Fundación Innovación Bankinter

FTF Future Trends Forum

25 English version

Cybersecurity, a worldwide challenge

The critical infrastructures of countries that are not prepared to defend themselves from cyberattacks should not connect their infrastructures to the network.

P. 26

Internet security should be guaranteed by the Government in the same way as electricity, which is a basic service.

P. 33

Authentication techniques must guarantee the protection of data, that is, they must protect the privacy of users using powerful encryption systems.

P. 38

The intention is that the data be monitored by the country that has them or its companies beyond national territorial boundaries.

P. 64

New computing capacity and “artificial intelligence”, which is becoming more powerful all the time, are allowing them to automate their attacks on a massive scale.

Acknowledgements

Our gratitude to **Ms. Amaya Quincoces,** journalist and author of this report. Without her collaboration were not possible the launch of this publication.

Our thanks to all of the Members of the XXV Future Trends Forum (FTF) who made the forum a success, and a special thanks to those who made contributions to this publication:

For their invaluable support in the composition of this publication:

Eden Shochat
Fabio Assolini
John Lyons
Caroline Baylon
Inbar Raz
Steve Wilson
Evan Wolff
Kevin Sale
Richard Parry

For their invaluable role in the methodology and organization of the Future Trends Forum:

Chris Meyer

The LUDIC Group

Garrick Jones
Clemens Hackl
Jake Holmes

DiBUJARiO

Fernando de Pablo

Finally we would like to thank the members of Fundación Innovación Bankinter team for their commitment and follow through in the development of the content of this publication:

Fundación Innovación Bankinter
Sergio Martínez-Cava
Marce Cancho
María Teresa Jiménez
Lara García de Vinuesa
Pablo Lancry

The views and opinions expressed in this report are those of the author and do not necessarily reflect the position of the experts that participate in the Future Trends Forum meeting.

Speakers and Assistants

Abdou Naby Diaw
Chief Security Office (CEO) Vodafone.

Carlos Jiménez
Founder and president of Secuware.

Caroline Baylon
Director, Cyber Security Research Programme, Center for Strategic Decision Research.

Drew Dean
Program director at SRI International.

Eden Shochat
Founder of Aleph and trustee of Fundación Innovación Bankinter.

Emilio Méndez
Director of the Center for Functional Nanomaterials (CFN) and trustee of Fundación Innovación Bankinter.

Evan Wolff
Partner in Crowell & Moring.

Fabio Assolini
Analyst of the company Kaspersky.

Fernando Vega
Information Security director at Bankinter Global Services.

Ilya Ponomarev
Russian member of Parliament, chairman of
the Duma Innovation and Venture Capital Subcommittee.

Inbar Raz
VP of Research at Perimeter X.

Isaac Gutiérrez
International Chief of Cibersegurity at Prosegur.

Jens Schulte - Bockum
Former CEO Vodafone Germany and trustee of Fundación Innovación Bankinterr.

John Lyons
Chief executive & founder at International Cyber Security Protection Alliance (ICSPA).

Julia Li
Founder and CEO of HCD Global.

Kevin Sale
IT Security specialist at King Abdullah University of Science & Technology.

Khoo Boon Hui
Former president of INTERPOL.

Michael Osborne
Manager Privacy and Security Cognitive Computing & Industry Solutions Department, IBM Research Division.

Michael Schrage
Research fellow, MIT Center for Digital Business.

Miguel Rego
CEO at IN CIBE (Spanish National Cyber Security Institute).

Philip Lader
Former non-executive chairman at WPP Group and trustee of Fundación Innovación Bankinter.

Ram Levi
Cybersecurity expert, CEO at Konfidas, co-founder at London Cyber Security (LCS).

Richard Kivel
Senior manager at Bridgewater and chairman at Rhapsody Biologics. Trustee of Fundación Innovación Bankinter.

Richard Parry
Principal at Parry Advisory.

Rolf Reinema
Head of Technology Field at Siemens.

Steve Wilson
VP & principal analyst at Constellation Research.

Tan Chin Nam
Senior corporate adviser and former permanent secretary. Trustee of Fundación Innovación Bankinter.

Wilfred Vanhonacker
Coca-Cola professor of Marketing, Olayan School of Business, AUB and trustee of Fundación Innovación Bankinter.

Thank you so much,
Fundación Innovación Bankinter

Index

Prologue by Eden Shochat

Founder of Aleph and trustee of Fundación Innovación Bankinter.

> The 2014 JPMorgan Chase cyber-attack compromised 83 million accounts of individuals and small businesses.

Investigators had uncovered a trail of 75 shell companies created by the four suspects, with activity going back as far as 2007, reaping "hundreds of millions of dollars in illicit proceeds"; In another incident, a group associated with the People's Liberation Army ran "Operation Aurora"- a series of cyber attacks targeting dozens of companies, including Google, Adobe, and Northrop Grumman (one of the manufacturers behind the F-35 stealth fighter). According to McAfee, the primary goal of these attacks was to gain access and potentially modify source code repositories at these high tech, security companies and defense contractor.

It is crucially important to understand that cyber warfare can also be used as a military weapon. More than 80,000 Ukrainian citizens suffered a power outage caused by a (never confirmed) Russian malware that took over the control centers of multiple power plants. The US Department of Homeland Security demonstrated, as early as 2007, how 21 lines of code can destroy a power generator. The attack of Stuxnet (a malicious computer worm) on the Iranian nuclear facilities demonstrated an actual live attack in the wild. This caused the US, and many other countries to create "Cyber Commands" for both defence and offense purposes.

We already pay for fraud through the fees for every transaction we make with our credit cards. The impact of these risks and threats is extremely broad. People fear identity theft and widespread "locked data blackmail", governments attempt to protect themselves against cyber-based spying and potential attacks on their critical infrastructure assets by other nation-states and corporates are burdened with financial loss and brand-destroying cyber attacks such as the one on Sony in 2015.

One of the biggest challenges defenders face is that attacks are rarely perpetrated within a single national border. The JPMorgan attackers were from Israel, Russia and possibly other countries. These cross-border issues make mitigation and prosecution hard (between western states) to impossible (if the attack is from another nation or one with lesser extradition treaties like China).

This is our reality today

The tomorrow is far more concerning. We have enjoyed speech and face recognition, autonomous vehicles and super-smart in-game opponents through advances in deep learning. These same strides in artificial intelligence (AI) could and will enable cyber attackers to target an attack on a significant number of high value targets and by that create a new form of advanced persistent threat. Basically, they will no longer have to choose between pin-pointed attacks of very specific high value targets and large-scale attacks of any number of vulnerable targets. This new generation of AI-based malware would be able to continuously evolve with new attack methods and never give up finding new vectors to reach a financial, military or other gain set by its operator.

These present and future scenarios emphasize the importance of being prepared. Cyber defense is notoriously hard since while the defender needs to succeed 100% of the time, covering all of the playing field, the attacker only needs to succeed once, usually at the point of least resistance.

This report by the Future Trends Forum includes recommendations about education, regulatory involvement (while trying to minimize risk of over-regulations) and the handling of enforcement challenges through cross-border collaboration.

We are sharing this report as one of the many steps required for education and as an instigator for further discussions. I hope you benefit from the information presented, even if daunting at times.

Bio

- **Eden Shochat** is a Bankinter Trustee. His passion is building "stuff", most recently Aleph, $150MM venture capital fund; The Junction, voted #1 startup program in Israel; face.com, a massive face recognition API acquired by Facebook; Aternity, the leading user-centric enterprise IT platform; and GeekCon, Europe's biggest makers conference. In his free time he teaches in the IDC Zell Entrepreneurship program.

Cybersecurity threats

1

Fabio Assolini
Analyst of the company Kaspersky.

John Lyons
Chief executive & founder at International Cyber Security
Protection Alliance (ICSPA).

Caroline Baylon
Director, Cyber Security Research Programme,
Center for Strategic Decision Research.

A new digital age opens with growing threats for worldwide security. Cyber felons have become a lot more sophisticated, organised and dangerous in their attacks, obtaining huge profits.

The phenomenon of connecting everything to the Internet, or the Internet of Things (IoT), is unstoppable, with increasingly abundant and cheap sensors that make the objectives of cyber felons easier to achieve, often protected in their undertakings by their own governments, which do not punish or pursue them. Furthermore, new computing capacity and artificial intelligence, which is becoming increasingly powerful, are allowing them to automate their attacks on a massive scale, using self-controlling computer networks that are able to make their own decisions.

Cyberwar, cyberespionage and massive surveillance are current threats, to which many others will be added. Beyond the countless economic and social advantages linked to the internet revolution, new dangers lurk in cyberspace: wars that could be fought by autonomous weapons or between machines and men, murders that could be perpetrated from the internet itself, major sabotage of countries' critical infrastructures. It seems that it will just be a matter of time.

Cyber Felons Profit from the Internet

1.1

▸ **The cybersecurity industry** handles multi-million budgets that are constantly growing. Each year the sector moves between 70,000 and 80,000 million dollars a year. By 2020, the figure is expected to be 2.5 times higher, according to **Khoo Boon Hui,** former President of INTERPOL (watch video).

Simultaneously, another very dangerous world is thriving: cybercrime, where cyber felons are attacking larger, more sophisticated and more organised companies and governments and are reaping profits in the millions. The economic losses it is already causing are enormous. Just last year, the figure was around 400,000 million US dollars, according to expert estimates, although it could be a lot higher, given that victims do not usually reveal details.

The boom in mobile phones, tablets and all types of sensors connected to the internet, the growing use of robots and increasingly powerful artificial intelligence systems, and more and more sophisticated automated learning machines connected to the internet make things more complicated. Cyberspace is receiving worldwide attention in view of the prospect of a likely growth in cybercrime, which is much more aggressive and even more lucrative for attackers.

Nobody is free from the dangers in cyberspace

Anyone can become a target of cyber felons. It can happen when paying with a credit card, when connecting to the Wi-Fi of a hotel, etc.

Cyber felons are always on the watch and they take advantage of any vulnerability in systems to access people's private data, which are dispersed in huge amounts throughout the Internet. This helps them improve their planning of crimes.

The inappropriate use of the "Internet of Things" poses a threat to both the digital and physical world. Terrorists and cyberattackers can manipulate the computer systems of national infrastructures that offer basic services to countries: electricity grids, telecommunications, banking, water, etc.

Khoo Boon Hui ▾
Former president of INTERPOL.

watch video

Several people have already died as a result of cybercrime. Some have committed suicide because their reputation has been tainted due to the unveiling of certain information; others because they have been extorted by cyber felons threatening to reveal sensitive photos on the Internet, as well as intimate sexual details.

Furthermore, cyber felons seem to have free reign to traffic without leaving a trail (weapons, drugs, children), acting from such "dark" environments as the Deep Web, which is an enormous, supposedly inscrutable, virtual space that escapes from the control of the traditional search engines, such as Google.

According to the former President of INTERPOL, "we are consumed by terrorism" on the Internet. The activity of conventional cybercriminals and professional cyber felons is increasing. Their actions can be masked in the Internet with much more ease than in the real world due to the absence of physical borders and because there is no international jurisprudence to penalise the cyberculprits.

Many States lack laws to punish these conducts and the felons themselves; from their own houses, and with a simple computer, they can attack objectives anywhere in the world. International cooperation is required against cybercrime beyond the work carried out by organisations such as the INTERPOL Global Complex for Innovation (IGCI) http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation and Europol https://www.europol.europa.eu/ and initiatives such as the Convention on cybercrime, also known as the Budapest Convention, which currently includes around forty countries.

Companies and governments that fight against cybercrime must share information in order to anticipate threats or to fight against them more efficiently when they are produced. "All international crime is a local crime somewhere", says the former President of INTERPOL. Every country should apply legislation against cyber felons within its borders and cooperate at international level when criminal offences go beyond them. The collaboration between governments and companies is essential, and public-private alliances are needed to share expertise and experience related to cybersecurity.

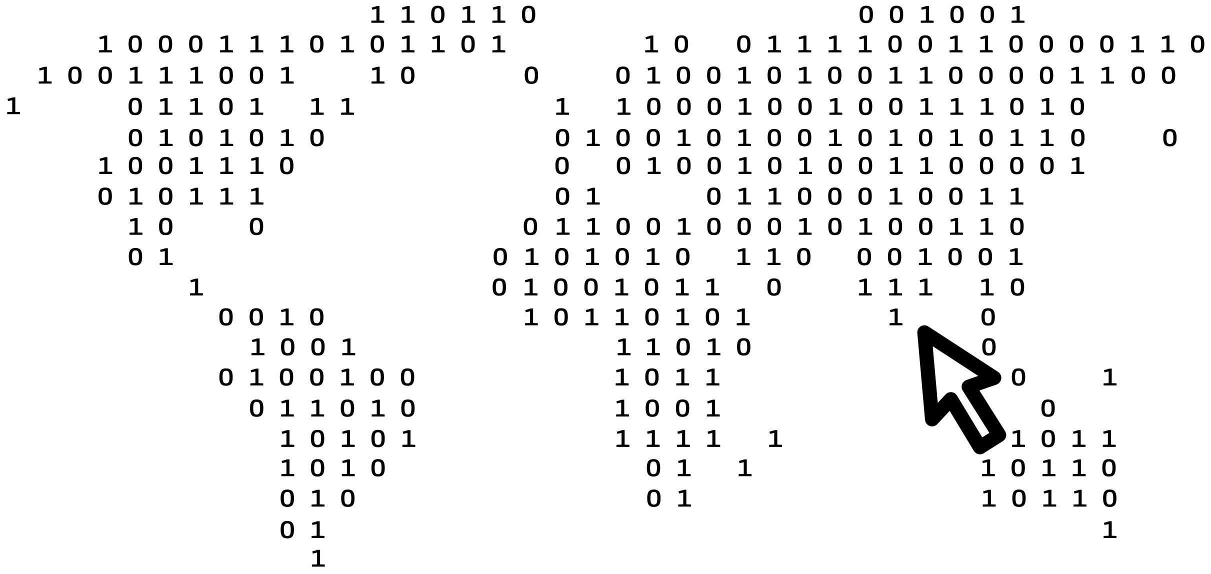
A forum of worldwide experts in cybersecurity

The former President of INTERPOL is one of a group of thirty international experts who have discussed the challenges of worldwide cybersecurity at the Bankinter Fundación Innovación Future Trends Forum – FTF https://www.fundacionbankinter.org/es during its twenty-fifth edition, which was held in Madrid in December 2015.

Coordinated by **Chris Meyer**, CEO of Nerve LLC, participants spent two days discussing the best way to move towards a safer world, and they succeeded in developing an ambitious, detailed list of proposals as a "road map", addressed to the different agents in the world dealing with cybersecurity for their possible implementation.

During the meeting held at the Future Trends Forum, the experts posed different hypotheses of how life would be in different models of society depending on the weight of some factors or others:

- In one of those worlds, privacy would be above everything
- The second one would be anarchic or libertarian in terms of laws
- In the third one, trade would take precedence over everything else
- The fourth one would be a closed system with absolute vigilance
- The last one establishes a parable on cybersecurity that poses which would be the consequences of a possible social and economic system controlled in the future by five major



technology companies: Microsoft, Apple, Google, Facebook and Alibaba, which has been called Magfa, as a result of their initials

The debates that took place contributed to shaping an image of the current outlook of security on the Internet and to identifying weaknesses and threats, as well as the countries' strengths to face them, with the purpose of presenting possible solutions aimed at improving cybersecurity. These solutions would focus on all levels of society: governments, legislators, consumers, companies, industry, educators, etc.

How to move towards a more secure world

Experts believe that the measures that can be adopted from now on will contribute to improving the world's security in the future. By 2020, they expect to reach certain landmarks: quality standards that guarantee the generalisation of secure software; better security strategies in work; an interconnected world with more protection for consumers; and greater awareness on cybersecurity. In addition, secure digital trade in all types of transaction; better digital authentication techniques with the purpose of guaranteeing privacy, for example, in medical records, which will be a critical area; and more global cooperation and international laws that ensure the enforcement of sentences on cyber felons.

Looking further ahead, to 2025, the participants expect that companies will assume more responsibility in terms of security; consumers will be provided further support in online security and they will have enough quality information at their reach to know how to carry out virtual transactions in a secure manner. In addition, the governments are expected to interact virtually with the citizen with further normality, and certain groups that by then could be already digitised, such as refugees or monks that currently live in isolation, will also have access to educational campaigns to learn how to use the Internet safely. By 2030, one of the key objectives is to guarantee secure financial transactions on the Internet, with the public being less vulnerable to possible sabotage and being able to carry out transactions on the Internet with a piece of mind.

Prologue by Fabio Assolini

Analyst of the company Kaspersky

watch video

Software is eating the world.

The words in the title are those of Marc Andreessen, who used them five years ago. He described how disruptive technologies could change our economy and the way we do business. Marc's prediction has turned out to be very real today.

More and major businesses are being run on software and delivered as online services. Disruptive technologies are changing the way we live. Could you ever have imagined that the world's largest movie distributor would own no cinemas? Netflix is revolutionizing the way we watch movies and series. What about the world's largest taxi company owning no taxis? Uber's arrival has been received badly in a lot of countries. Then there is the largest accommodation provider that owns no real estate. Airbnb makes it possible for anyone to rent a room. There is no question about the economic importance of software. We know that modern companies are becoming software-defined. However, despite this importance, software has a universal problem: **bugs and vulnerabilities.**

Humans develop software, so it is natural for errors and bugs to appear. The impact of a bug depends on how quickly a company responds to reports of that bug. We still see major software companies that are not prepared to respond quickly to a bug report. Few companies are adopting standards like Security Development Lifecycle (SDL). However, it doesn't matter what development methodology is adopted, **bugs will always exist.**

Cybercriminals know this and use it to their advantage: millions of computers could be infected exploiting a single vulnerability in a program like Flash Player. However, cybercriminals are not alone; governments have a strong interest in bugs – so-called 0 days – which have digitalized government and corporate spying around the world. Their interest has resulted in the creation of a lucrative market – governments are voracious buyers of 0 days, they influence the adoption of weak cryptography and software structure and standards – **to the detriment of everyone's security.**

In conclusion, and looking forward to 2020, I believe in the near future we will face **strict regulation** of security research, 0-day markets and the disclosure of software vulnerabilities. I also believe in a **great fragmentation of operational systems** due to the widespread adoption of mobile devices – Windows will no longer be the leader. Cybercriminals will need to adapt their attacks to these new platforms.

Software is eating the world

1.2

Some years ago U.S. entrepreneur **Marc Andreessen**, co-founder of the Netscape Communications Corporation and co-creator of Mosaic, one of the first web browsers with a graphics interface, said: "Software is eating the world".

In fact, Netflix, the largest film company, does not have any cinemas; it uses software; Uber, the world's leading taxi company, does not own vehicles, and Airbnb, the largest supplier of accommodation, has no physical properties. And software is not only eating the world by transforming the economy and the way in which business is done, but is also becoming more intelligent, helped by computers that are able to learn by themselves from their own experiences and to make decisions through "deep learning" using "artificial intelligence".

"Software is creating a new revolution in our world", says **Fabio Assolini**, analyst of the company Kaspersky. "We are living very interesting times with innovative technologies that are becoming very popular and are changing our way of life", he adds (watch video).

"The problem is software will always present vulnerabilities. The development method adopted will be irrelevant", which, on the other hand, is understandable, if we consider that it is carried out by the human being. The danger is that cyber felons know that software will always have weaknesses, and they will take advantage of this fact. To avoid this, it is recommended that companies guarantee security during the entire process of product development, from the beginning, using the so-called Security Development Lifecycle (SDL).

Countries, also chasing vulnerabilities

The interest for finding these weaknesses in software is not exclusive to cyber felons. Some governments are joining this "game" of exploiting vulnerabilities. Some countries are particularly interested in 0-day vulnerabilities, a type of failure that neither the manufacturer nor the developer of the product know it exists. They are highly sought because it provides access to the software and they can be used to infect systems or to initiate computer espionage campaigns all around the world.

Enormous potential of software as a result of the boom of artificial intelligence.

These 0-day vulnerabilities are feeding an enormous "black market" on the Internet. "Some governments pay a lot money for just one of them, for example, of an iPhone. It enables them to cyberspy or compromise companies by infecting their computers", according to Assolini.

One of the predictions made by the experts at the Future Trends Forum for 2020 is that governments will regulate, with determination, research on security in these 0-day vulnerability markets. They will seek its absolute control for their own profit.

Eden Shochat ▾
Founder of Aleph and trustee of Fundación Innovación Bankinter.

In addition, the countries' authorities will try to regulate the companies that sell these vulnerabilities, and by this date, many nations will apply severe regulations to software companies and the companies that operate, sell and export these vulnerabilities.

Increasingly smarter computer systems

Eden Shochat, founder of the venture capital fund Aleph, warns of the enormous potential of software as a result of the boom of artificial intelligence, and of the fact that beyond its unquestionable contributions to society, it gives rise to new cybersecurity dangers. In a next phase of evolution, computers may be able to improve the planning of attacks by using personal data that are very easily accessible on the Internet, such as the Personal Identification Information (PII) of Internet users. This capacity, which is being provided to computers with the purpose of tracking contents and analysing in an "intelligent" way the information that is available to them, will help cyber felons better define the scope of their objectives and direct their attacks more efficiently.

Computer systems continue to be highly insecure, despite the many security advances implemented in recent years. We continue to produce a wide range of software products, and it does not seem like it is going to change. However, their quality has to be improved, according to **Drew Dean**, director of programmes for SRI International (watch video).

The cost of having products that are secure by design is around 30 per cent of the total amount out there.

He insists on the considerable evolution of software in the past fifteen years with very significant improvements in terms of being able to solve computer failures. "Considering how the world is currently interconnected, if we would still be using defence technologies from the year 2000, we would be in an even more complicated situation", he points out.

It would be interesting to build a secure protocol for Internet addressing. He highlighted the progress made in recent years in Domain Name System Security Extensions (DNSSEC). Cyber felons have it more difficult now, although it is fair to say that many dangers persist. Dean suggests solutions, such as semi-private networks, that identify whether the opposing parties are trustworthy or not, communicating only with those that inspire trust. The key aspect in this issue could be trust. According to experts, it is not a technical problem, as establishing private networks is simple, it is knowing which ones can be trusted.

Security versus profitability

For manufacturers, from an economic point of view, one of the difficulties in terms of security is determining when that parameter should be added to the product before it is too late. Not knowing if a new product will be successful or not in the market complicates things. In fact, any investments in security before gaining market share are really "a waste of money", especially in the case of small businesses whose future is more uncertain, says **Drew Dean**.

The cost of having products that are secure by design is around 30 per cent of the total amount out there, according to approximate data provided by **Rolf Reinema**, director of Technology in Siemens. He adds that more than 80 per cent of security problems in cyberspace are associated with the quality of the software.

Drew Dean
Program director at SRI International.

watch video

Prologue by John Lyons

Chief executive & founder at International Cyber Security Protection Alliance (ICSPA).

watch video

Cyberwarfare has been defined as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”.

Many people might suggest that cyber terrorism relates to the infliction of death or serious injury by a terrorist group utilizing internet-based attack tools. All of these attacks are, sadly, possible, but to date, thank fully we have no evidence of any terrorist groups employing these tactics. That's not to say that they wouldn't wish to do so and accordingly, national cyber security strategies look to address these vulnerabilities.

It is more common, however, that terrorist groups use Internet-based tools and software, such as encrypted voice and text apps, and TOR networks to plan and support their operations. Given that we live in a world of escalating tensions both at state level and with increasing terrorist activity aimed at creating significant harm and division in societies, what are the pinch points that need to be addressed?

Attribution: it's not always easy, even for very advanced and mature cyber-capable countries, to identify the source of cyber attacks.

Defence first: most countries choose first to build and to increase their defensive cyber capability. But you cant do that well, if you don't understand what offensive cyber weapons are available and what techniques and methodologies could be deployed against you.

Cyber MAD Strategy: a strategy based upon the Mutually Assured Destruction of one's adversary.

Unintended Consequences of Attack: it is not always possible to isolate the victims of a cyber attack.

In conclusion, it is highly likely that we will see national cyber offensive weapons deployed more regularly as a precursor to armed conflict. Governments have a great deal to do, if we are to see such threats mitigated sufficiently well, for us to be comfortable about the future security of our Internet-connected systems.

Cyberwar and cyberterrorism

1.3

Before 2020, there will be a significant event involving a loss of life linked directly to a cyberattack perpetrated by some nation or State, or by a terrorist group. This is one of the predictions made by **John Lyons**, chief executive of the International Cybersecurity Protection Alliance (ICSPA) in the United Kingdom (watch video).

Another of his predictions is that some governments will have the technical means to block communications on the Internet in order to reduce the flow in different parts of the world of radical content from terrorist groups. In addition, governments will adopt measures to fight against encryption mechanisms and successfully monitor hostile groups on the Internet, with the purpose of intercepting their communications.

The power of military persuasion

When talking about cybersecurity, **John Lyons** focuses most of his intervention on considering the old lessons learned during the Cold War: the long rivalry between the USA and the Soviet Union following World War II. He emphasises on "dissuasion" as the central idea and on the so-called Mutual Assured Distraction (MAD) as one of the keys to maintain the power balance in the world that will avoid attacks between the parties.

Even now, in the new age of the Internet, he explains, we need to convince the adversaries that "we are very well prepared" to take any possible cyberoffensive from a technological point of view; that "we have the skills and ability" to implement them; that we "acknowledge the opposing parties have a similar technological potential"; and that they are ready to protect their networks successfully.

"I believe that cyberoffensive operations could be key in a stabler future society", although we would have "to avoid the political schizophrenia in which our leaders give into from time to time, and be more mature", that is, countries should maintain coherent approaches instead of continuously changing them according to the whims of the circumstances, he adds.

He explains that the aforementioned strategy of Mutual Assured Distraction requires a balance between offensive and defensive skills. "You have to be good at both." If a country is technologically ready to attack but its infrastructures are not secure, the MAD strategy will fail. "I believe that both things come hand in hand in military terms", he insists.

Miguel Rego, Managing Director of INCIBE (National Institute of Cybersecurity), warns of certain

> The aforementioned strategy of Mutual Assured Distraction requires a balance between offensive and defensive skills.

The so-called "botnets" or computer networks that are executed autonomously and automatically and controlled generally from a central node, usually with criminal purposes.

techniques that are being used by countries that could be considered as part of the cyberwar. "Many times, we can see malware or sophisticated malicious code that provides access to sensitive information belonging to public administrations and companies in other countries." How should the international law evolve for the year 2020 in order to prevent and regulate this type of practices?

"I believe that we will need to solve previous matters, such as who has Internet and where its sovereignty reigns before discussing any international laws", answers Lyons. "The differences between countries regarding the sovereignty of the network complicate other legal matters. I do not see many developments in this field in the next five or ten years", he adds.

Carlos Jiménez ▲
Founder and president of Secuware.

Cyber-cyber and machines vs people conflicts

Drew Dean warns of the presence of new actors in these wars, such as autonomous weapons, that could change the political power balances in the world. Next time a major armed conflict occurs between advanced nations, it will be complemented by cybernetics, that is, weapons with artificial intelligence that will make their own decisions. This is already happening, adds **Eden Shochat** categorically. He also adds that if we consider the current development of robots, drones and independent vehicles, the future could hold cyber-cyber conflicts, that is, battles between smart weapons. He reminds us that, after all, robots deploy software and thus can also be attacked by software.

Drew Dean answers that we will most likely see battles between machines and humans. Nonetheless, he is sceptical about the possibility, at least for now, of cyber-cyber wars happening with any relevant consequences. He does not think that a conflict between machines will be decisive up the point that it can cause one of the sides to surrender. The effects of a drone shooting an enemy drone will not be decisive in the outcome of a war.

Miguel Rego ▲
CEO at IN CIBE (Spanish National Cyber Security Institute).

Inbar Raz ▲
VP of Research at Perimeter X.

Perverse artificial intelligence?

In the book Daemon, by Daniel Suárez, a bestseller in the USA, an autonomous software programme creates a sort of augmented reality for each person and threatens to end the interconnected world. In the Terminator films, Skynet is the AI system that leads the army of machines to kill human beings. “This does not seem very likely at this moment in time!” I am not saying that it will never happen; we are simply not at that stage yet, says **Inbar Raz**, of PerimeterX.

However, he warns of the threat of exploiting vulnerabilities at a massive scale in an automated way by using hundreds of machines at the same time within the framework of the “Internet of Things”. He also warns of a dangerous artificial intelligence. What would happen if we went beyond the current line of defence in which artificial intelligence resides and we entered the perverse side of attacks?, wonders Raz in shock. He explains that artificial intelligence permits weapons to become semi-autonomous without having to be controlled by man. It is possible that certain people will think about creating a “dangerous artificial intelligence”. In fact, the incentives are very significant if we consider that “the cybercrime market is very lucrative”.

Carlos Jiménez, chairman of Secuware, reminds us that in 2001 “nobody had taught us how to use an aeroplane as a weapon”, referring to the brutal terrorist attack against the Twin Towers in the USA. Well, he explains, “we should transpose this to computers”. These and mobile devices are also potential weapons, which can also be placed in locations where an attack has been planned. Their operation would only require a person using them from the location itself or remotely. When we talk about practices such as a massive surveillance by governments to control citizens on the Internet and placing Trojans in systems to prevent attacks, according to the leaders that implement these control actions, the problem is that those same computer networks can be used by people with criminal intentions.

The so-called “botnets” or computer networks that are executed autonomously and automatically and controlled generally from a central node, usually with criminal purposes, are not weapons by themselves, but they can become attacking devices in the sense that they can be activated and their effects multiplied and spread immediately to millions of devices. The solution would not be to provide the governments with access to the systems, but instead to guarantee that they can be used securely. In the same way that a driving license is required to drive a car, a similar requirement should be established to use certain computers, explains Jiménez as an example.

Prologue by Caroline Baylon

Director, Cyber Security Research Programme,
Center for Strategic Decision Research

watch video

For much of our critical infrastructure, being 'air gapped'—or completely isolated from the public internet— traditionally formed the mainstay of defenses against cyber attack.

However, critical infrastructure is increasingly connected to the internet. Even in sectors like nuclear that have very stringent regulations, a number of facilities allow remote access through virtual private networks (VPN) or have undocumented or forgotten internet connections, some installed by contractors. Moreover, air gaps are not a guarantee of protection; Stuxnet has shown that all it takes is a flash drive to breach an air gap.

Many industrial control systems used in critical infrastructure were designed in the 1960s, when it was inconceivable that a malicious actor would try to attack them. As a result, they lack basic security measures such as authentication and encryption, making them 'insecure by design'. Moreover, the flexibility of code means that any attacker who can get past network perimeter defences can make logic changes that are very difficult to spot. And standard cyber security solutions used in home or office IT environments, such as patching, are difficult to implement in industrial environments.

Concerns involved in connecting critical infrastructure to the internet

1.4

The risk of a serious cyberattack on a nuclear plant is growing, given the increasing dependence of these infrastructures on digital systems. The tendency towards digitalisation, together with the lack of awareness at managerial level of the risks that it involves, means that the staff at facilities may not be aware of the cybervulnerabilities to which they are exposed, and, therefore, are not suitably prepared in cybersecurity to face potential attacks.

This is pointed out in a report published in October 2015 by the Institute of British International Relations, Chatham House https://www.chathamhouse.org/. **Caroline Baylon**, co-author of the publication, has warned that before 2020 there could be a macro-cyberattack against an electricity grid that would leave significant areas of the country without power for at least a day. Given its magnitude, we would learn about it in the media. By that year, she adds, a terrorist group could join forces with a team of professional cyberattackers, paying them for their services to attack a critical infrastructure (watch video).

She did not only refer to the cybersecurity risks of national infrastructures, but also to those linked with the materials and parts provided by suppliers. “It is really complicated to guarantee absolute integrity in the supply chain. Everybody is very worried about this”, and she warns of the problem involved in products not being secure by design. She also referred to the particular risk of critical infrastructures in developing countries, as only some of them are starting to learn about cybersecurity now.

The Stuxnet case, a malicious code against an Iranian nuclear power plant

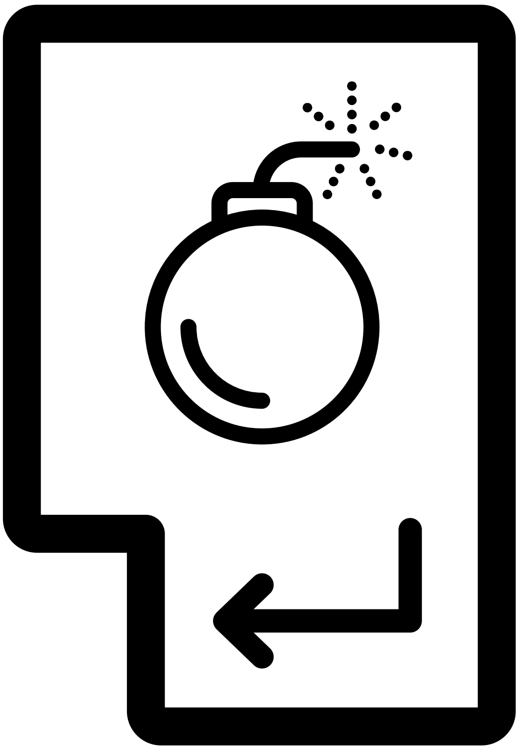
In this context, the participants recalled the cyberattack against an Iranian plant using the malicious code Stuxnet, which became known in 2010. This attack was a heavy blow to the country’s nuclear programme. Supposedly, the cyberattack was perpetrated by the National Security Agency of the United States (NSA) and the Mosad, the Israeli secret service, according to most of the evidence.

This sophisticated virus, which has been operational since at least 2007, was introduced in the computer systems of an Iranian plant and it caused around one thousand of the 5,000 centrifuges to overheat, becoming the first case of a cyberattack able to damage an infrastructure in the physical world.

“I do not think we should consider that attack as the Holy Grail of cyberoffensive interventions”, as the adversary was not particularly sophisticated, said Lyons, of ICSPA. “There are currently much more complicated objectives that could be destroyed.” Therefore, “we should not relax as a result of that success”, he adds.

The critical infrastructures of countries that are not prepared to defend themselves from cyberattacks should not connect their infrastructures to the network, answers Lyons to Caroline Baylon,

> The critical infrastructures of countries that are not prepared to defend themselves from cyberattacks should not connect their infrastructures to the network.



who also asked him if more money should be invested in "kill switches" or immediate shutdown mechanisms for those facilities in order to guarantee security in emergency situations.

"Yes", answered Lyons emphatically. "I believe it is dangerous that we are not able to disconnect those infrastructures in the event of any type of attack." Governments in countries with a higher risk of vulnerabilities in those facilities could collaborate in cybersecurity by not allowing the people responsible for those infrastructures to operate them if they have not been sufficiently trained to defend them against attacks. "These high standards should be required, but they are not", he says with regret.

By 2020, the deputy chairman of Constellation Research, Steve Wilson, says that he finally believes that "they will come to their senses". One of his predictions is that smart thermostats in nuclear reactors will be prohibited. "I do not trust that the software will behave."

Conclusions

Chapter 1 — Cybersecurity threats

Cyberattacks are a current problem. They increase exponentially every year and they become increasingly sophisticated and perverse, which is seriously worsening the problem. According to the experts, the cyber felons aspire to greater challenges with the technologies they have within their reach, which are easily accessed on the Internet.

At the same time, certain governments are using cyberwar techniques and frequently going to the markets to purchase 0-day vulnerabilities with the purpose of accessing computer systems from these back doors and massively surveilling citizens and companies by using security as an excuse. According to the experts, the problem with this type of access is that it can also be used by cyber felons.

Artificial intelligence, with all its economic and social benefits, could be threatening and cause machines to take evil decisions against people in the future. So far, there is no sign of any cyber-cyber wars, that is, between autonomous weapons, although they could occur in a more distant future.

Furthermore, computer networks that are remotely controlled by cyber felons allow the effects of these attacks to be spread massively, as it is already happening, although the problem will become more serious with the "Internet of Things", according to the experts.

With regard to specific infrastructures, these represent a serious security threat due to being connected to the Internet, as a cyberattack could jeopardise essential services in cities, such as electricity, water or gas. For all these reasons, software needs to be secure, despite the difficulties involved, whereas devices should be secure by design, despite the economic disbursement involved for companies without having any guarantees that they will sell their products.

Surveillance –
to detect, to respond to, and to remediate cyber
#FTFCybersecurity
nts & Corporations

The security of the internet user

2

Inbar Raz
VP of Research at Perimeter X.

Steve Wilson
VP & principal analyst at Constellation Research.

Evan Wolff
Partner in Crowell & Moring.

Kevin Sale
IT Security specialist at King Abdullah University of Science & Technology.

The “Internet of Things”, an unstoppable phenomenon of connecting everything to everything that is advancing at full speed, will inevitably bring surprises in terms of security, surprises that will not always be pleasant, as it is currently already happening.

The revolutionary computer innovations in this age, which are increasingly more powerful and smarter, together with the proliferation of sensors that are getting smaller and cheaper are becoming crucial factors in global interconnectivity. Any electronic device connected to the Internet, as small as it may be, can automatically become a potential target to cyberattacks, and this entails very serious risks for people’s security.

No sector seems to escape from the seduction of Internet, the experts agree. However, certain areas will be more sensitive. For example health: the bracelets and wristbands that have become very popular in different parts of the world and that measure all kinds of biomedical parameters and indiscriminately send the data they compile to the Internet run the risk of being accessed by anyone, endangering their owners’ privacy.

Privacy in the “Internet of Things” is setting the alarm bells ringing. The millions of items of data spread throughout the Internet as a result of this phenomenon can reveal private information of people when massively processed and analysed by the extremely powerful computers that are currently available. Furthermore, the current verification systems for digital identities do not always guarantee the privacy of the person, and neither are communication systems one hundred per cent reliable when ensuring that the receiver of the message will be the only one reading it.

Prologue by Inbar Raz

VP of Research at Perimeter X.

watch video

Our lives today are controlled by computers, and all computers run software. When the software contains bugs, they turn into vulnerabilities which can be exploited and used to cause damage. Hackers and governments commonly use those to achieve their goals.

These bugs exist mostly because of lack of security in the design stage, whether because vendors are rushing to get the product out, or simply because the vendors don't have anyone who's knowledgable enough. Since vendors are generally not punished for creating vulnerable code, even if it's already been exploited and damage has been caused, then they have no incentive to change or improve.

We would like to change that, by creating a new standard for secure development, in a manner that does not impede innovation and creativity on one hand, but also imposes stricter regulations on software that has a big impact on the public, on governments or on critical infrastructure.

"Differential Standard for Security Scrutiny" says, in plain words, that the more popular or influential your product gets, the stricter security standards you will have to adhere to. Start-up companies will still be able to rush their development and get their product out, but as the popularity of the product rises or if the product ends up getting installed in critical places, the compliance requirements will rise accordingly.

This way, we hope to significantly reduce the security incidents in software that has great effect on the public.

The "Internet of Things", a paradise for cybercrime

2.1

Intelligent refrigerators that inform the owner when something is needed, autonomous and semi-autonomous cars that warn the driver if, for example, he is falling asleep, and countless devices, such as television sets, bracelets or watches, which can be found anywhere, are already connected to the Internet with the purpose of simplifying people's lives. "We are surrounded by these devices. The Internet of Things is already here", says to **Inbar Raz**, deputy chairman of PerimeterX (watch video).

The problem of this omnipresent connectivity is that "we all become potential attackers and potential victims of cyberthreats." Currently, anyone can create their own device and connect it to the Internet, says Raz. In fact, computers are increasingly cheaper, smaller, more accessible and easier to use. For example, Raspberry Pi Zero is a tiny PC with great functionalities that can be purchased for a few euros, or Arduino, a free hardware platform developed by Spanish people that allows building and programming very cheap electronic devices from home.

Any device with an Internet connection cannot only attack but also access platforms used for this purpose. Raz also spoke about a computer network controlled by cyber felons discovered a few months ago that infected smart refrigerators and from which a large number of junk mail was sent. "Who would imagine that this would happen?", he wonders.

We need to establish some type of regulation on cybersecurity, in addition to setting requirements such as the Security Development Lifecycle (SDL) and security by design -or from the device's design itself-, he said. Security has to be "a feature" of the product, an inherent requirement and not something that is added arbitrarily depending on the manufacturer. In this context, the user should not be burdened with the responsibility of managing it when using a device; it should be made secure beforehand, states the expert.

"When my car breaks down, I take it to the workshop. I do not need to know how the engine works, nor do I want to know. When the decoder breaks down, I call the technician; I do not need to know how it works. The same thing happens with a practitioner: he studies for many years how to cure me; I do not have to know how to do it myself", he adds.

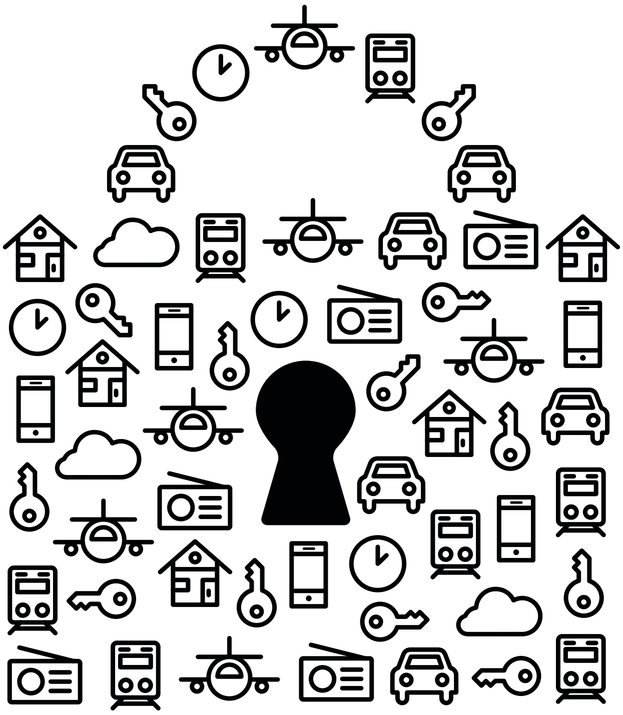
Rolf Reinema ▾
Head of Technology Field at Siemens.

watch video

Internet security should be regulated as a basic service

Internet security should be guaranteed by the Government in the same way as electricity, which is a basic service, he adds. It is a resource for countries, and its security should be regulated by the Government. On an individual level, the citizen cannot do much on his own to guarantee that it is safe, explains Raz.

He has the following two predictions for 2020: One is that anyone will have access to another person's private data and these will be even more spread around the Internet than they currently are. In addition, cyber-blackmailing will be made much easier: the cyber felon will only need to press a button to make the customer pay for freeing his computer from the viruses that the cyber felon has infected it with.



Internet security should be guaranteed by the Government in the same way as electricity, which is a basic service.

His second prediction is that a murder will be committed from the Internet. So far, this has not happened. However, although indirectly, deaths have already been reported from crimes linked to the Internet, such as suicides, by cyberextorsions and cyber-blackmailing victims under the threat of cyber felons publishing their intimate details if they are not paid substantial sums of money.

With regard to the cybersecurity of companies, **Rolf Reinema**, director of Technology of Siemens, a company with an ambitious security program, has warned that the current great challenge in cybersecurity is to know how to deal with the unknown when under threat. "You can only search for what you know", he said. "We are constantly under the risk of being attacked. You cannot prevent everything that is going to happen. The question is how do we deal with the problem?", he wonders. The immediate answer would be to monitor data and see where the "bad guys" are. We usually do not know their location, hence the interest of monitoring them (watch video).

He referred to two challenges. One: to differentiate between a genuine attack and an abnormal behaviour from a conventional user, as the limits are not so clear-cut. A second challenge: to advance in the development of technologies that help detect the attack from the moment it is produced.

On a global level, most of the experts agree that there is a need to increase consumers' awareness of protecting oneself.

Fernando Vega ▲
Information Security director at Bankinter Global Services.

Michael Osborne ▲
Manager Privacy and Security Cognitive Computing & Industry Solutions Department, IBM Research Division.

The secure encryption of systems as a subject in University

In this context of threats, the University's role seems to be decisive when it comes to encouraging the training of experts on secure encryption, although it is currently not the case. "We are talking security by design, but we have a root problem. It is currently not studied in computer sciences, at least in Spain that is", says **Fernando Vega** with regret, director of Information Security in the Bankinter Group. Is this the case in other countries? How does the future look like with regard to this issue?, wonders the expert.

Universities, in general, do not seem too worried about training on secure encryption, explains Fabio Assolini of Kaspersky. In the end, this is something that is learnt once students are working in the cybersecurity sector. In fact, many companies are specialising in the control of source code and in solving vulnerabilities. He reiterates, "Universities are not teaching their students to encrypt securely and this is something that they have to change."

Careful with children on the Internet and "virtual" candy

Teaching children from an early age how to protect themselves on the Internet is crucial, according to the experts. "In this new era of the Internet, children have to understand that they should not accept virtual candy from strange websites, in the same way as children in the past learnt to not accept candy from strangers", assures **Michael Osborne**, of IBM, in a relaxed tone.

On a global level, most of the experts agree that there is a need to increase consumers' awareness of protecting oneself, especially minors when surfing on the Internet or when carrying out transactions. However, during the debates there were different opinions on the level of responsibility that should be assigned to the person or individual in the task of having his security guaranteed. Whereas some especially defend the consumer adopting a cautious behaviour as a key aspect of his security, others are more in favour of shifting this responsibility to the industry, which should guarantee secure products anyway. Nonetheless, the widespread view is that solutions involve a joint collaboration between consumers, legislators, governments, industry, companies, etc.

“We all become potential attackers and potential victims of cyberthreats.”

Inbar Raz

VP of Research at Perimeter X.

Prologue by Steve Wilson

VP & principal analyst at Constellation Research.

watch video

It is well known that most Internet fraud is related to weaknesses in online authentication. It can be hard to know who you are really dealing with online.

Uncertainty about the origin of emails and websites leads to phishing; weak proof of identity allows identities to be taken over and fake new identities created. The response to identity problems tends to be to pile on more identity! Over time, we have tried to reinforce weak digital identities with card verification codes (CVCs), "Knowledge Based Authentication", and biometrics, but all that additional evidence only gets stolen and abused too.

At last the tide is turning, with identity engineers shifting their attention from "who" someone is to "what" someone is. That is, what do you need to know about someone in order to do business with them? What specific attributes matter about people in each transaction context? Identity is abstract and fluid and actually very difficult for computers to deal with. We are making better progress now by dropping down a level to look at concrete attributes: credentials, qualifications, memberships, account numbers, health identifiers, demographic details and so on.

Modern identity management should be concerned with **the contexts** of transactions and particular attributes of interest, **the relationships** between parties and preserving them online and **the provenance** of attributes (where they come from, who vouches for them).

Thus we will make progress towards usability, the reduction of passwords, resistance to identity theft and fraud, easier proof of identity, better privacy, and less disclosure of personal data.

The weaknesses of digital identity

2.2

The identity of an individual is exactly the opposite of his privacy. The identity is that which is needed to know about someone and privacy is precisely the opposite, that which should not be known of that person, explain the experts.

Identifying exactly who you are dealing with is fundamental in real life but also in digital life. In cyberspace, things are more complicated because we do not see the person we are dealing with physically. Despite the existence of attributes associated with the individual's digital identity, these can be modified, hidden and even fraudulently replaced by others. There are different digital authentication and identification systems, but the market does not offer a unified one yet. "Safe authentication protocols are needed for a secure future", according to **Drew Dean**, of SRI International.

In the physical world there are many personalities: cultural, recreational and occupational. Some mix easily, others do not. On the other hand, in life online personality convergence is conspicuous by its absence. "Digital identity is mathematical, precise." assures **Steve Wilson**, of Constellation Research (watch video).

The key is in knowing what the person is and not who he is

The aim of authentication is to provide security. It consists in confirming the digital identification by means of a unique characteristic or object of the individual. But, what do we really need to know about someone in the digital life?, ask the experts. It is not about knowing who the person is, but what he is. "It is not important whether the individual is called one way or the other. That is irrelevant." The important thing is to know that the person is who he claims to be and that he has not committed anything illicit previously that would impede him from continuing with a transaction, explains **Richard Parry**, a manager at Parry Advisory.

The way in which a mother knows her child is completely irrelevant for a bank. The important thing is that the keys used for operating match those used by the person to which they were provided. "The important thing is that whoever has been given keys can control them" and that, on the other hand, they are not being used by another person without authorisation, adds Steve Wilson.

Identity verification is essential to identify people and to manage the risk involved in dealing with people when it comes to doing business, for example. Some sectors are more sensitive to the fraudulent use of digital identity, such as the financial and

The aim of authentication is to provide security. It consists in confirming the digital identification by means of a unique characteristic or object of the individual.

banking,the health or the online retail sectors. Fraud on the Internet has a lot to do with the weaknesses around the authentication of a person, which is easy to replicate and manipulate, insist the experts.

The digital world does not involve trusting everybody

It is a utopia to think that in the digital world you can do businesses with any stranger and that you can trust any identity behind ones and zeros, warns the deputy chairman of Constellation Research. In life online you would have to reject the supposedly insecure experiences in the same way as you would do in the physical world, adds the expert.

In digital authentication "a physical key" is needed, a number that simply connects two points. "People are given the locks for that identification, but, as a nation, there is no way of knowing who has been given the keys. We do not have a national framework", warns Parry.

Instead of considering people as tokens that include data to identify the person, individuals could become tokens whose information would automatically confirm if someone is the person he claims to be and if this person can perform certain transactions according to his history.

> Authentication techniques must guarantee the protection of data, that is, they must protect the privacy of users using powerful encryption systems.

Experts have also debated on biometrics, an identification technology that recognises unique and non-transferable morphological and behavioural characteristics of people, such as the face, back of the eye, etc. Wilson believes that there is no, and there will never be, biometrics in the world with the engineering characteristics that provide sufficient reliability. The director of programmes in SRI International, **Drew Dean**, agrees and states that this technology, as far as recognition is concerned, has non-trivial error rates.

The need for powerful encryption systems

Experts believe that authentication techniques must guarantee the protection of data, that is, they must protect the privacy of users using powerful encryption systems, not the fragile ones that have been employed up to now. The content of the communications must be unreadable for those who do not have the key to decrypt it, including governments, they add. A powerful authentication is required for legitimate intentions, an authentication that provides security and transparency to the digital relationships of individuals with companies and governments.

Furthermore, the Russian Member of Parliament **Ilya Ponomarev**, chairman of the subcommittee of Innovation and Venture Capital of Duma, warns of the paradox of many people demanding privacy for themselves above everything and at the same time demanding maximum transparency from the Government. "Yes, they want transparency in others, but not for themselves", he says.
This type of approaches will probably end up causing upheavals in areas like Europe, he adds.
He believes that a broad agreement should be reached with respect to these matters, especially considering those businesses engaged in new technologies that will be particularly affected.

“Safe authentication protocols are needed for a secure future”

Drew Dean
Program director at SRI International.

Prologue by Evan Wolf

Partner in Crowell & Moring.

watch video

Current global policy debates highlight the tension between cybersecurity, with its emphasis on increased information monitoring and sharing, and privacy, with its expectation that personal information will be protected above all else.

Trust, from three different perspectives, is the key to reducing this tension and harmonizing cybersecurity needs with privacy expectations.

First, individuals must trust technology and custodians of personal information not only to protect their data but also to provide solutions when things go wrong. That trust arises from custodians being transparent about how electronic information is collected, secured, used, shared, and disposed of.

Second, businesses must trust information security systems and related controls to provide reasonable, risk-based protection for their intellectual property and business data and their customers' and business partners' data. Businesses also need to trust technology to be sufficiently robust and flexible to comply with an evolving array of government regulation, information sharing initiatives, and privacy requirements.

Third, nations must trust that the cybersecurity technology, policies, and practices upon which they rely will be sufficient to defend their electronic borders against cyber threats, while also protecting the data of their citizens and businesses in a manner that strikes a reasonable balance between national security and law enforcement needs and citizen's privacy expectations.

Cybersecurity technology, tools, and policies are critical for protecting information and physical security, just as privacy laws and policies are necessary for protecting personal information. Trust that cybersecurity and privacy can not only co-exist but also complement each other will develop with discussions about the intersection of cybersecurity and privacy, the challenges that cybersecurity and privacy pose for each other, and the importance to each of transparency and accountability.

Intimacy and privacy versus cybersecurity

2.3

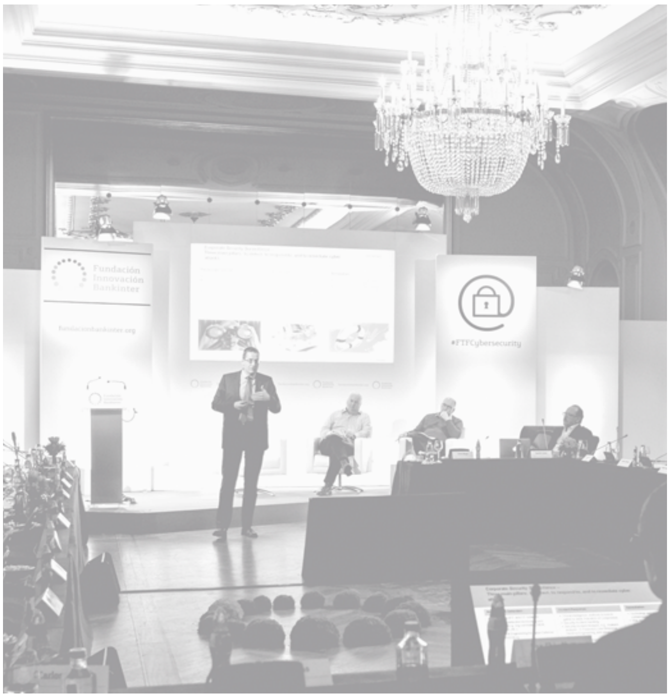
Since the controversial revelations of Edward Snowden in 2013, the public have known that world governments have a serious interest in having access to all the data that circulate on the internet. The former computer engineer at the National Security Agency (NSA) https://www.nsa.gov/ uncovered unethical practices by the U.S. Government and its "Prism" program, which used 0-day or "zero day" vulnerabilities to monitor certain sectors of the population.

Would the loss of privacy with the aim of supposedly achieving citizen security be justified in modern societies?

One of the five settings of society that the experts worked on was precisely a system that is completely controlled by the Government. From a technological point of view, this is a possible situation in the new era of the Internet thanks to the widespread existence of systems and sensors at a low price, which would make it a possibility in some countries, especially after a massive terrorist attack that would send the population into a panic. The conclusion of a model like this is that there would be no privacy and people would end up suffering from mental disorders.

On the other hand, according to experts, guaranteeing security in a world where privacy is above everything would be complicated, because data would always be encrypted so it cannot be revealed, including any communications between terrorist. Nonetheless, individuals would have control of their data and their privacy would be safeguarded. The experts warn that cyber felons would tend to abuse the easy access to all types information on the Internet.

"I really do not believe in privacy on the Internet. I believe that we need a stricter authentication for Internet privacy and security when necessary, but when it is not required, anonymity should prevail", explains **Evan Wolff**, a partner at Crowell & Moring (watch video). The citizens are currently at a disadvantage in cyberspace and felons have an advantage over them, he insists. Why? , he wonders. Managing digital identification is very complicated and managing authentication even more. Authenticating somebody in cyberspace



By 2020, he predicts that the cycles of threat detection will be reduced in companies with the use of more predictive systems and intelligent security analytics.

and verifying that the digital and real identities of a person match has become a very complicated task, whereas maintaining a user's anonymity is "very, very easy", he adds. For example, "WhatsApp", the popular communications service, hardly requests any details to register.

The expert is confident that the upcoming quantum leap in technology programming and innovation will be decisive in improving authentication systems and defining concepts about privacy that benefit the digital citizens.

As a result, they will be more protected against cyber felons. He also expects that countries and large companies will start to organise themselves to work together towards these objectives.

One of his predictions for 2020 is that companies will be more transparent with respect to what they do with their customers' data, and this will contribute to guaranteeing their privacy. Regulations will be part of the process, but they will not be decisive, because these things do not work by enforcing legislation, he points out.

From the business sector, **Rolf Reinema**, of Siemens, assures that "we have to find a suitable balance between the necessary control of security and preserving privacy. Usually, the tendency is to compile everything and then analyse it. This has some negative privacy implications, because the data collected by companies to prevent cyberattacks could also be used for other intentions.

The use of personal data by companies

Some companies work with very powerful threat detection and monitoring tools, but there are still vulnerabilities in their infrastructures. The processing of millions of data in real time or Big Data is now possible thanks to current computers being increasingly smarter, and they also allow defining behavioural patterns, trends and guidelines of cyber felons, as well as predicting possible threats from data analysis.

In the same way that governments monitor citizens under the argument of security, companies tend to collect all possible data with the purpose of subsequently deciding which could be useful, says Reinema. "We must make sure that these data is not used inappropriately. We focus on the collection of data, but many times, we do not concentrate on protecting them. And these data could be interesting for others", according to Reinema.

The citizen does nothing; technology takes care of guaranteeing his security.

By 2020, he predicts that the cycles of threat detection will be reduced in companies with the use of more predictive systems and intelligent security analytics, which in the event of cyberthreats will trigger alarms much earlier than now. This will provide companies with real-time cybersecurity indicators, and it will expedite the mitigation of attacks.

With regard to these issues, "the stupidity" that one sometimes detects is unbelievable, warns Michael Schrage, of the MIT Center for Digital Business. On the one hand, we demand security, but paradoxically, on the other, our privacy cannot be violated, he adds. The question has nothing to do with legislating or not, but with the inherent conflicts between regulations that compete with each other to fulfil their own objectives and with the purpose of guaranteeing a security that, in some way or another "does not infect or contaminate other assets." This, by itself, "is not only naive but also a mirage", he specifies.

Does technology change the behaviour of people? Which would be the best way of promoting privacy and security? Through new technology solutions or by encouraging different behaviours? The majority defends the combination of several measures as the key to success. The solution would have to involve the search for a balance between legislation, social and educational awareness, innovative technology, etc.

Regulations are important, maintains the deputy chairman of Constellation Research, **Steve Wilson**. Although some countries disagree, "of course laws change the behaviour of people in the very long term", he assures. To justify his arguments, he points to the compulsory

Michael Schrage ▾
Research fellow, MIT Center for Digital Business.

The solution would have to involve the search for a balance between legislation, social and educational awareness, innovative technology, etc.

use of seat belts in vehicles as an example, which was highly successful in guaranteeing the security in the automotive industry.

Michael Schrage, of the MIT, says that technology by itself is much more effective than any law that seeks to impose certain behaviours, even in terms of personal security. He proves this by presenting the example of the airbags used in cars to protect passengers in the event of an accident. He explains that the user does not have to remember whether to activate it or not, because it works automatically when needed. The citizen does nothing; technology takes care of guaranteeing his security.

He even adds that certain small defects in the architecture of technologies, intentionally built in by its developers to activate from time to time, would undoubtedly guarantee the security or privacy of the user much more effectively than many recommendations or laws.

If we ask someone, for example, to memorise a new password every six weeks in order to protect his identity on the Internet, it probably will not be so effective as the activation of some type of mechanism in the system that from time to time automatically encrypts the user's passwords in order to force him to set new ones for security reasons, he adds.

The book "Nudge" by professors Richard H. Thaler and Cass R. Sunstein, specifically explains that you can help people to make important decisions in their life by slightly pushing or nudging them to do so, as exemplified by the aforementioned case of encrypting passwords from time to time with the purpose of forcing users, in a nice way, to change them.

John Lyons, of ICSPA, makes good use of the debate to highlight the importance of privacy on the Internet not only for citizens but also for companies, whose significance should not be underestimated under the argument of having to give preference to other requirements such as security, which, of course, is also important. He warns that South American countries or some Asian countries, among others, could prefer technological products and the innovation produced by certain geographical areas in the world, such as Europe, instead of others, because they guarantee a further commitment to privacy in their products and services.

“I really do not believe in privacy on the Internet. I believe that we need a stricter authentication for Internet privacy and security when necessary, but when it is not required, anonymity should prevail”

Evan Wolff

Partner in Crowell & Moring.

Prologue by Kevin Sale

IT Security specialist at King Abdullah University of Science & Technology.

> Consumers and stock holders don't really care about an organizations cyber security. After the data breaches of Target and Home Depot customers returned and the stock price of both organizations rose above their pre-breach levels.

Now a few years on from these events both organizations appear to show no long term ill effects. My conclusion from this is that there is little incentive for organizations to place cyber security at the center of their organizational strategy.

We need to get to the point where consumers are making purchasing decisions based on based not only on factors such as price and customer service but also on the organizations attitude to security. If customers are educated enough to include security into their purchasing decisions it would directly impact sales. Successful and innovative organizations would then use their security as a differentiator and an arms race between organizations with security as a selling point would become a reality.

Allowing market forces to drive improvements in security is not a quick process but like all good building projects it starts with the right foundations. The first step is mass public education programs to inform consumers about basic security hygiene and the value of their data. We should use the same models of sustained and coordinated public education successfully used by governments to inform the public of the dangers of smoking or the spread of HIV/AIDS to deliver education around citizens' digital health. Today we have the World Health Organization, let's adopt the same model and have the World Digital Health Organization. Once the public have a strong awareness around their digital health they will make purchasing and lifestyle decisions based on the impact to their digital health and at this point market forces will compel organizations to use security as a selling point.

“We need to get to the point where consumers are making purchasing decisions based on based not only on factors such as price and customer service but also on the organizations attitude to security.”

Kevin Sale

IT Security specialist at King Abdullah University of Science & Technology.

How to improve cybersecurity

Experts suggest the immediate adoption of a series of measures in different fields with the aim of improving global cybersecurity by 2020:

2.4

Respecting the law

- Ensuring that the laws are effective when applied to cyber felons.
- Severely punishing cyberattackers

Technology-based industry

- Developing perfect computer encryption systems with quantum computing.
- Completely renovating computer security measures and the Security Development Lifecycle (SDL) in order to guarantee security throughout the entire development of the software.

Education

- Governments helping citizens protect themselves in the digital world as the most effective measure.
- Defining clearly what privacy means versus security.

Legislation and regulation

- Promoting regulatory standardisation and international regulations to improve security in software development, in the use of data when governments share information and in the "Internet of Things".
- Guaranteeing the balance between public security and any possible intrusions or economic interferences from the Governments, bearing in mind that they will probably increase their preventive action orders when the cyberterrorist risks increase.

Companies

- Promoting security certificates for hardware and software and compulsory standards, by international organisations, in close cooperation with companies and governments. Digital products would have to pass cybersecurity tests.
- Improving the balance between managing the risk and managing security.

Individuals

- Trying to balance the public conflict around a different approach to privacy and security issues initiated by a new social class that will seek other lifestyles.

Multiparty collaboration

- Promoting a securer Internet by using authentication, behaviour rules, etc., in a similar way to when roads are built, which are required more security measures by complying with laws and fulfilling standards.
- Searching for creative formulas to encourage the promotion of cybersecurity with collaboration between governments, industry, universities, etc.

Computer hackers

- Being vigilant against artificial intelligence with a higher level in skills in order to better direct attacks from the access to Personally Identifiable Information (PII) of users on the Internet.
- Improving cooperation with the private sector.
- Assigning the attacks to the source. There is currently almost no punishment for cyberattacks and Justice must make attackers pay for their crimes.
- Improving authentication techniques and establishing protocols. Passwords are a thing of the past. Biometrics has failure rates that are not at all trivial.
- Starting to work on a reference cybersecurity architecture, equipped with greater resilience. The banks could be a starting point.
- Effectively protecting the connections to the "Internet of Things", that is, connecting everything to everything (vehicles, homes, etc.), which will become the largest source of vulnerabilities in the future.
- Adding cybereducation in all technological training degrees.
- Educating and qualifying software developers in secure programming techniques.
- Changing mentalities.
- Promoting a network of identity recording authorities to help governments and companies recognise who is behind every digital transaction. In addition, providing every individual with a unique digital identity for every virtual interaction based on reliable concepts.
- Protecting the countries' critical infrastructures as an urgent challenge.
- Progressively increasing international collaboration and regulation on cybersecurity.
- Monitoring that the traditional regulations do not limit innovation or economic growth.
- Giving preference to a fast and less painful capacity to recover in cybersecurity strategies, bearing in mind that "bad" things will happen.
- Being more aware of the situation of cybersecurity and attaining better means when sharing the most sensitive information of the organisation.
- Developing a solid digital authentication technology and governance by the industry and governments.
- Differentiating, in a safer way, encrypted accesses and allowing a shared use of detailed databases.
- Committing to real time measures when talking about cybersecurity.
- Integrating the training on personal cybersecurity into higher education.
- Being vigilant against a new level of control similar to "Big Brother" or surveillance carried out by governments that could cause popular resistance.
- Organisation such as the United Nations implementing international regulations to be ratified by the countries as local laws.

Conclusions

Chapter 2 — The security of the internet user

Any citizen, without being famous, even if not especially important in social, political or economic terms, is much more attractive to cybercriminals than one would imagine. For cyberattackers, all Internet users are possible victims of being scammed out of money at any given time. If we consider the increasing presence of the public on the Internet, the probability of a conventional individual being attacked will be gradually larger.

The boom of commercial solutions that easily and cheaply allow manufacturing small electronic devices that can be connected to the Internet will skyrocket the probability of each individual becoming a target of cyberattacks, as well as a potential attacker. According to the experts, it is technically possible.

The "Internet of Things", where everything is connected to the Internet, has hugely increased the spreading of private data of people, and it has simplified their access from anywhere by cybercriminals, which can now plan their attacks more effectively.

Personal privacy is being encouraged much more in the digital world than in the physical world. Among others reasons, it is due to the ease with which the new smart technologies for processing and analysing information, which allow performing real-time calculations of millions of items of data, can establish correlations between them and reveal, from previously unrelated information, not only the identity of people but also their intimate details, at the expense of their security, among others aspects.

With regard to authentication, according to the experts, there are many challenges involved in, for example, verifying that people who interact on the Internet are really who they claim to be and avoiding any identity theft by cyber felons. These challenges are overcome, among other ways, by standardising systems that provide completely secure communications and that guarantee the privacy of the transmitted messages.

Fundación Innovación Bankinter
fundacionbankinter.org
Corporate Security Surveillance – Three main pillars: to detect, to respond to, and to remediate cyber attacks
Monitoring & Detection
Incident Response

The future cybersecurity

3

Richard Parry
Principal at Parry Advisory.

The new security threats and risks that cyberspace is facing is affecting the whole world, in addition to all the economic and social layers. “We are all under threat”, assure the experts. Therefore, global solutions with interdisciplinary measures from all types of fields are required, that is, from governments, institutions, companies, industry, legislators, educators, etc.

The dangers that are threatening cyberspace, which are becoming more and more severe, sophisticated and dangerous, will reach such dimensions in the next few years that countries should start thinking about how to fight against them. They should sit down to negotiate seriously and search for solutions to this problem. Experts agree that worldwide debate forums are required to talk about cybersecurity in a similar way as other international issues are discussed in high-level worldwide meetings, such as the climate change or energy.

Cybercrime, pornographic networks, arms trading in the Deep Web and cyberextorsion with deadly consequences for some victims are just some of the cyberthreats that are gaining importance on the Internet, and they are becoming increasingly more profitable for criminals. Some of the major risks in the future are cyberattacks against devices connected to the Internet (cars, pacemakers); international cyberwar; the public display of private information (health, financial data); digital identity theft (including financial theft); bioattacks (against the person); physical attacks through the Internet (mugging, domestic intrusion); and the massive surveillance by governments.

“The Internet of Things” will end up being “the Internet of All Things”, according to experts. Practically everything and everybody will be connected. According to the experts, this world, with infinite accesses to the Internet, opens up tremendous opportunities for cyber felons, and they believe that the problem will be unmanageable if we do not implement uncompromising and coordinated solutions that help fight cybercrime globally.

Previously, the countries must have a map that specifies the real situation of cybersecurity worldwide and the most urgent threats that should be fought in cyberspace, a world that should be indisputably linked to the physical world.

Experts have prepared a detailed road map with ten proposals aimed at advancing towards the objective of a securer cyberspace. They also point out that Internet users have to feel safe when carrying out financial transactions, allowing them to communicate without a fear of being extorted and of their personal data being manipulated or used with illicit purposes.

The advantages of the Internet are incalculable. The digital revolution has opened the doors to a world full of benefits, and societies must guarantee that it is all secure. The protection of the honest Internet user must be guaranteed, whereas the cyber felon has to be punished. "The bad guys" currently surf around the Internet without any boundaries where they can attack any part of the world with a simple computer; many times even with the help of their government and systems that are not always legally prepared to punish the culprits.

In their list, the experts propose a wide-ranging series of measures: international cooperation; in terms of product security, they should be secure by design; technologies for authentication with several requirements to verify the user's identity; campaigns aimed at the public to teach them how to protect themselves in the online world; training for companies and legislators aimed at making society aware of how it should adopt a secure digital consumption; and protection of national data, as countries do with currencies beyond their physical borders.

Similarly, secure and quality software is required from the industry. The law should guarantee that products meet certain security requirements and thus punish developers if they do not, as in any other industry. Experts insist that we should establish uniform global standards at an international level that include the characteristics that the secure software should have. They also insist that we should promote a strategy for global cybersecurity with a clear mandate for the governments, as well as providing sufficient economic resources for cybersecurity and promoting national and international public-private partnerships in order to combat cybercrime.

Experts have prepared a detailed road map with ten proposals aimed at advancing towards the objective of a securer cyberspace.

Prologue by Richard Parry

Principal at Parry Advisory.

When inflationary booms peak, and then begin to collapse, one is normally left with a glut of whatever the underlying commodity was.

Examples letter history, both distant and recent, be it tulips in 1637, technology companies in the dot-com crash of 2000, or housing in 2008. Some argue we're seeing the collapse of an inflationary boom in Cybersecurity, yet we don't see a glut of being secure, more the reverse. But we are awash in security technology. We see something resembling perpetual market failure.

In spite of staggering public and private sector investment in security solutions, better hardware, improving methods, international forums of cooperation, pledges to do more, spend more, the litany of breaches, successful hacks, and interceptions continue unabated.

Each year the application of capital, both financial and human, has risen to dwarf the last, while politicians fret of deliberate systemic failure at the hands of individuals, causes, and nation states. Meanwhile consumer/citizens become resigned to the notion that nothing can be done, and besides, all is well because everything continues to become more convenient.

2016 may be the year of fire-sales as Chief Technology Officers and Chief Information Security Officers conclude that more subscription services for tools that more speed reaction, but do not prevent, are becoming less likely to save their job, or that of their CEO.

Attentions may now be turning to address the consequences of an infrastructure designed for another time and purpose. Band-Aids on bullet holes won't do. Neither will a surfeit of startups who must reward their investors with perpetual revenue from subscription-based services that do not quite solve the problems.

What our web-enable conveniences are worth to us, and what we are prepared to do to continue enjoying them. The infrastructure manufactures may need to lead, with its operators.

A road map with ten proposals

3.1

01

read more

Reduce the global cost of cybercrime

02

read more

Guarantee the integrity of the technological solutions and infrastructures

03

read more

Generalise the use of two-step authentication technology

04

read more

Educate the public in basic cybersecurity

05

read more

Raise security awareness among digital consumers

06

read more

Protect the national data on the Internet beyond territorial borders

07

read more

Criminal liability for insecure software

08

read more

Quality software

09

read more

Promote a strategy for global cybersecurity

10

read more

Public-private cooperation

01 ▾ Reduce the global cost of cybercrime

The objective would be to modify the traditional balance of costs within the scope of cybersecurity, which until now, unfortunately, has resulted a lot more profitable for cyber felons than for honest digital citizens.

For cybercriminals, it is very cheap and easy to operate on the Internet, where they are able to easily achieve their objectives without barely any resources, often with a simple computer, and to perpetrate their crimes from any remote country but finding victims for their attacks in any part of the world.

On the other hand, protecting and defending oneself from cyberattacks is very costly and complicated for the victims. To solve this unfair imbalance, experts recommend working together at an international level. An overall image of all the actors that pose a threat to cybersecurity worldwide is required. We need to fight more efficiently against cybercrime, and a common technological cybersecurity standard must be approved.

Working together against cybercrime

We suggest that organisations act jointly and not individually against this problem under the umbrella of a non-governmental entity that helps blur the risks of any possible individualised retaliation from cyber felons.

The intention is to initially grant this leading role to the European Union Agency for Network and Information Security (Enisa) https://www.enisa.europa.eu/, an organisation that is currently assisting the EU to better equip and prepare itself to prevent or answer problems related to information security. The idea is for it to work jointly with the countries' own Community Emergency Response Team (CERT), integrating the experts in the development of preventive and reactive measures against security incidents in the States' computer systems.

According to the experts, when countries act jointly under the guardianship of an organisation, such as Enisa, it is much easier for them to theoretically remain on the sideline as a specific target or objective when against an eventual attack. This umbrella organisation would be selected by agreement of its members.

The success of the measures would be defined by the reduction of time that the organisations are exposed to threats, that is, by the agility to detect the attack from the moment it is produced. The challenge would be to reduce the impact and identify the felons. It should also be possible to recover any losses caused by cybercrime through prosecution.

The challenges would involve defining the terms under which countries would participate and cooperate in this cyberprotection model. The first step would be to organise a round table to debate protocol and the implementation of the plan.

Protecting and defending oneself from cyberattacks is very costly and complicated for the victims.

02 ▾
Guarantee the integrity of the technological solutions and infrastructures

The experts encourage creating a differential standard to examine security and promoting it, as well as privacy and security by design, that is, they have to be guaranteed from the beginning of the product's creation process. It is important to instil transparency and responsibility in the corporate values.

The company leading this proposal would be, again, Enisa https://www.enisa.europa.eu/, in collaboration with already established organisations, or their equivalents, that share information about standardisation processes, such as the International Standards Organisation (ISO) http://www.iso.org/iso/home.html and the ISAC http://www.isaccouncil.org/memberisacs.html or similar, that is, the centres that supply information to the authorities in the USA about cyberthreats to critical infrastructures.

The success of the initiative would be determined by confirming the reduced vulnerability or the CVE's of products made by companies committed to these security standards. It would also be determined by the rate of participation of these companies and by demonstrating that the adopted measures help reduce breaches of security.

The drive of companies to join the initiative is an important aspect, as it would allow them to prove to their customers that their products are better than many of the competition's as a result of having passed a series of security tests that support this, tests to which other companies have not been subjected or, at least, in such an exhaustive way.

One of the challenges of the proposal has to do with the aim of globalising solutions. The objective would be that all products, as well as the infrastructures, be tested in terms of security before launching them to the market. Experts point out that when new software becomes so popular that it reaches a critical mass, there should be guarantees of its security.

To promote this proposal, an industrial leader should be appointed to act as an "evangelist", and it should be another type of entity, not so much an organisation. This challenge would require the collaboration of several entities and it should not be carried out independently.

Avoid regulatory barriers

Far from this proposal being implemented through regulatory procedures that could result excessively bureaucratic, it should be promoted using the market's own mechanisms, which would encourage the demand of certain products once it is proven that they provide further security. Experts trust the market's mechanisms, and not so much in decrees issued by the Government.

The leading role of companies in the insurance sector when it comes to indirectly promoting industry quality levels and the requirement of companies meeting certain levels of security in order to obtain a policy, which helps them raise their standards, were highlighted during the debate.

> Creating a differential standard the product's creation process. It is important to instil transparency and responsibility in the corporate values.

The intention is to initially grant this leading role to the European Union Agency for Network and Information Security (Enisa) an organisation that is currently assisting the EU to better equip and prepare itself to prevent or answer problems related to information security.

03 ▾
Generalise the use of two-step authentication technology

The intention is to improve security for online transactions via technologies that verify identity twice (2FA). This type of techniques require from the user, in addition to the usual password, some other identifier that confirms that the person is really who he claims to be.

Many banks, for example, provide this technology for customer transactions when customers are required to confirm an order, beyond passwords or coordinates, by receiving a series of digits on their personal mobile phone.

How can the use of this technology be promoted? This question is intriguing the experts. Reality is not very encouraging for some organisations when it comes to initiating alone this road to a safer multi-factor technology. Therefore, they need to be incentivised to take the leap together, by means of a collective effort, and protected by some sort of legislation.

Whichever the technology that is finally extended, it should be "agnostic", sufficiently broad. A deadline should also be set for its implementation by the organisations.

It has been suggested that the Government should lead this measure in collaboration with the central banks and credit card companies.

The spotlight would mainly be on the finance industry, particularly on digital payments, because of their great appeal to cyber felons, as huge amounts of money are involved.

How could the success of its implementation be defined? Basically, by employing usage metrics, public adoption levels, indicators on the online security guaranteed by a specific system and, especially, measurements on the cybercrimes associated with criminal fraud.

The challenge of popularising this multi-factor technology

One of the objectives of the proposal is to genuinely spread the use of this 2FA technology. It would demand both a national and an international coordinated effort for it to be introduced in a synchronised way by specific territories, for example, at a European level. That way, any regional imbalances resulting from some countries drastically expediting its use, as opposed to others, would be avoided.

The implementation of a multi-factor authentication system would involve great challenges in very specific sectors, because it would transform how many companies go about their business; for example, in the online retail business, whose model of purchase is based on a "click" on a product.

In order to spread this technology, we would first have to identify which groups would be able to lobby together and raise the government's awareness, at an international level too. Lobby groups could be consumer associations, industries, etc. Regulations and legislation that demand the implementation of this securer technology should be encouraged.

The intention is to improve security for online transactions via technologies that verify identity twice (2FA).

04 ▾ Educate the public in basic cybersecurity

In general, the citizens have scarce knowledge regarding cybersecurity and as how to protect themselves on the Internet. The experts remind us that citizens do not usually protect their personal identity on the Internet as much as in normal life.

To deal with this, they suggest designing educational campaigns aimed at citizens with the purpose of globally raising their awareness on the risks of not protecting oneself on the Internet. They believe that this mission should be led by an independent NGO, far from the direct influence of the governments, although they would work together. They should also work with large businesses and the academic network, including schoolteachers.

Raise awareness from childhood

This is precisely the age level we want to reach when sending messages to bring awareness towards the need of protecting oneself from the virtual world.

The organisations involved in starting the initiative would act jointly and voluntarily, with the common incentive of feeling part of the possible acceleration of a schedule of actions. The key of this initiative would be precisely this collaboration. One of the organisations involved would lead the process of pressing for the implementation of the measures.

How can we reach the citizens with these messages? The perception of which each person considers private information varies significantly from

This is precisely the age level we want to reach when sending messages to bring awareness towards the need of protecting oneself from the virtual world.

country to country, from culture to culture. The degree of confidence in a government or school also varies by society or individual. This is why an independent non-governmental association is proposed to lead the process of trying to educate the public in cybersecurity matters.

The Media, the great ally

The messages issued would have to be very simple. They must be easily accessible to the public. They must reach people easily. Therefore, investments in commonly used communication channels (television, games, etc.) should be a priority. This includes radio and telephone, with messages on how to protect oneself on the Internet that would reach the citizen even in remote areas where the mobile phone is the only telecommunications infrastructure.

Experts point out that, sometimes, beautiful websites are designed with carefully elaborated messages that are non-productive in the educational mission for which they were conceived, simply because the user does not know how to reach them.

In order to determine the level of success of the measure's implementation, we suggest some type of impact assessment on the general knowledge of citizens by using some kind of benchmark, as well as metrics that determine if people operate securely in the online world.

As challenges, it is worth highlighting the identification of the type of issuer that people would trust when assigning the mission of communicating the messages used to influence the public and to encourage them to protect themselves. In addition, the appropriate channels to reach the public must be defined.

Educational materials and methods on cybersecurity need to be developed before starting with the proposed global awareness actions. An implementation plan should also be designed, together with indicators to measure the evolution of the measures' application.

A long-term financing would be required, bearing in mind the continuity required for training cycles to reach different groups with advice adapted, in every phase, to the new threats of that point in time, as they continuously evolve. Experts say that becoming aware of certain habits usually requires time and this is why educational campaigns require long-term investments. It would be necessary to identify the deficiencies of each group regarding cybersecurity in order to pinpoint the actions required.

05 ▾ Raise security awareness among digital consumers

The objective is to educate the consumer in basic cybersecurity to make him change non-secure purchasing behaviours on the Internet. The initiative should be tackled using a pyramidal approach. On the one hand, by means of educational campaigns for the public, and, on the other, at a higher level, with measures aimed at companies and legislators to contribute to raising awareness on cybersecurity and with international agreements at an institutional level.

The WHO, a model to be followed

From the point of view of raising public awareness, the idea is to create an entity to lead the process, which would be a cyber version of the World Health Organization (WHO) http://www.who.int/es/. The intention is to transfer the work strategy of the WHO on health prevention to the Internet and the use that the public makes of the technological services and products.

The idea would be to raise public awareness in the need of protecting oneself in the digital world, and it would be carried out following a similar model to the WHO when it tries to educate citizens on taking precautions against certain sexual practices of risk in order to avoid spreading diseases such as AIDS.

The main partners of the cyber version of the WHO would be large technological businesses, such as Google or Apple, and the media would have to play a key role as a distribution channel of the messages intended to raise public awareness.

The World Health Organisation is a non-repressive organisation. It is not a regulatory company and does not impose obligations. It simply contributes to raising public awareness, point out the experts. It also facilitates coordination between all the different actors, not only state bodies, which are actually a minority. As part of the cyber entity suggested, cybercrime experts, research centres, companies and NGOs could be included.

Its structure would be similar to that of the WHO, which has a network of research organisations, both public and private, in different countries that contribute to the knowledge of illnesses, and in the case cybersecurity it would provide information on computer vulnerabilities.

Subsequently, in the WHO's case, the organisation distributes that information to the States, which launch their respective national educational actions to raise public awareness on new threats and to prevent epidemics.

The idea is not to make the consumer understand the new viruses or technically analyse them, but just teach them to adopt certain behaviours, some of them standardised, in the event of certain indications subject to affect their cybersecurity.

The objective is to educate the consumer in basic cybersecurity to make him change non-secure purchasing behaviours on the Internet.

> From the point of view of raising public awareness, the idea is to create an entity to lead the process, which would be a cyber version of the World Health Organization (WHO).

As an example of successful citizen educational campaigns, although in the field of health, experts recall an initiative against AIDS that took place in the United Kingdom in the eighties with an enormous social impact that used all the media channels available to raise awareness on the risk of certain sexual practices.

Experts say when the public is provided with enough information, they are qualified to make better decisions faster; for example, to decide, without sacrificing their personal security or the security of their private data, if one continues with a digital transaction based on the information they possess.

They emphasise that the simplicity of the content of the message that wants to be spread is essential to reaching the masses successfully. The experts also recalled an old and very popular campaign in Australia aimed at raising awareness on skin cancer, as well as a current initiative in the United States under the slogan "Stop. Think. Connect" https://www.stopthinkconnect.org/ aimed at raising awareness about cybersecurity.

Regional particularities require special attention

One of the great challenges of this proposal would be to adjust the messages to local conditions. The definition of privacy varies enormously in different parts of the world. The way in which privacy is seen in China is very different from the view in America or Britain. One another's level of awareness on how third parties can use their personal data and profit from them is also different. That is why the message to raise awareness on cybersecurity in one part of the world or another should be different and adjusted to each specific context.

According to the experts, changing the behaviour of the consumer when choosing a product or another in accordance with the security levels provided would be decisive in defining the success or not of the initiative.

Furthermore, they suggest including cybersecurity quality indicators with the purpose of identifying, for example, which suppliers meet certain requirements. In addition, parameters could be added to measure the awareness on cybersecurity in order to define if the measures are being effective. As behaviours take time to change, a long-term analysis would have to be conducted.

The first step towards this would be to get all the large technological companies to commit to this type of measures. The idea is to make them see that it is preferable if they join voluntarily, otherwise the Government could impose on them at any given moment how to act.

The key is that digital products and services should be inherently secure as an essential requirement before being marketed.

Greater support for the consumer in matters of cybersecurity

In spite of the user's behaviour having a direct impact on his security and being something that cannot be ignored, the behaviour of citizens should not be considered as the sole responsible in cybersecurity. Many of the participants say that the key is that digital products and services should be inherently secure as an essential requirement before being marketed.

Security by design should be guaranteed. An example of security in the automotive industry was presented. A car is marketed with a series of basic security requirements established by law. Another thing is whether the consumer freely chooses the model that has the best reputation in security. The weight of security should also be extended to the vendors without the consumer having to bear all the weight.

06 ▼ Protect the national data on the Internet beyond territorial borders

This objective puts the spotlight on data protection, which is a commodity in this new digital age due to their mass production. Its proliferation is the result of the boom of innovative technologies and sensors connected to the Internet, together with the expansion of the "Internet of Things", which has skyrocketed the global circulation of information and increased its accessibility at any time and place. Experts urge countries to find ways to preserve the data they own in the completely global, borderless Internet environment. States need to understand the digital limits of their information and protect it as they do in the financial field, with their currencies, for example.
The introduction of a "cyber" organisation has been suggested, along the lines of the Financial Action Task Force on Money Laundering (FATF) http://www.fatf-gafi.org/. The idea would be to transfer to data protection the model used by countries part of this entity whenever they try to maintain the integrity of their financial system abroad, regardless of whether their currency is used in the United States, Russia or any other territory.

Who would integrate this cyber organisation?
It would be made up by different countries, their cyberorganisations; some newly created and others that already exist. A key role would be played by cooperation with international information and communication technologies (ICT) organisations and large businesses such as PayPal, Amazon and Google, who are involved in financial transactions and very interested in prosecuting cyber felons.
The intention is that the data be monitored by the country that has them or its companies beyond national territorial boundaries. Experts say the FATF model is an example of good practices by organisations related to issues about applying

The intention is that the data be monitored by the country that has them or its companies beyond national territorial boundaries.

legislation in the fight against offshore financial fraud. They claim that experience in other industries could contribute to present proposals in the field of cybersecurity that are easy to debate and susceptible of being implemented quickly. The success of the measures presented within the scope of data preservation would be defined by the degree of participation of the States in that cyber organisation equivalent to the FATF, as well as by its types of actions, ideas, etc. The levels of awareness and prevention achieved in data protection are also decisive. To this end, valuation metrics should be established previously to quantify the impact of the measures. The countries themselves would have to take the first step, supported by large international technological businesses.

Countries are reluctant to the exchange of information

Experts warn that, in general, it is very complicated to get countries to enter international agreements with the purpose of working together on the Internet, and, of course, to share data, even if it is to fight cybercrime. In fact, many States sponsor it, as it has been emphasised several times throughout the debate. Although most countries publicly show their position against cybercrime, when it comes down to it, many of them support it, which complicates sharing data. To this problem, we have to add that some of those that fight against this type of criminal offences are still not sufficiently ready to exchange information or to involve themselves in anything similar at an international level.

07 ▾ Criminal liability for insecure software

With regard to the software, the objective of this measure is to encourage legislation on criminal liability. The legal principles applicable to other industries should be followed in security.

Experts acknowledge that regulating this is especially complicated due to the complexity to establish global standardisation parameters for what secure software should be due to the lack of international coordination towards this objective.

How should it be legislated? The participants urge to take other industries as an example. They remind

With regard to the software, the objective of this measure is to encourage legislation on criminal liability.

us that in fields like car safety or pollution people can go to prison if they fail to comply with certain security requirements in manufacturing processes.

The lack of indicators to assess the software's quality

Specific metrics would be needed to strictly determine and establish whether a specific software is good or not and secure. In addition, legal standards against certain behaviours are also required. Not so much technical standards but best practices, although they admit that it is complicated to determine which should be the reference to set the boundary between what is secure and what is not in terms of software.

The experts warn of "insufficient tests" to check its quality and the "scarce" verifications that are carried out before the programmes are launched to the market or are integrated into new systems within the so-called "Internet of Things". There is no homogenisation either, they add.

A legislation that demands criminal liabilities in matters of software security would contribute to reducing vulnerabilities in computer systems and their use by groups such as cyber felons for their own profit.

From the point of view of its implementation, the participants warn that it would also be complicated to accurately decide if the new measures would be or not successful in their aim of confirming to which extent they contribute to reducing the number of cyberattacks.

The challenge of the international coordination of governments

This objective is crucial. Like in any other security organisation, an entity responsible for implementing whatever has been adopted at a national level would also be required. This cybersecurity authority would be created in every country under parliamentary rules, within the framework of the national law. It would work in collaboration with the industry, the academic network and the standardisation institutions.

When there are national action procedures, it is possible to progress towards the sphere of international coordination. In fact, the experts remind us that nothing is more international than software and the Internet.

For the proposal to be carried out, a "typical cascade" is needed: a political sponsor in the specific country and lobbying. A certain level of activism is required for the existing entities to think out of the box and be a bit more aggressive in this sense.

In the long-term, the experts predict a long road to cover in the world of software engineering, with intense debates about methodological aspects, the development of the programmes' life cycle or the different programming languages.

08 ▾
Quality software

The objective is to reach an agreement within the field of engineering with the purpose of progressing towards quality software. The proposal would be led by an existing company, which would be granted such competence to encourage an agreement along these lines.

> The objective is to reach an agreement within the field of engineering with the purpose of progressing towards quality software.

If we would ask the associations linked to the computer industry how they collaborate with software security, they would probably say that they are doing everything possible to improve it from a point of view of its engineering, for example, delivering conferences, writing books, etc., specify the experts.

They also mention that there is certain complacency in these software and IT professionals, who are probably enjoying conferences a lot and doing very good research, but are not equally interested when it comes to creating legislation.

An agreement is required on the meaning of software engineering

A consensus or agreement with reasonable arguments that help decide on specifications, requirements or some type of reference measure on software engineering is required. It would contribute to overcoming the difficulties around the resolution of controversial court cases when defining or not supposedly negligent uses of this software engineering. Certain professional organisations should focus their actions precisely on this objective of defining what quality software is.

Current lists of broadly accepted vulnerabilities could be used as a reference, such as those published by SANS, https://www.sans.org/, an organisation engaged in the certification of computer security, with the purpose of measuring the success or not of actions. As an example, a specific product or type of implementation could be tested against the 25 main vulnerabilities to see if it has really improved or not. The great challenge would be innovation.

One of the challenges would be to achieve stability in software engineering, although there is disagreement in the sector. Not only can the code be changed all the time, but also programming languages. The experts are raising the question

El objetivo es alcanzar un acuerdo en el ámbito de la ingeniería para avanzar hacia un software de calidad.

of why not stop continuously inventing new languages and just programme using one. The first step to implement the measures would require a certain level of activism that would encourage professional companies to do something different.

09 ▾ Promote a strategy for global cybersecurity

There is a lot of activity carried out by governments in cybersecurity. Every party involved tries to do things the best they can, but a global strategy is lacking. The experts urge launching an initiative like this one that could be led by the United Nations (UN) http://www.un.org/es/index.html. The key partners would be the INTERPOL or the Europol https://www.europol.europa.eu/. Other organisations could collaborate in this work, such as the IT-ISAC or the World Economic Forum (WEF) http://www.weforum.org/.

A clear mandate should be required of governments

According to the experts, the first step would be to adopt a resolution at a global level that grants the partners a clear mandate of support to other countries so they can establish their own strategies and to help them in their implementation. Many countries still do not really understand this. Some need to be demanded this commitment. Bringing some type of awareness on the current situation of cybersecurity is essential to establish the appropriate priorities.

The challenge would be to counteract the lack of confidence of companies and governments. It is necessary to create a sort of "sense of emergency" as well as mechanisms to establish the necessary confidence to understand this problem of global dimensions which everybody should work on.

One of the key elements would consist in narrowing the focus of the priorities to be fought. The basic issue would be to address cybercrimes, as well as their national and political connections, as it occurs in some cases. This fight should not be limited solely by the desire of doing so; the strategy should also include money investments, specific budgets, for example, those destined to INTERPOL http://www.interpol.int/es/Internet, among other organisations.

Which steps should be taken? We need to establish the appropriate channels with the governments, as well as with the private sector, in order to create a critical mass around these issues and bring awareness towards the fact that managing this is a priority. We expect the private sector to agree on which could be the organisation responsible for achieving the set targets.

10 ▾ Public-private cooperation

These types of partnerships are crucial in the field of cybersecurity. The private sector should lead this cooperation, as it has been especially harmed by cyberattacks. Who suffers more harm? This question is intriguing the experts. Of course, citizens can suffer cyberattacks, but the companies are victims of losses in the millions.

Therefore, the logical thing is that the private sector leads the partnerships, together with the major software vendors, which play a significant role in this field. But, of course, with the collaboration of the public sector.

One of the key aspects of this type of cooperation would be to improve the exchange of information about security between the different intelligence services. This should not only involve communicating the day-to-day incidents, which is a very abstract area, but also to provide specific data regarding cyberproblems that help understand the real situation of the threats. A better understanding of the real situation would help everybody better prioritise the measures that should be implemented.

> One of the key aspects of this type of cooperation would be to improve the exchange of information about security between the different intelligence services.

Cooperation is also required to guarantee a broader security from the design stage of the products, models and prototypes, with a view to establishing global standards. Many of them are emerging in different industries at a local level, although far from progressing into something global.

Indicators to evaluate the success of the measure

Data are required to demonstrate specific coordinated actions: a combined operation, resolution of vulnerabilities or the exchange of information about problems that involve a challenge.

The larger the work groups of governments, the more abstract the information intended to share with others usually is. However, the experts remind us that smaller groups usually have a greater predisposition to exchange sensitive data, and, as a result, they are more productive.

It is essential to make the parties involved understand that there is a genuine benefit for everybody in this objective of sharing information. The aim is to establish trust between the different actors. The experts also warn of the desire to avoid any excessive regulation that could kill any innovation before it is materialised.

The first step would be to press the private sector to understand the value of all these measures. And make them see that they mean advantages for everyone. The implementation of the measure would start with a nationwide approach in terms of strengthening those relationships of trust. Having completed the implementation phase, it would be then be carried out globally.

Conclusions

Chapter 3 — The future cybersecurity

Cyberspace has evolved exponentially in a very short time. Traditional barriers against cybercrime have become completely obsolete. Cyberwall-type defence systems aimed at repelling cyberattacks are something of the past, because cyber felons are at another level and use highly sophisticated techniques to penetrate computer systems by taking advantage of any vulnerability or simply by means of creative techniques designed to steal personal data or passwords of users. Protection alone on the Internet is no longer sufficient, because felons will eventually find a way to attack.

The important thing now to protect oneself is being vigilant at all times. Advanced data monitoring systems are required to detect alarm situations and identify dangers in real time in order to prevent problems. We also need much more sophisticated tools and solutions to stop threats in time, latest generation technologies that enable us to restore systems from attacks as soon as possible and many other things. But above all, a global cooperation is required.

Experts insist that the effort invested in cybersecurity has to be collective. In fact, in their list of proposals they encourage a whole array of actors to work together: international organisations that safeguard security, response teams for computer emergencies, homogenisation and standardisation organisations, national centres that supply information on cyberthreats to countries, governments, companies, financial institutions, lobby groups (consumers, industries), legislators, Internet suppliers, citizens, technologists, academics, professors, NGOs, the media, etc.

The challenge is worldwide and the commitment must also be global. The challenge is enormous, but as an Eastern proverb says, "A journey of a thousand miles begins with a single step."

Cybersecurity, a worldwide challenge Experts predictions

	Home	Citizen	Techin	Work
2015	Continue streamlining my life. Claim back more time for myself. Reduce my distraction with machines. And 'nothing' can be done to oppose that.		Improve information-shaving by encouraging companies to shave "indicators of compromise" anonimously. Provides a sort of "early warning system" about current attacks, what vulnerabilities are being used, etc. And thus allows companies to put defenses in place.	Education: create awareness.
2015 2020		For children: Just are children are told not to accept sweets from strangers that the do accept virtual goddies frm strange websites.		
2017	Start National wide simulation game competition on Cyber defense and offense in China, and provide certified training to everyone online.			
2018	MAGFA will automatically rate the quality of the software I use.			
2019	2FA and other better authentication techniques enhace online privacy.			
2020	IoT will make us more connected and less secure, and methiny can be done to oppose that.	Ability to make informed digital transactions safe in the knowledge that your transaction in secure and your PII will be wed appropriately. A connected and secure world for a better tomorrow. Able to have a secure digital life similar to real life (transparent, usual...) (e-commerce, e-government...). Advantaging digital citizens while increasing the resources and difficulty for the digital criminals. My kids will study Cybersecurity at School.	Innovation. Significant increase in regulation and enforced minimum for corporations until 2020. International bodies. Software design anual verifications. Government enforcement actions. Software and internet companies will be regulated like today.	Develop low practice group focused on targeted Cybersecurity latigation ofense. Tech industry: put security as a priority in software development , help companies to achieve that goal. Lacking my daily kick of achieve line, by getting out of continously sighting series.
2020 2025	I´d happily have an electric health record. Food diary/ fitness/ consults. I´m pessimistic of a better tomorrow without pessimy through am as yet undefined cataclysmic event that will force MAGMA to rethink priorities for a broader good to sustain them.		Better standards create more secure software but might be an economic burden SMB' s and bureucratic. Recognised international organisation for Cybersecurity providing a mandatory certificate (security conformity) and ensuring that security products meet applicable sec. directines and standards.	Transformation of the sw industrie. Business will be more secure.
2025	Accountability for insecurity will make the world I live in a slightly saler place, and it will hopefully change the moral compass for corporatioins and give support for consumers. Internet will be safe for me as a grandfather for my grandchildren coheir we will all be particulary vulnerable to cyber threats and yet higly dependent on the internet (wherever wwe choose to be in the world). More + sounder sleep.	Improve Cybersecurity as a result of any of their actions. More trusty, more efficient at work, even more hooked to internet at the expense of anything else. Cyber-ISIS will become the greatest threat to international stability and security. Appear new ways of communications and improve educational level of the people in all continents. Governments will become more dependent on citizens and more populist. Nation wide populist campaigns will threat political systems but more people engagement. Citizens online would be less vulnerable to financial loss whilst at the same time they would be more confident in their internet usage. Happy to transact online and over mobile devices with trust, safety and security. Better health based on statistical medical shared data and increasinf knowledge.		I will feel like a fish in the invisible net life has never been so unreal like a game to me. I will start a School system for the future monks or refuse camp who needs to find the new spiritual belonging and emotional heeling.

Michael

Fundación Innovación Bankinter
Paseo de la Castellana, 29. 28046 Madrid
www.fundacionbankinter.org