrophe.



Guinier D. (2009): Evolution des cybermenaces et période de crise. FRC 2009 Plenary Meeting, at ENA in Strasbourg, 26 Nov.

"Botnet" for attacks or mass distributions

Currently, most experts agree that the threat is mainly internal, resulting mainly from accidents or human maliciousness. **In the next five years**, the internal threat is expected to decline under the effect of increased security measures taken by companies. However, the external threat is expected to increase due to the overall development of the Internet and system interconnectivity. The rise in social engineering is expected to lead to an increase of this approach, which mixes internal and external activity.

By 2020, the **internal** threat will still be present, although most experts agree that it will fall sharply, primarily due to greater ease of access to computer systems and the good understanding of sensitive, usable information. Information system security (ISS) in businesses will then have reached a level of maturity, and the means for fighting against internal fraud will be formalized. Concerning the **mixed** threat, social engineering will continue to be developed in order to seek internal complicity and to counter increasing levels of security.

Externally, **most experts** believe that there is a growing risk associated with transnational organized crime, which will continue to grow due to a lack of international cooperation. Additionally, cloud computing will eventually outsource risk and make some external threats larger.

References:

Clusif (2009): Fraude interne, malveillance interne: détection et gestion (Detecting and handling internal fraud and internal malice). CLUSIF conference of 4 June 2009.
CSI (2009): 13th CSI Computer Crime and Security Survey 2008.
CSI (2010): 14th CSI Computer Crime and Security Survey 2009.

http://accenture.com/dataprivacyresearch
http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1110&Itemid=37
www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf
www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf
www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

3.2. Profiles and Types of Threat Agents

This section presents the analysis of the classification of threat agents by category, during the 2011 to 2020 decade[37]*.*

The Strong Trend and Skills Networks

Most experts find a strong trend related to the industrial organization of cybercrime activities, including a business model, business plans, and pricing policies borrowed from the commercial world and even its customer service. This observation entails that the independent *hacker*/cybercriminal profile will disappear in exchange for a mercenary workforce recruited to carry out an assignment, based on skills, working in teams to share the work – and the risk – due to international dispersion. To this end, there appears to be national specialisations, such as *software in Russia, hardware in Japan, etc*. There are also hacker groups and those specialising in propaganda, destabilisation, and manipulation, who will be able to use social networks and methods of production and falsification that have so far been reserved for counterfeiters.

These skills networks sell themselves to the highest bidder, regardless of whether it is a criminal group, terrorists, major industrial groups, or rogue countries that use sophisticated off-the-shelf tools for attacks, concealment, and propaganda, which they need in order to reach their financial or political goals. Cybercrime is therefore within their arsenal as a particularly effective weapon due to its low cost.

Some experts believe that countries are likely to convert some of their defensive potential into tools and offensive strike forces in order to try to restore deterrence in cyberspace,

[37] According to question Q32: What will be the change in profiles of threat agents by category, including independent hackers, social groups, activists, organized crime groups, terrorists, governments, etc.?

adding to the diversity of threat sources. **Beyond this major trend**, some mentions the persistence of a low-intensity criminal (*ex. scammers among individuals*) who takes advantage of opportunities and the anonymity of digital flows.

Difficulty of Clarifying Profiles

It seems illusory to establish a clear differentiation of profiles, being that the pool is common and always increasing with the spread of technology and "*employers*" who somehow maintain convergent interests. Also, identifying the tracker remains random, with a particularly complex and rarely convincing attack traceability. **Activist groups** (*partisan, terrorist, or extremist groups*) represent an increasing threat, seeking the media multiplier effect and the anonymity of their actions through information technologies. These movements will use the Internet increasingly more often as a way to support their actions.

References:

Rosé P., Le Doran S. (1998): Cybermafias, Denoël.
Rosé P. (1996): Crime organisé et délinquance informatique, in L'Evolution de la criminalité organisée, actes du Cours International de Haute Spécialisation pour les Forces de Police, La Documentation Française (Organized crime and cybercrime in Evolution of organized crime, documents of the International Court of High Specialisation, for the Police Forces, French Documentation).
Clusif 2010): Une entreprise criminelle au microscope (A criminal organization under the microscope), Panorama cybercriminalité (Cybercrime Panorama).
Guisnel J. (1995): Guerres dans le cyberespace, services secrets et Internet (Wars in cyberspace, secret services, and the Internet), La Découverte (Discovery).
CSIS (2008) – Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies, Washington DC, December.

3.3. Skill Levels and Required Resources

This section presents the analysis of the study, focusing on skill levels and the required resources for carrying out acts of various types and severities, during the decade from 2011 to 2020[38]*.*

Skill Levels and Resources

Experts are divided on changes to skill levels and required resources. The change is expected to be distinct in terms of the various categories of threat agents. Particularly significant is the importance of mastering and selling kits that make it possible to create or expand cybercriminal activity. With new procedures that are sure to arise, especially for automating and concealing attacks, there will be criminal groups specialising in the resale of criminal services, as well as other, more diverse groups, who will use these services or work for the benefit of bigger groups. **Advanced legal and financial skills** will be sought after for carrying out money laundering and actions to protect the originators.

Industrialization and the Economy of Cybercrime

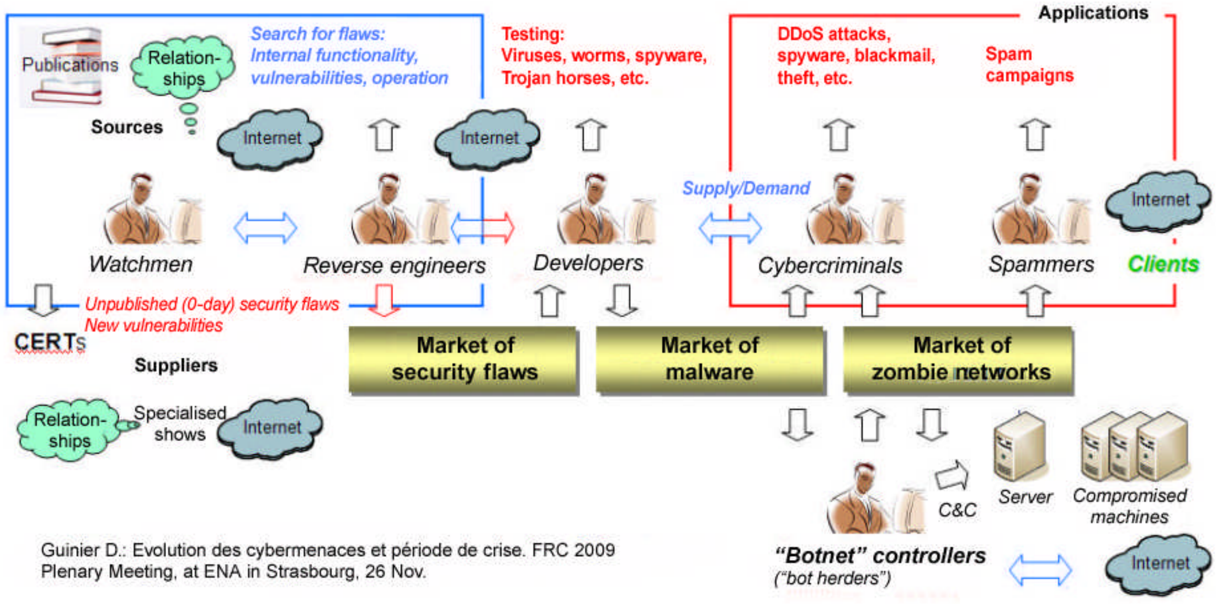
The more complex the defences, the more advanced the level of attack will have to be. It is easier to penetrate systems (*critical systems, banks, etc*.) for those who played a role in developing them. It will be important to ensure that the people creating such systems are loyal. This will be the same for people fighting against cybercrime, the risk being that they

[38] According to question Q33: What will be the change of skill levels and required resources for actions that are more or less serious, on a more or less large scale?

may breach the divide due to the social climate, their level of compensation, or even a lack of recognition. We should therefore expect a higher level of skills and equipment for organized cybercrime, with the availability of expertise in criminal operations. Along with that come industrialisation and the establishment of a real economy based on cybercrime, including:

- **Higher skill levels for the creators of resources:** *tools and kits*
- **Lower or stable skills for the users of such resources:**

Cybercrime is looked upon as a service, with the idea "*CyberCrimeware as a Service!".* It already borrows botnets and proxies for distributed denial of service (DDoS) attacks and spam campaigns, Trojan horses that are bought and sold on specialised sites, and auctions that are available to the general public.



Guinier D.: Evolution des cybermenaces et période de crise. FRC 2009 Plenary Meeting, at ENA in Strasbourg, 26 Nov.

The Argument for Growth

The argument in favour of growing skills is also based on the understanding of ICT and the Internet, brand new methods of programming, constant connectivity in a virtual context, and the increasing skill level – whether *internal, experts, or expert consultants* – exploiting the knowledge of the computer system. **The argument in favour of the growth in resources** is based on organizations who have a very high level, including countries *with advanced research and considerable computing power,* businesses that cooperate with government organizations, and highly-qualified individuals who are needed in order to achieve such resources.

The Argument in Favour of Stability or a Reduction

The argument in favour of stability or a reduction in the level of skills is based on that fact that many online scams are committed by people without sophisticated resources, but rather with knowledge of human psychology and personal behaviour. This is combined with information and tools, which are freely available and sold on the Internet and are powerful enough to allow people with few skills to enter the world of cybercrime on their own. Knowledge and work are shared through active community sites.

References:

CSIS (2008): Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December.

www.cnis-mag.com

3.4. The Place of Organized Crime

This section presents an analysis of the significance of organized crime and how it will change, during the 2011 to 2020 decade[39].

Evolution of Organized Crime Place

All experts agree to the idea that organized crime will have a significant – if not major – place in cybercrime. The nuance between the experts is more in terms of quantity than quality, namely that, despite its weight, the activity of organized crime will always remain as discrete as possible in order to be able to continue. As pointed out by the experts, the relative place of organized crime may be lessened by competition and internal tensions, as well as by the emergence of state or semi-public players with the financial and technical power to challenge a potential hegemony.

The Convergence of Organized Crime and Cybercrime

Similar to how human activities are becoming increasingly more dependent on new information and communication technologies, organized crime has clearly identified all of the potential at its disposal, including discretion, speed, lack of paper trails, internationalisation, low risk, high profitability, and more. The use of these technologies is therefore expected to increase, both for a wide range of mafia activities and for concealing and laundering financial gain from these activities, making cybercrime an essential convergence for organized crime. If the digital divide were to increase to the point that it adversely affects the abilities of law enforcement due to the notable difference in human and material resources at stake, organized crime would still benefit by increasing its use of digital tools relative to the "*traditional*" route for its activities.

Strategy and Structures of Organized Crime

The most commonly mentioned strategy is **to exploit the globalisation of connections in order to develop the criminal network on a global scale** by overcoming geographical constraints and using expertise wherever it is, similarly to the international division of work. A true "*digital crime*" economy is setting up with a range of services that is tailored to the needs of organized crime, which can also be exploited by other entities for a fee.

Organized crime develops into powerful structures, like digital crime businesses, as is seen today in the former Soviet block and as is expected to emerge from Africa and South America. It is and will be a major player with wide-scale operations, including embezzlement, financial and economic fraud, and money laundering, in a way that is less visible relative to the number of incidents. Various activities that were previously handled in the real world are now housed in the virtual world, including *sexual exploitation, prostitution, gambling, money laundering, illegal sales, and counterfeiting*, all done through the Internet. This also includes

[39] According to question Q34: How will the importance of organized crime change? *Will it be a major player? Why? With what strategies?*

misinformation for the purpose of destabilising companies or countries that interfere in the activities of these groups.

References:

CSIS (2008): Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December.

Clusif (2010): Une entreprise criminelle au microscope (A criminal organization under the microscope), Panorama cybercriminalité (Cybercrime Panorama).

Rosé P., Le Doran S. (1998): Cybermafias, Denoël.

Rosé P. (1996): Crime organisé et délinquance informatique, in L'Evolution de la criminalité organisée, actes du Cours International de Haute Spécialisation pour les Forces de Police, La Documentation Française (Organized crime and cybercrime in Evolution of organized crime, documents of the International Court of High Specialisation, for the Police Forces, French Documentation).

GRASCO (2010): Garantir que le crime ne paie pas – Stratégie pour enrayer le développement des marchés criminels (Ensuring that crime does not pay – Strategy for stopping the development of criminal markets), under the scientific direction of C. Cutajar, Strasbourg University Press.

4. VICTIMS

4.1. Most Targeted Sectors

This section provides an analysis of the prospective description of the socio-economic sectors that are expected to be most targeted, during the 2011 to 2020 decade[40].

Order of the Most Targeted Sectors

Few experts venture to determine the priority order of the sectors that will be most targeted over the next ten years, except to use the existing classifications. It remains very difficult to classify the sectors by their vulnerability. They are all concerned, with none being immune from cybercrime, regardless of the size of its structures. All sectors involve strategic information and financial risk. Although finance and e-commerce are often mentioned due to their strong appeal among cybercriminals, all other sectors are already targeted and will become even more vulnerable with their growing dependency on digital technology and the strategic information of the data they manage, representing a potential for disorganization. The threat will be even greater, as the discussion to anticipate risks and develop adequate protective measures will not have been completed. Furthermore, because the threat is becoming more multifaceted and using increasingly more complex channels, it is likely that the success rate of stealth attacks to steal personal or confidential data will increase.

All Sectors by Purpose

For a large majority of experts, no sector will avoid cybercrime altogether, but a distinction of the attacks will be made based on the purpose, such as intellectual property theft for monetary gain – *for companies that may or may not have been aided by their government* –, the rapid financial gain or malicious destabilisation – *including terrorism, reputational damage, cyber-conflicts, and more*. In the first case, there will be a systematic looting of market leaders in their field. In the second, the finance and online transaction sectors will be very frequently and heavily attacked. In the final case, the attacks will be extremely targeted toward manufacturing, energy – *including nuclear* –, defence, vital infrastructures, and highly political or societal sectors, in order to destroy or create as much disorder as possible to guarantee the highest possible media exposure.

Notwithstanding the many counterfeits, many sectors, including transports, agri-food, and pharmaceuticals, are currently in a truly global economic war. They are expected to face a large number of attacks to gain trade secrets and project information. Finally, it is highly likely that some sectors, like the entertainment industry already, will be forced to change their business model under pressure from counterfeiters and massive illegal downloads.

The ICT Sector

The IT and telecommunications sector – *more generally ICTs* – appears to be a key target with its undeniable potential for destabilisation in a society that is ever more dependent on new technologies and used as a mean to reach other sectors. Similarly, third-party companies that process sensitive information, such as audit firms, insurance companies, consulting firms, etc. are likely to be targeted as well, to the extent that the regulatory or legislative environment continues to increase their role and scope of involvement.

[40] According to question Q41: Which socio-economic sectors will be the most targeted: online finance and transactions, industry and transports, energy and defence, IT and telecommunications, services, agri-food industry, health, research, government and territories, etc.?

References:

CE (2009): Cybersecurity and politically, socially and religiously motivated cyber attack, Study by the European Parliament, February

Verizon (2010): Data Breach Investigations Report, Verizon/US Secret Services.

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France), 2010.

4.2. Victim Behaviours

This section presents the analysis of the prospective description of changes in the behaviour of victims (individuals and organizations), during the decade from 2011 to 2020[41].

Individuals

There is a general consensus among the experts that individuals, who are better informed and more aware of digital risks, are expected to be able to avoid a lot of trouble by having acquired the resources with which to act, *including platforms for submitting reports to the state or to ISPs[42] regarding illegal content, a reporting button on social networks, and online complain forms*.

The reporting and filing of complaints is expected to grow significantly with the increasing violation of personal privacy and data. However, this trend clearly could be largely thwarted if means of repression such as *law enforcement, magistrates, legal framework, and criminal policy* are not quickly strengthened to meet the needs in terms of both quantity and quality.

Few experts believe in a particular effort to invest in logical security solutions because protections, which are often costly, may not be up to par whatever the sector may be. Their saving grace will be that, fortunately, such solutions will eventually come standard – not merely as an option – in software and in operating systems. However, none of these solutions will be beneficial if the protective services available to complainants are not considered to be effective.

Legal Entities

Legal entities, also better informed about digital risks, should be able to reverse a general trend. They are expected to invest in security, insurance, and employee training solutions, but they will always be reluctant to report cybercriminal attacks and less inclined to complain in order to maintain their reputation (user/customer confidence) and to save costs of an uncertain legal procedure. Only a binding legal framework and an effective response from law enforcement would be likely to encourage legal entities to identify themselves as victims of a cybercrime.

However, with the fast-growing popularity of phishing, banks, once reluctant to discuss the subject, have begun to complain and recognise a certain helplessness they have when faced with the problem. Their main concern was that their customers would flee once they discovered the corruptibility of the electronic safes used for online bank accounts. But the combined action of the police, the legal system, and international legal institutions, CERTs[43], helped to maintain confidence and to develop countermeasures.

[41] According to question Q42: What changes will there be in the victim behaviours: reporting of complaints, protective measures, etc.? *Distinguish between individuals and organizations*.

[42] Internet service providers.

[43] For "Computer Emergency Response Team".

Victim Expectations

One constant common finding is that the effort of prevention, of training and educating of end users, whether individuals or corporate body, seems to be the best way to influence behaviour, increasing awareness and maturity in their activities in cyberspace. There are strong expectations regarding state actions, which currently seem to be minimal and powerless, given the magnitude of cybercrime. Failing that, one expert suggests setting up pressure groups to obligate governments to react.

The current legal system can hardly consider these cases of cybercrime, either during instruction or judgment. This is because of procedural delays, which are incompatible with retaining data and a difficult international cooperation outside of the European Union. Combine this with the technical challenge of the cases and the low level of compensation that is awarded. Without a quick improvement, courts may handle fewer and fewer cases. Several experts point to the risk of information rejection by the society, but more likely of the vulgarisation of cybercrime. Without an immediate or otherwise satisfactory response, victims would be pressured toward resignation. Also, recent studies clearly show this distrust toward the ability of the police and criminal systems to handle cybercrime, along with a widespread feeling of guilt or shame among victims, who blame themselves for being careless, which encourages them to keep discreet about their troubles.

References:

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France).
Symantec (2010): Norton's Cybercrime Report: Impact on Victims.
Myriam Quéméner, Joël Ferry (2009): Cybercriminalité, défi mondial (Cybercrime: a global challenge), 2nd edition, Economica.

www.cybercrime.gov/reporting.htm#cc
www.internet-signalement.gouv.fr
www.ic3.gov

4.3. Factors Influencing Behaviours

This section presents an analysis of the prospective description of factors likely to influence the behaviour of future victims, during the 2011 to 2020 decade[44].

Security Factors

The responses from the panel of experts are in line with the answers to the previous question. Rising prevention action and education is crucial, yet still insufficient to truly change behaviour. Some say that it should be better coordinated, similar to road safety programmes. Although such an action can have a clear impact on the credulity of the most vulnerable users, the greed, vanity, and lust of human nature will always need to be reckoned with.

The majority agree that security related costs should be shared so that users alone are not burdened with the cost left to their own discretion. The use of security could be required by Internet service providers and software publishers. A first step would be to offer a series of practical advice, telling users *what to do in the event of*…, beyond the traditional awareness measures, communication, education, training, and ethics. The limit would be the

[44] According to question Q43: What factors are likely to influence the future victim behaviours: information, requirements, uncompensated losses, etc.?

schizophrenia of users who, in many cases, also participate in cybercriminal behaviour through illegal downloads, purchasing counterfeit goods and unhealthy curiosities.

Constraint Factors

To continue with the road safety analogy, most of the experts feel that it will be necessary to use restrictive measures with personal consequences in the event of proven negligence or non-compliance. The goal is to build accountability among users of technological tools to help them avoid guilty behaviours for their own safety, including *limited compensation, penalties, obligations relative to the protection of information systems, reporting requirements,* etc. In the event of judicial proceedings, it might be essential to prove one's real security in comparison to the current standards of the profession. Some experts, however, are speaking out against what amounts to a second punishment, aimed a victims rather than at criminals.

The mass media turned out to apply more and more pressure by reporting on massive data leaks involving personal data and identifying responsible companies[45]. Leaders may have more reliable and shared information on cybercrime[46]. Other, more involved, public policies could be considered[47]*.* Digital security could become one of the government's primary goals, ensuring a number of effective obligations. The country would benefit from it for the safety of its own systems.

References:

CSIS (2008): Securing Cyberspace for the 44th Presidency, CSIS Commission on Cyber-security, US Center for Strategic and International Studies, Washington DC, December.

Symantec (2010): Norton's Cybercrime Report: Impact on Victims.

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France).

4.4.Victims by Age Distribution

This section presents the analysis of the prospective description of changes in the distribution of the most often affected individuals by age range, during the 2011 to 2020 decade[48].

All People

The experts do not expect any real change to the age ranges that are targeted by cybercrime in the short term. The arrival of younger generations changes nothing, because they also adopt high-risk behaviours. The most vulnerable age ranges are at the two extremities of the age pyramid, where there is less maturity with regard to the use of digital technology. Some experts point out that – *what is more revealing than age ranges* – is **the situation of weakness**, *whether physical, psychological, or intellectual,* representing preferred targets. In addition to the youngest and oldest members of our population, there are also the most socially excluded and isolated people, the most disadvantaged and least receptive populations to accepting advice, building awareness, and processing information.

[45] See the current case in the USA involving bank data and public trials.

[46] For example, the publication on the current status of the main types of incidents and vulnerabilities, based on standard indicators.

[47] For example, the English government's plan to rid its IT inventory of the threat of botnets.

[48] According to question Q44: What changes will there be in the age ranges distribution of the most commonly affected individuals?

The Youngest people

The youngest users are between 10 and 20. Although they are "digital natives" and appear to be trained on how to use technology, they are still *young and carefree, attracted by things that are forbidden and risky. They have an insatiable curiosity and naivety, a need to assert themselves, and a high-risk mixture on social networks.* The current habits of adolescents include sharing massive amounts of information about their personal lives, which is not offset by risk awareness and weaken them facing potential aggressors. As the executives of tomorrow, holders and responsible for sensitive information, there is a need to improve their high-risk behaviour.

The Oldest people

For **senior citizens over the age of 60,** there is a constraint – not a desire – to use ever present digital technology, which leads them into many high-risk situations in an environment they scarcely understand. Their demographic will be highly targeted. It is vulnerable and growing, and they will particularly be the victims in cases involving a breach of trust or fraud.

References:

www.bva.fr/administration/data/actualite/actualite_fiche/193/fichier_cp_genetic_juin2010_vf902af.pdf
www.tns-sofres.com/_assets/files/2010.05.27-enjeuxnumeriques.pdf

5. MEASURES

5.1. Applying Corporate Security

This section presents an analysis of the description of companies trend to apply security standards and to control the implementation of measures and procedures, during the 2011 to 2020 decade[49].

Expected Improvements

Companies mainly operate according to their return on investment. Security standards will be better applied and controlled if their benefits can be clearly identified – *considering the balance between perceived encountered risks and the cost of precautionary measures*. Currently, this is very difficult to do without a complete assessment of computer incidents.

However, collected pressures are also revealing significant improvements in the ISS's assessment, which is expected to continue under the influence of outside constraints[50]. Based on a theoretical assessment of computer system security policies, the reported progress went from 55% in 2008 to 73% in 2010 in 350 surveyed companies.

Most experts believe that large companies and high-risk industries – *finance, services, telecommunications, manufacturing, transportation, and energy* – should be at the forefront, followed at a slower pace by SMEs, who are more hesitant to implement a complete strategy. Outsourcing and cloud computing could be a strategy for avoiding the issue, without actually providing a solution or applying an internal security policy that is consistent with all of the services implemented at various levels.

External Requirements

This increased awareness has already led to the introduction of monitoring, prevention, and incident management procedures, along with compliance with standards already established for the business. This will be especially so, given the need to implement protective measures involving business resumption plans or business continuity plans[51], combined with backup resources and data backup plans.

Quality and relevance of standards and guidelines are added to this major trend and they are continuing to expand due to their growing specialisation in some domains, including *ISO 27002, ISO 2000, ITIL, PCI DSS, Basel 3, Solvency 2, guidelines issued by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), and European standards.*

Among the outside pressures are the legal framework of the most sensitive activities and the security demands expressed by consumers, regulatory authorities, and partners for all sectors to apply security standards which provide a competitive advantage. In some cases, they may mean that *a certificate is required for some contracts, and advertisement focuseing on quality*. For some experts, this is a condition of survival in the mid-term. Insurance companies could also influence this by requiring increasingly stricter and stricter

[49] According to question Q51: What trend will companies follow in terms of applying security standards and controlling the implementation of corresponding measures and procedures? *Answer by business category and socio-economic sector*.

[50] This improvement was highlighted in the 2010 annual survey on computer threats and security practices, written and published by the Club de la Sécurité des Systèmes d'Information Français *[French Information Security Club]* (CLUSIF).

[51] BRP: business resumption plan; BCP: business continuity plan.

protective measures in order to qualify for compensation. To prevent costly technological outbidding, there could be a general regulation on the minimum objectives for protection, which could effectively clarify the situation. One expert, however, points out that this approach is – *not necessarily guided by a search for maximum protection, but rather by compliance with an external obligation*. It does not garanty monitoring or internal control over time because of a lack of appropriation by the governance and staff members.

References:

Clusif (2010): Menaces informatiques et pratiques de sécurité en France (Computer threats and security practices in France)*; et seq.*
Deloitte (2010): Technology predictions.
Guinier D. (1994): Catastrophe et management – Plans d'urgence et continuité des systèmes d'information (Managing disasters – Disaster recovery and business continuity plans for IT systems), Ed. Masson, 336 pages.
Guinier D. (2006): Dispositif de gestion de continuité – PRA/PCA: *une obligation légale pour certains et un impératif pour tous* (Continuity Planning – BRP/BCP: *a legal requirement for some and a vital necessity for all*). *Expertises,* no. 308, Nov. 2006, pp. 390-396.

http://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9
www.cigref.fr/cigref_publications/RapportsContainer/Parus2010/Position_CIGREF_sur_le_Cloud_computing_Septembre_2010_CIGREF.pdf
www.marchesetcontrats.fr/index.php?option=com_content&task=view&id=2689&Itemid=2

5.2. Response Adaptability to Cybercrime

This section presents an analysis of the prospective description of how to adapt our institutions scheme and training to respond to cybercrime in its diversity, during the 2011 to 2020 decade[52].

Awareness, Education, and Training

Most experts focused on the issue of training, identifying a crucial element of the handling of cybercrime, along with awareness and education.

With a few exceptions, the consensus is that there is currently inadequate training in place, whether in initial training or ongoing training, aimed at top management or everyone in general. With the boom in digital technology, this assessment could be handled by the education system, which is gradually adding modules to build security awareness and the protection of information and computer systems. However, some experts have questioned the importance of these modules, pointing out that there is often only a relationship between the child and the machine and that the schoolmasters teaching this module are not necessarily up-to-date on the technologies being discussed.

Experts are calling for continued efforts and the systematic integration of these issues into school curriculums in order to educate the entire population. A more in-depth training may be required for managers and decision-makers, following their initial training, with regular updates. Specialised technicians should receive updated training each year. Implementing specialised training aimed at the legal system, including the courts, law enforcement, and

[52] According to question Q52: In what ways can our current institutional and initial training plans be adapted to respond to all aspects of cybercrime, *from ordinary risk to cyberwar*?

legal experts, bring an added value. These should be expanded. If good training currently exists, it should be expanded over the next decade using a few pilot projects.

Reorganization of Institutions

Some experts expressed their views on institutional changes, pointing out that the 2008 White Paper on national security and defence led to a reorganization of state activities in order to protect vital infrastructures against cyberattacks (*Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), "Piranet" plan and exercises, Observatoires Zonaux de la Sécurité des Systèmes d'Information (OZSSI))*. Law enforcement officialsand the court system are steadily building awareness among their staff through an evolving legal framework, resulting in a better understanding of cybercrime. Experts frequently mentioned *cyber-infiltration and digital identity theft*. Multidisciplinary training are developed to bring together barristers, representatives from the private sector, specialised investigative services, and magistrates to share their knowledge and experience.

However, there is not necessarily a balance between willingness, political positions, and actual means in place. Currently, only 0.2% of law enforcement employees have the technical qualifications to conduct digital investigations.

There are two reported problems. Firstly, the call to battle among state services should not hide the fact that security is everyone's business and everyone's responsibility. Security should be considered a component of all businesses, and public/private partnerships should strengthen, with some even advocating "leadership" from the more responsive private sector. Secondly, regardless of the qualities of the national systems, cybercrime could only be fought through global action.

Offensive Posture

Beyond the mainly defensive stance emerging, with additional strengthening of all levels of infrastructures[53] and the integration of crisis management responses, some experts would also like to see an offensive response to cyberwar – *with recruitment, training, the development of special tools* – and discussion on issues such as deterrence, self-defence, and law and order in cyberspace.

References:

http://userpage.fu-berlin.de/~jmueller/its/conf/Madrid02/abstracts/Ghernaouti-Helie.pdf
www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1101&Itemid=57
www.bestpractices-si.fr/index.php?option=com_content&task=view&id=1022&Itemid=93
www.ined.fr/fr/pop_chiffres/france/structure_population/regions_departements/
www.mcafee.com/fr/local_content/reports/virtual_criminology_report/virtual_criminology_report_2009_fr.pdf
www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf

[53] Including space satellites and data centres.

5.3. Minimizing the phenomenon

This section presents the prospective analysis concerning the fastest measures that can be taken to reduce cybercrime, during the 2011 to 2020 decade[54]*.*

The Need for an Appropriate Culture

Some experts did not feel that there is a reason to distinguish the impact of the measures according to whether they apply to individuals or organizations, since organizations are made up of individuals and because they believe that the most important measures apply to both.

Therefore, in the continuity of the previous question, **unanimity** is essential to the basic development of training and building awareness. Educating users on digital risks and on their personal responsibilities is an essential condition to understand all the other possible measures. There must be a broad culture of security, whether it is defensive or offensive in a cyberwar. It is possible to rely on an internal organization that is designed to protect the security of sensitive information. Some countries have already started to train specialists for this purpose.

Organizational Measures and their Sharing

Organizational measures are **especially highlighted at the state level**, whether related to the institutional positioning of pilot organizations in the fight against cybercrime or the need for national coordination to be more assertive with a cross-state mission that is generally valued as being essential, given what is at stake. This approach is combined with the call for a more effective public policy that is less declaratory, using financial and human means to address the magnitude of the threat. The complexity of investigations that the police will face regarding anonymity and cryptography will require more state-of-the-art expertise. New investigative means will have to be invented from a technical, ethical, and legal perspective. In the meantime, efforts to share best practices through guides and forums should be continued and intensified.

Finally, **some experts** mentioned the sharing of the burden with the private sector in the fight against cybercrime. They specifically mentioned a regulatory framework that is increasingly strict for access providers in terms of traceability and identification requirements, security standards for software developers, and commitment to responsibility affecting commercial sites. Internet service providers will have to comply with more and more draconian requirements to save data and protect users.

Legislative and Technical Measures

There is a debate over legislative and technical measures. **Some experts** feel that the legal boundaries and regulatory arsenal is satisfactory, but underused and generally unenforceable outside of the country. It would be relevant to make the texts consistent and more widely known. **Others** believe that it is inevitable or at least desirable to develop a law within the French Criminal Code and the Code of Criminal Procedure. The result of this would be greater transparency in identifying and reporting cybercrimes. It would also provide for the procedures and resources to be allocated to law enforcement officials to intercept and infiltrate, while still reinforcing privacy and personal data of users. As for technical devices,

[54] According to question Q53: What will be the legislative, political, technical, organizational and human means that can most quickly minimize cybercrime? *Distinguish between individuals and organizations.*

although they need to be improved, it will always be possible to circumvent them and they will remain too costly for ordinary users.

Conditions for Success

Regardless of the measures used, one of the highlighted conditions of success is their **application at an international level**. There is a priority on developing a common ground for devices, cooperation, and data, and on re-establishing the 24/7 network for sharing information and alerts, preventing cybercriminals from having a "*digital paradise*". For this purpose, there should be discussion over cyber-borders.

On an international level, it should be emphasised that there is currently only the Budapest Convention issued by the Council of Europe that can be enforced. The Council of Europe should continue its expert "Octopus Interface" meetings[55], which are annual meetings to discuss emerging issues, such as data outsourcing and privacy protection. However, this instrument is being contested by important countries, such as China and Russia, which are arguing for a universal convention. In January 2011, the UNODC[56] initiated an international study on cybercrime that could potentially result in a universal legal framework. At a European level, several directives are being negotiated to provide a community response. **These initiatives encourage people, provided that they are put into concrete actions**.

References:

INSEAD (2009): Safeguarding the Corporate IT Assets, Micro Focus

www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_fr.pdf
www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf
www.marchesetcontrats.fr/index.php?option=com_content&task=view&id=1804&Itemid=80

5.4. Partnerships and Cooperation to be Developed

This section presents the analysis of the prospective description of the partnerships and cooperation to be developed at various levels, during the 2011 to 2020 decade[57].

Public-Private Partnerships and Initiatives

Experts all agree that the fight against cybercrime involves a joint effort and the pooling of resources, bemoaning a lack of initiative in this field. Addressing cybercrime requires extreme responsiveness in order to offset the volatility of data and traces in cyberspace.

The public-private partnership (PPP) seems to be the most promising by sharing the financial burden, as well as the available information. **Various initiatives**, such as R2GS, OCTOPUS conferences, the international forum on cybercrime (FIC), and the Upper Rhine forum on cyber threats (FRC), are aiming to encourage group discussion and shared expertise.

[55] Within conferences organized by the Council of Europe’s Economic Crime Division and its General Directorate of Human Rights and Legal Affairs.

[56] United Nations Office on Drugs and Crime.

[57] According to question Q54: What partnerships will be developed on a national, European, and international level? *What kind of public/private, citizen, and legal cooperation will be developed?*

The PPP appears to be highly relevant in researching and developing countermeasures and detection tools with companies working in the area of information technology and communication with private think tanks and laboratories.

However, several experts point out that this partnership needs to be balanced and that protocols need to be established to form relationships based on trust and confidentiality in order to improve information sharing and operational collaboration (*investigations, traceability, alerts, crisis management*) with private partners, which are often English-speaking.

Think Tanks and Incident Response Centres

Information technology think tanks and incident response centres are key players that are only beginning to respond to requests by law enforcement officials. Legal authorities will have to be able to count on their ability to identify, report, and stop incidents and their ability to store data. These engineer networks and partnerships can take down[58] any server anywhere in the world within less than one hour by contacting the hosting providers and Internet service providers in order to stop the fraud.

It is important to establish a relationship based on trust and to convince legal authorities of the information value sent by these centres. The state think tank CERTA[59], *which is under the authority of ANSSI*[60], and the other CERTs[61] are already in cooperation with the OCLCTIC[62] and are providing valuable information to help fighting cybercrime. European experience in training, with 2CENTERS[63] centres of excellence and their networking is turning into a path to be followed with interest. Mixing these different worlds is mutually beneficial in terms of approach and handling of the threat.

International Cooperation and Exchange Bodies

Citizen response also seems to be getting stronger through the establishment of exchange bodies, such as the rights forum on the Internet or reporting tools that allow the user to play an active role in being vigilant, while ensuring a balanced response in terms of protecting individual rights.

Nascent **international cooperation** is still a key element with a wide freedom of improvement. The strengthening of the threat will make it imperative to the risk of a digital disaster. National and European boundaries are gone in the fight against cybercrime. There are already international partnerships in place in terms of police cooperation, with INTERPOL, EUROPOL (*European Police Office*), and the G87/H24 network. Legal authorities are expected to develop relationships with private, national, and international CERTs (*Centres d'Experts et de Réponse aux Incidents liés aux Technologies de l'Information*) in order to increase responsiveness to generally offshore incidents. Some experts, however, believe that it will be impossible to cooperate with some rogue countries.

[58] Stop of harmful activity

[59] State think-tank responsible for responding to and handling attacks.

[60] National Agency for Information System Security.

[61] Think tanks and incident response centers specialized in information technology, such as CERT-SocGen *(CERT for Société Générale)*, CERT-Lexsi, and others.

[62] Office Central de Lutte contre la Criminalité des Technologies de l'Information et de la Communication.

[63] 2CENTERS brings together universities, NTECH companies, and law enforcement.

References:

www.2centre.eu
www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_fr.pdf
www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf
www.fic2010.fr
www.foruminternet.org

CONCLUSION

The analysis of the experts' independent responses results in a broad consensus. It provides rich and abundant indications regarding everyone's sensitivities. This also provides a prospective view of trends in cybercrime between now and 2020 through its various components, including threats, attacks, authors, victims, and measures. Everyone agrees that **cybercrime will play a predominant role in the spectrum of conventional crime**, while security will be a recurring problem.

Whilst the conclusion from the last prospective analysis prior to 2005[64] proved to be correct with regard to computer security, it is worth noting that this analysis reveals many similarities. However, there are new features and an increase in the fast development of information and communication technologies. Some are due to their widespread use and border-less services, while others are related to the rise in organized crime. Organized crime networks can be developed at a global scale while sidestepping geographical and legal constraints. They will also be seeking powerful structures for seizing new opportunities, diversifying, and facilitating their criminal activities with large-scale operations *such as financial and economic fraud and money laundering* and more real-world activities *such as prostitution, gambling, illegal sales, and counterfeiting*, which will be hosted virtually and operated over the Internet.

The founding principles of the Internet – namely interoperability, openness, and neutrality – are fast to develop, but they become an economic, political, and geostrategic risk, with emerging drifts and monopolies. Global governance at an international scale should promote regulation and security, protect the interests of governements, businesses, and citizens, and fight against cybercrime, while avoiding cyberwars where the first virtual manoeuvres already appear. Terrorism could also exploit various weaknesses and develop methods to apply them with a considerable impact. Also, regardless of the quality of the system, **cybercrime can only be confronted at a global level**.

Main Focus

Emerging **threats** affect data, transactions, systems, infrastructures, and strategic services, while innovations are subject to vulnerabilities and misuse. Various factors play into them, some of which are recurring and others are specific to crises, increased competition, and new uses that expose new risks. Threats to organizations, businesses, communities, and countries will be unavailability, data attacks, and image attacks. Changes in social networks, along with an increasing interest among users, will certainly generate threats against individuals, businesses, public organizations, and governments. Trouble exists in managing crises and the possibility of paralysis. Threats to individuals will include scams and abuses, data theft, identify theft, intrusions, and fraudulent use of personal data.

Attacks include identity theft and fraud, especially through social engineering using powerful methods and tools, such as botnets, phishing, and spam in order to commit other offenses. Child pornography is expected to change in the way images and videos are exchanged, with greater availability and more discretion. Critical infrastructures will be targeted for various reasons. In this case, attacks could cause unprecedented crises at multiple levels. Reputational damage is expected to grow, and intellectual property theft and counterfeiting will become common, with intellectual property violations. Aggravating factors were listed, relating to their various goals, mostly linked to seeking profit and power. There is also a possibility of compromising fragile countries, with the temptation for others to initiate attacks with devastating consequences for these countries.

[64] Prospective analysis covering 1991 to 2005, Rosé P. (1992), pp. 137-142.

Authors will be variably both internal and external. Most of the experts agree to a strong trend related to the industrial organization of cybercriminal activities, based on elements borrowed from the world of commerce, with skill networks that will sell to the highest bidder. There will also be crimes that take advantage of mass opportunities involving scams and the development of social networks as new reaches of influence. Groups of hackers and activists will also represent increasing threats, often seeking media recognition for their actions over the Internet, such as to gain support for their actions. Changing skill levels are expected to distinguish criminal groups specialising in reselling services, and others, more diversified, users of those services or working for the benefit of some more important than themselves. Advanced legal and financial skills will also be needed for carrying out money laundering and actions to protect originators. Despite their size, organized crime groups will remain as discrete as possible so that they can continue operating.

Victims will come from all sectors where strategic information and financial issues exist. The IT and telecommunications sector appears to be a prime target, with its ability to destabilise a society that is highly dependent on such technologies. Sectors already being targeted are those that promise a potential for monetary gain or disruption. Distinctions are made based on the goal of attacks, such as whether that are acute attacks against a leading company and finance organizations or general attacks against online transactions that will be frequently and heavily attacked. Or perhaps they seek to cause destruction and to create as much disorder as possible in order to achieve the greatest media impact. As for age ranges of individuals, the most vulnerable are those at both ends of the spectrum, who lack maturity in how to use digital technology. They are physically, psychologically, or intellectually weak, which makes them preferred targets. Added to the young and old are people who are alienated and isolated, the most disadvantaged populations, the disabled and less responsive.

Measures include the legal framework governing highly sensitive activities and security requirements from various sources, including insurance companies. This would favour the implementation of consistent security measures, based on the application of security standards and policies and based on certifications with a guarantee of monitoring and internal control in the long run. Everyone agrees about the need for training and awareness programmes, and there is a consensus on deficiencies and the need to be integrated into curriculums. High-level training should become commonplace over the next decade, based on pilot projects and on the white paper on security and national defence to protect vital infrastructures. Beyond the defensive positioning, there is a desire for a discussion to develop an offensive positioning. Organizational measures are implemented at the state level, while legislative and technical measures are a larger debate. The public/private partnership seems promising, along with the existence of think-tanks and incident response centres, not forgetting a citizen response that has an active role in being vigilant. Large companies and highly sensitive sectors are expected to be on the forefront, followed by SMEs, who are more hesitant to implement an appropriate strategy. Finally, the establishment of a universal legal framework is key, along with a common ground for devices and cooperation at the international level and at the public/private level.

Appendix 1: METHODOLOGY

The ***Delphi method*** *is applied in order to highlight* ***the convergence of opinions****, to reach a certain degree of consensus, and to glean as much information as possible on* ***trends in cybercrime over the next ten years*** *(2011-2020).*

Delphi[65] **was applied** by involving a **panel of French-speaking experts** of different origins, including cyber-investigators, IT security experts, and other specialists, including lawyers, magistrates, and others. These experts independently responded to a **questionnaire** to make their judgements in several rounds, during which time each expert was asked to pursue or reformulate his or her opinion, in the light of **entirely anonymous responses in order to avoid the leadership effect**. The goal of this iterative process was to reduce dispersion among the responses and to identify the middle ground. This generally lead to a consensus, but also to obtain richer and more detailed information. **The systematic use of electronic means** makes exchange of ideas easier with little cost and correspondence time.

Phases of the Delphi Method

1. The preparatory phase consists of two parts

- **The selection of experts**, based on their skill, experience, foresight, and independence, in order to have a final panel of 20 to 30 people who are formally committed,
- **The development of a questionnaire**, with specific, yet open-ended questions that could be as quantified and independent as possible.

2. The questionnaire phase in three rounds

- **During Round 1**, the questionnaire is sent to the experts, specifying the object of the method, practical conditions,, the deadline for responses, and anonymity. Each expert describes his response, based on his own level of expertise relative to each question.
- **During Round 2**, each expert is given anonymous responses in a summarized form and must approve, clarify, even change his previous response. They must justify their opinion if it is much different than other's opinions, estimating their ability to judge each question.
- **During Round 3**, each expert is asked to comment on deviant arguments and to give their final response, given a median consensual opinion or a disparity of opinions.

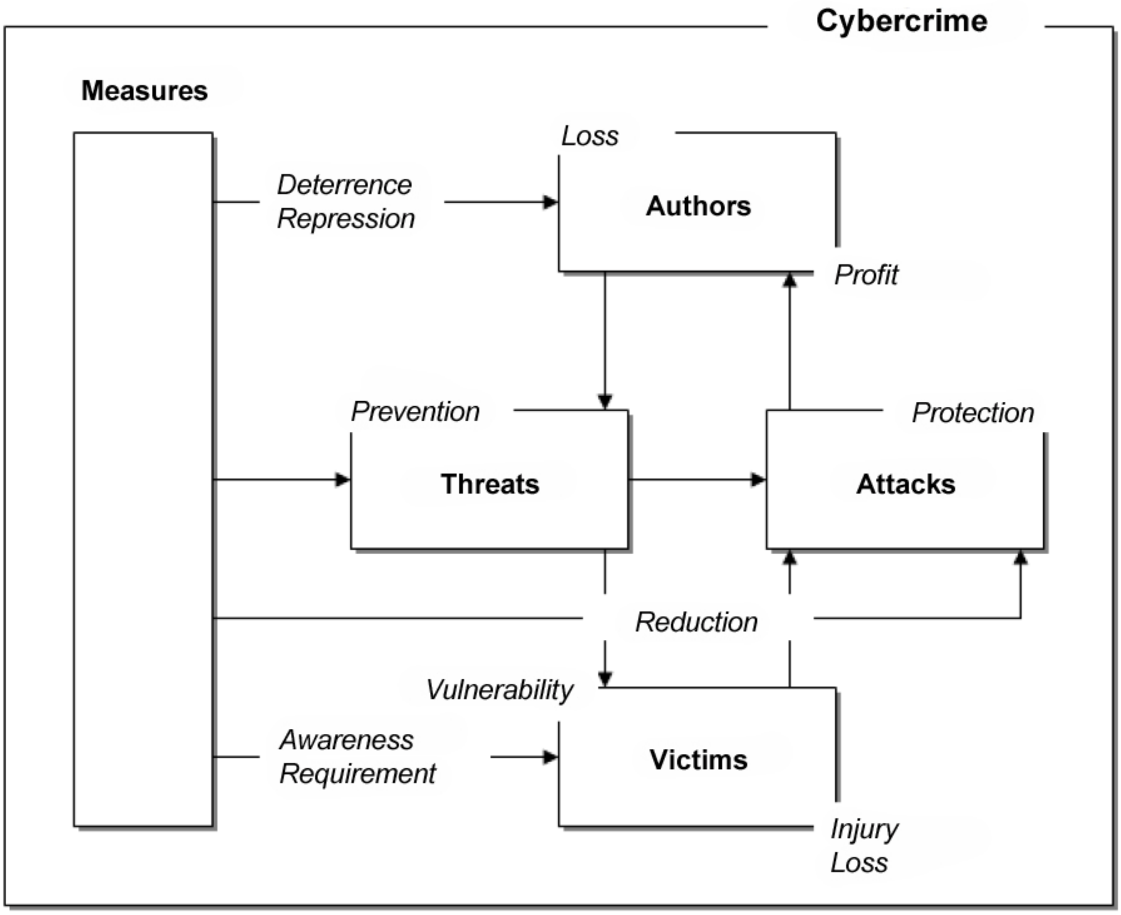
3. The final phase

- **Tallying of responses and final use** of the study,
- **Summary and formatting** for distribution,
- **Distribution** of the final study.

[65] See also Rosé P. (1992), pp. 30-32.

Thematic Model of the Questionnaire

In order to develop the questionnaire while maintaining as much independence in the questions, these questions were developed on a thematic model presented on the following scheme with the relative entities, their relationships, and some attributes:



This enabled to **design the questions around the following five chosen themes**:

- **Threats** that result from a removal, destruction, disruption, interruption, modification, disclosure, interception, or damaged image,
- **Attacks** that result from infrastructures, hardware, software, data, or reputation,
- Cybercriminal **authors** of criminal attacks,
- **Victims** who, due to vulnerabilities, are harmed by threats that lead to attacks,
- **Measures** aimed at reducing cybercrime, such as legislative, political, technical, organizational, and human measures, including cooperation and coercion.

The scientific committee developed four questions for each theme, along with three general questions about cybercrime and its evolution at the start of the questionnaire.

Appendix 2: ORGANIZATION

The study is organized around a scientific committee and a summary drafting committee for arranging and coordinating the interactions with the experts.

Scientific Committee of the Study

This committee is responsible for approving the proposed method, based on a schedule, researching experts, and the sending and receipt of the documents.

- **Lieutenant-Colonel Eric FREYSSINET**, head of the Anti-Cybercrime Division, Technical Department on Legal Research and Documentation, Legal Division of the Gendarmerie Nationale.
- **Mr Daniel GUINIER**, PhD in Computer Science, CISSP, ISSAP, ISSMP, MBCI, expert witness for the International Criminal Court of The Hague, Lieutenant-Colonel (RC) of the Gendarmerie Nationale.
- **Mr Philippe ROSE**, PhD in Economics, journalist, writer, editor-in-chief of Best Practices Systèmes d'Information, editor of IT Business Review.
- **Lieutenant-Colonel Dominique SCHOENHER**, regional intelligence and economic security correspondent for the Nord-Pas-de-Calais Gendarmerie[66].

Summary Committee

This committee is in charge of writing the different summaries in order to draw up a final document based on the questionnaires returned by the experts.

- **Mr Daniel GUINIER[67]**, PhD in Computer Science, CISSP, ISSAP, ISSMP, MBCI, expert witness for the International Criminal Court of The Hague, Lieutenant-Colonel (RC) of the Gendarmerie Nationale.
- **Mr Philippe ROSE**, PhD in Economics, journalist, writer, editor-in-chief of Best Practices Systèmes d'Information, editor of IT Business Review.
- **Lieutenant-Colonel Dominique SCHOENHER**, regional intelligence and economic security correspondent for the Nord-Pas-de-Calais Gendarmerie.

Experts Participating in the Study

These experts formally committed to participating in the study. They are responsible for returning their questionnaires on time, in three rounds.

- **Mr Laurent BOUNAMEAU**, Federal Computer Crime Unit, Belgian Federal Police.
- **Mrs Sylvia BREGER**, criminologist, director of CRIMINONET.
- **Mr Alain CORPEL**, ISS teacher and researcher at the Université Technologique de Troyes (UTT).
- **Mrs Chantal CUTAJAR**, adjunct professor at the Ecole de Management de l'Université de Strasbourg, directory of GRASCO and Master: Fight against economic and financial organized crime, Lieutenant-Colonel (RC) of the Gendarmerie Nationale.

[66] Responsible for the anonymous distribution of responses to the community for summarisation.
[67] Also in charge of preparing the final document to be submitted to the ad hoc committee.

- **Lieutenant-Colonel Eric FREYSSINET**, head of the Anti-Cybercrime Division, Technical Department on Legal Research and Documentation, Legal Division of the Gendarmerie Nationale.
- **Mr Gérard GAUDIN**, Supélec engineer, founder of R2GS, security management consultant.
- **Mr Daniel GUINIER**, PhD in Computer Science, CISSP, ISSAP, ISSMP, MBCI, expert witness for the International Criminal Court of The Hague, Lieutenant-Colonel (RC) of the Gendarmerie Nationale.
- **Mr Joseph ILLAND**, general engineer of weaponry, defence security official for CNRS.
- **Chief Warrant Officer Thierry JACQUOT**, NTECH investigator, BDRIJ of Strasbourg.
- **Mr Philippe JOLIOT**, engineer, expert witness for the Court of Appeals of Nancy, TRACIP, president of the AFSIN.
- **Mr Denis LANGLOIS**, engineer, cryptologist, safety and security consultant for tangible and information assets.
- **Mr Bertrand LATHOUD**, Information Risk Manager for PayPal.
- **Captain Olivier NAEL**, head of the technical section, OCLCTIC.
- **Mr Jean-François PACAULT**, general engineer of weaponry, head of the communication and information technology security department for a senior official of defence and security for the Ministries for the Economy and the Budget.
- **Mr François PAGET**, secretary general of CLUSIF, cybercrime researcher, founding member of McAfee Labs.
- **Lieutenant-Colonel Alain PERMINGEAT**, head of the anti-cybercrime division of the technical department of legal research and documentation.
- **Mr Jean-Paul PINTE**, PhD in scientific and technical information, lecturer, standby intelligence expert at the Université Catholique de Lille, Lieutenant-Colonel (RC) of the Gendarmerie Nationale.
- **Ms. Blandine POIDEVIN**, attorney in Lille.
- **Mrs Myriam QUEMENER**, magistrate to the general prosecutor of the Appeals Court of Versailles.
- **Mr Philippe ROSE**, PhD in Economics, journalist, writer, editor-in-chief of Best Practices Systèmes d'Information, editor of IT Business Review.
- **Mrs Isabelle TISSERAND**, PhD in EHESS, coordinator of the European Circle of Information System Security.
- **Chief Warrant Officer Franck VAN DE VELDE**, NTECH investigator, BDRIJ of Villeneuve d'Ascq.

Appendix 3: QUESTIONNAIRE

General Questions on Cybercrime and its Evolution

Q01: How would you redefine or clarify the areas of illegal activities and redefine the term "*cybercrime*" for the next decade?

Q02: What place will cybercrime have and how will it be related to other forms of crimes and offenses, including *counterfeiting, financial and economic crimes, child pornography, drug trafficking, human beings trafficking, terrorism, and other crimes*?

Q03: What will be the overall impact of technological changes and breakthroughs, including *cloud computing, virtual systems, mobile systems, cryptology, steganography, and malware, on the control – or rather on the rise – of this phenomenon*?

Questions Organized by Theme

Theme 1: Threats

Q11: What are the emerging threats and the new expected forms of cybercrime, along with their level of sophistication?

Q12: What will be the most serious threats to organisations, such as businesses, communities, and government services? *Three threats per category of organization.*

Q13: How will threats to personal assets and information develop?

Q14: What changes can be expected in the distribution of threats to the confidentiality, integrity, availability, and accountability of *information and systems*?

Theme 2: Attacks

Q21: How will the distribution of attacks change, both in terms of number and severity, given the offense, including fraud, interception, data theft, intellectual property violations, identity theft, child pornography, e-reputation, etc.? *Distinguish between individuals and public and private organizations, specifically noting whether the attacks to critical infrastructures (ex. telecoms, power networks, etc.) may become a major risk*.

Q22: What will the aggravating factors be: dependency, crises, mobility, cloud computing, etc.?

Q23: What will be the main goal: financial gains or losses, damaged privacy, instability, disorganization, misinformation, destruction, terror, etc.?

Q24: Would it be possible to compromise the stability of countries?

Theme 3: Authors

Q31: What changes will there be in the origin of threats (internal, external and mixed)? *Provide the distribution in terms of percentages in 2010, 2015 and 2020*.

Q32: What will be the change in profiles of threat agents by category, including independent hackers, social groups, activists, organized crime groups, terrorists, governments, etc.?

Q33: What will be the change of skill levels and required resources for actions that are more or less serious, on a more or less large scale?

Q34: How will the importance of organized crime change? *Will it be a major player? Why? With what strategies?*

Theme 4: Victims

Q41: Which socio-economic sectors will be the most targeted: online finance and transactions, industry and transports, energy and defence, IT and telecommunications, services, agri-food industry, health, research, government and territories, etc.?

Q42: What changes will there be in the victim behaviours : reporting of complaints, protective measures, etc.? *Distinguish between individuals and organizations*.

Q43: What factors are likely to influence the future victim behaviours: information, requirements, uncompensated losses, etc.?

Q44: What changes will there be in the age ranges distribution of the most commonly affected individuals?

Theme 5: Measures

Q51: What trend will companies follow in terms of applying security standards and controlling the implementation of corresponding measures and procedures? *Answer by business category and socio-economic sector*.

Q52: In what ways can our current institutional and initial training plans be adapted to respond to all aspects of cybercrime, *from ordinary risk to cyberwar?*

Q53: What will be the legislative, political, technical, organizational and human means that can most quickly minimize cybercrime? *Distinguish between individuals and organizations.*

Q54: What partnerships will be developed on a national, European, and international level? *What kind of public/private, citizen, and legal cooperation will be developed*?

GLOSSARY

Computer attack: A generic term for a malicious action whose target and means involves computing.
Botnet: Network of malicious robots ("bots"), installed on compromised machines ("zombies"), in a number to ensure active camouflage and to direct its actions to one or more determined targets (ex. distributed denial of service (DDoS) or mass emails ("spam")).
CERT ("Computer Emergency Response Team"): Team assembled to report vulnerabilities and threats and to respond to attacks.
Confidentiality: Property of security associated with keeping a secret, with access only to authorised entities.
"Botnet" controller ("bot herder"): Individual responsible for remotely managing and monitoring a network of robots through a C&C Control and Communication server.
Trojan horse: Hidden malicious code that can take control of the compromised computer without the knowledge of the legitimate user.
Cloud computing: Method of processing client data, using the Internet, in the form of services provided by a service provider. This is done using a cloud computing model that provides access to a shared set of configurable resources over an on-demand network. Its resources include networks, servers, storage, applications, and other elements, arranged into "clouds" in various geographical locations, without the specific location or operation of the cloud being made known to clients.
Malicious code ("malware"): A program developed for the purpose of causing harm through a computer system or a network. *Trojan horses, viruses, and worms are forms of malware, characterised by the presence of propagation, triggering, and action mechanisms that are often developed with an intent to cause harm.*
Cyberattack: A malicious act through a computing device, generally over a telecommunications network.
Cyberthreat: A local or remote threatening action targeting information or information systems.
Denial of Service (DoS): An action to prevent or greatly limit the ability of a system to provide an expected service.
Distributed Denial of Service (DDoS): An action launched from multiple sources, especially by means of a botnet.
Defamation: An allegation or charge made in bad faith, undermining the honour, consideration, or reputation of the individual or legal entity being charged.
Availability: Security property associated with the proper delivery under the stated terms regarding times, deadlines, and performance.
Phishing: Misleading technique intended to obtain personal information by misleading the holders of that information.
Fraud: A deliberate illegal act carried out by one or more subtle means, with the intention to deceive in order to gain an advantage. This can take various forms, which may or may not require complicity, leading to injury to the victim.
Social engineering: A method of obtaining an asset or information by exploiting trust, ignorance, or credulity, or by applying psychological pressure or appealing to one's compassion.
Accountability: Security property associated with monitoring performed operations and functions, without possible repudiation.
Integrity: Security property associated with storing data and components without corruption in space and time.
Intrusion: Introduction and maintenance of a fraudulent character in a system for the purpose of retrieving or modifying, or else altering or destroying.
Pirated machine or "zombie": A machine compromised by a malicious robot ("bot") on a network ("botnet") directed by a "bot herder".
Hacker: An individual who breaks into a computer system for an intellectual challenge, with malicious intent, or for profit, acting alone or as part of a group.
Spam: Unsolicited email messages, often sent in large numbers.
ICT: Acronym referring to Information and Communication Technologies.
Address spoofing: The act of deliberately replacing one address with another address, such as a physical MAC (Medium Access Control) address, IP address, domain address, email address, etc.; similar to identity theft, listed as an offense under French criminal law.
Identity Theft: Temporary or permanent borrowing of a person's identity by appropriating the victim's identifiers. The Loppsi 2 law provides for a punishment of two years imprisonment and a fine of €20,000 for the crime of identity theft, digital or non-digital.

Also see: www.clusif.asso.fr/fr/production/glossaire/

Cybercrime evolves and grows over time, as new information and communication technologies (ICT) are introduced. Everyone involved in the fight against cybercrime need to understand it in order to anticipate their actions.

Twenty-two experts contributed to a prospective study on the decade from 2011 to 2020, based on an iterative process of electronic consultations, using the Delphi method and an open-ended questionnaire based on an ad hoc model.

Their combined analyses made it possible to form a consensus on the trends and changes affecting cybercrime between now and 2020, through a discussion of the threats, attacks, authors, victims, and measures designed to keep information, government services, business and individual security and to provide a national defence in order to protect basic services, critical systems, and vital infrastructures. The dissemination of the results of the study is intended to encourage discussion on the strategies and resources to be implemented by decision-makers. For this purpose, it was presented during the 4th Upper Rhine Forum on Cyberthreats FRC2011, held at ENA (Ecole Nationale d'Administration) in Strasbourg, France, on 9th November 2011, on the topic *"Cyberthreats at the horizon 2020",* organized by the Région de Gendarmerie d'Alsace and the reserve officers (RC) of the Gendarmerie Nationale.

McAfee Labs is pleased to present the translation of the results of this new French study on computer-related crime. This methodical and original research—based on the knowledge of 22 experts, including François Paget of McAfee Labs—explains the threats we face today and predicts what we might see in the years up to 2020. Armed with this expertise, we can more effectively protect ourselves against future cybercrime.

David Marcus
Director, Advanced Research and Threat Intelligence - McAfee Labs