

Cybersecurity Trends

UK edition n.2 / 2020

VIP INTERVIEWS:

- General Anton Rog
- Rahav Shalom Revivo

 **BLOCKAPT**
Safeguarding your digital world

**Keep your business alive =
build your cybersecurity culture**



An automated, intelligent cyber defence platform

- ✓ **Integrated web-based security** – reduce financial and reputational risks.
- ✓ **Active monitoring of web-based attacks** – monthly threat reports.
- ✓ **Automated security alerts** – preventative approach to threats.

**FREE 60 DAY TRIAL
WEBSITE SECURITY**

www.blockapt.com

info@blockapt.com

BlockAPT Platform

- ✓ **Deep integration**
- ✓ **Unified security ecosystem**



Monitor – Deep integration with a single pane of glass view.

Manage – Automated threat intelligence, vulnerability management, device and incident response management on one platform.

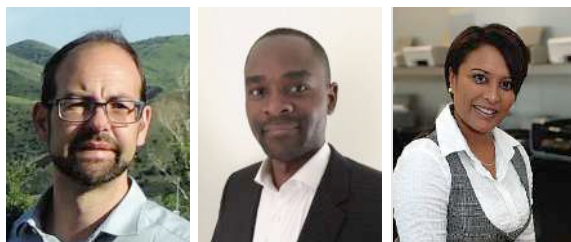
Automate – Single command & control of your devices with automated playbooks to manage responses – 24/7.

Respond – Incident response management integrated into your change control processes to prevent future cyberattacks.



Contents

2	Editorial: Time to challenge our digital culture and cyber awareness certitudes. Authors: Laurent Chrzanovski, Marco Essomba, Raj Meghani
3	“Complexity is the enemy of security” Author: Marco Essomba
6	Welcome robots! But no fear: man is something else. VIP interview with Luciano Floridi, Oxford University. Author: Massimiliano Cannata
9	There’s a war out there. Author: Nicola Sotira
10	The Israeli Cert system. VIP interview with Rahav Shalom Revivo, founder of Israel’s Cyber-Fintech Innovation Lab. Author: Nicola Sotira
12	Cyberspace: a domain to control? Author: Massimo Cappelli
16	The West is no more. Author: Olivier Kempf
19	Exclusive VIP Interview with General Anton Rog, General Director of the National Cyberint Center within the Romanian Intelligence services (SRI), Romania. Author: Laurent Chrzanovski
22	Facial recognition and defence industry. Authors: Daniel Leu & Ștefan Dorneanu
24	VIP interview with Rick McElroy, Head of Cyber Strategy, Carbon Black. Author: Elena Mena Agresti
27	Technology and law must ally for good digital governance. VIP interview with Antonello Soro, President of the Special Warrant Authority for Personal Data Protection (Italy). Author: Massimiliano Cannata
31	Where to start again? VIP interview with Domenico De Masi. Author: Massimiliano Cannata
34	Memory and Identity are strong values that we must cultivate in the digital society: they tell us who we are and where we come from. Vip interview with Pietro Jarre. Author: Massimiliano Cannata
39	Humanist manifesto for a “slow digital “ Author: Laurent Chrzanovski
43	Book reviews: Shoshana Zuboff, The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power Michel Onfray, Théorie de la dictature. Précédé de Orwell et l’Empire maastrichtien Author: Laurent Chrzanovski



Authors: **Laurent Chrzanovski,**
Marco Essomba, Raj Meghani

Time to challenge our digital culture and cyber awareness certitudes

Whilst preparing this issue of Cybersecurity Trends, we were sadly amazed by how aggressively cyberattacks grew this year. Cyber criminals have leveraged and profited by the sheer number of people stuck at home and using the net for every single activity, from ordering food and chatting with family and friends to remote working and performing daily professional tasks for their employer.

There has been a lot published about individuals being used as a principal target for “obvious” money-aimed cybercrimes, with scams, spams, phishing and spear-phishing amounts reaching a never witnessed level.

On 25th March, Marc Rogers, the well-known co-founder of Defcon, created the “Cyber Threat Intelligence League”, gathering more than 700 selected specialists worldwide to help law enforcement agencies and private companies cope with the tsunami of digital piracy. He motivated his decision by witnessing: “I’ve never seen this volume of phishing. I am literally seeing phishing messages in every language known to man”.

More recently, on 23rd May, the UN Deputy SG for Disarmament Affairs, Izumi Nakamitsu, stated that during the COVID-19 pandemic, malicious emails increased by 600% worldwide and stressed, besides this factor, that a major attack “takes place every 39 seconds”.

In an article by Henry Martin published in CEO Insight on 21st July, the top three most targeted countries by sophisticated cyberattacks were the USA, the UK and India. The UK leads on top of the criminals list as it is ranked 1st for the number of “usual-type” individually addressed cyberattack attempts per inhabitant.

In addition, we are witnessing an increase of state-targeted, heavy technological disruptive attacks - “pieces of real cyberwar” disassociated with any type of military action. As the entities are attacking with top advanced, previously unknown techniques, we should worry.

As history teaches us, once used, those sophisticated tools will soon join the arsenal of pay-per-service crimes a company could buy to hit its competitor. . .

So better to follow the example of Siemens, which ordered and published four masterpiece studies on the state of security in the petroleum field. These studies were led after their engineers stopped a new kind of attack hitting, a precise Siemens-made component and reversing its logical behavior (exactly as in the case of Stuxnet used on Iran’s uranium centrifuges at Natanz), potentially leading to a complete explosion of the whole plant, in that case Saudi Arabia’s most modern refinery.

Yet the main problem remains as humans increasingly become attached with their private IoT and Smart devices both at home and at work. No SOC will be ever able to cope with the exponential increase of threats brought in the heart of a company by its own employees, spied day and night by those “iconic devices” of our modern life, which never ever sleep. . .

As such, from robots to military-style attacks, we will continue to find counter-measures with state-of-the-art new generation of security specialists and tools. However, the human danger still looms led by the very CEOs attending sensitive business meetings with their smartphones on the table. It really is time to understand what’s going on and how truly exposed you and your business can be.

Cyberespionage is far more active than cybercrime, but a lack of proof, media visibility and direct quick consequences lead to a constant but deadly underestimation of it.

We have seen decades of digital education, cyber-culture, adult and business awareness. Today, we are surrounded by IoT and hundreds of “Smart” (or spy?) devices

What have we really learnt from the pre-5G, pre-IoT, pre-Smartphone period? Are CEOs and members of decision-making boards implementing SOCs just to feel secure? Having CISOs and CSOs on board but rarely giving them the additional technological and human resources they need to counter the ever-growing quantitative and qualitative sophisticated methods being adopted by cybercriminal groups.

Our focus for this specific issue has been an all encompassing and eclectic choice of articles and interviews with some of the most influential personalities in various domains - from robotics to secret services, from human behaviours in the virtual world, each having a corollary of related moral, ethical and philosophical questions we have to think about in order to define the digital limitations and choices we must take account of in our private and professional lives.

Only by understanding the entire social, ethical, technological makeup for each individual, irrespective of his decision making power, can we truly begin the journey to securing and protecting a company’s biggest asset – its people. ■

“Complexity is the enemy of security”



Author: Marco Essomba, Founder & CTO BlockAPT

We live in a world where technology is moving at a pace that far exceeds our ability to keep abreast of it.

The IT architecture of businesses – large or small are also having to evolve and often this creates a headache for those responsible for managing IT environments. Particularly when the cyber attackers and their

techniques to penetrate the security infrastructures of businesses are getting increasingly smarter and more sophisticated.

In the light of these challenging times, many businesses will look at bolting on additional security solutions to help mitigate against these cyberthreats. Millions of pounds get spent on adding more devices or software solutions but with this comes another challenge. The more businesses add into their security ecosystem, the more complexity they create as often these solutions do not talk to one another and remain disparate. This also comes with an increased cost burden as vendor specific expertise support services often makes the businesses more and more reliant on them.

So complexity reduces security.

BIO

Marco Essomba is the Founder & CTO of BlockAPT. A leading edge UK based cybersecurity firm empowering organisations with an advanced, intelligent cyber defence platform. The BlockAPT platform allows organisations to Monitor, Manage, Automate & Respond (MMAR) to cyber threats – 24/7. Marco’s passion, expertise and knowledge over 15 years of providing cybersecurity solutions has culminated in the design of our unique BlockAPT platform.

Developed over time as a toolkit to help small and large enterprises business security issues, BlockAPT’s platform brings together threat intelligence, vulnerability management, device management and proactive incident response management to help fight the war against cyber attackers.

LinkedIn - <https://www.linkedin.com/in/marcoessomba/>

Twitter: <https://twitter.com/marcoessomba>

Company website: <https://www.blockapt.com>



The cover of one of the latest studies on this topic © Cyber Resilience Think Tank

Over the last few decades we have moved from mono to micro to macro disparate security services, from on-premise to cloud, from manual incident response management to automated actions removing human error and improving agility. This is a natural progression which is creating additional vulnerabilities for businesses’ existing cyber ecosystems and also makes it harder for IT resource to detect where the cyberthreats are emerging from. Each access point becomes a potential entry point for infiltration by cyberattackers. Each cyberthreat becomes that much harder to address and more time consuming.

Focus - Cybersecurity Trends

Most of these cyberattackers are smart enough to realise that 90 percent of all organisation face attacks on application vulnerabilities that are at least three years old. 60 percent of these attacks target vulnerabilities that are ten years old. This becomes a cyberattackers focus point.

With many IT networks having to evolve at a rapid pace, multiple devices and security solutions already been invested in, businesses need to start changing their mindset. The hassle and implied cost of changing systems, solutions providers, etc in addition to the reluctance of changing existing processes and policies is often seen as a big, time consuming, expensive, digital transformation program.

Why fix something that is not broken right? Wrong.
Simplification improves security.

MAKE IT ~~INTERACTIVE.~~
MAKE IT ~~RESPONSIVE.~~
MAKE IT ~~CREATIVE.~~
MAKE IT ~~VIRAL.~~
MAKE IT ~~360.~~
MAKE IT ~~SIMPLE.~~

Having a centralised security management platform where digital security solutions are deeply integrated, automated reducing the reliance on businesses to track, update, act doesn't just make the management for security more efficient and effective but also helps

manage a businesses' cash flows by reducing costs in these challenging COVID-19 times.

Data is BIG money. Cyberattackers are savvy enough to realise that often vulnerability patches are not applied, software is not updated and so it becomes a gateway for them to hibernate within a businesses' network, learn the network's traffic flows and use this to decide the best time to attack. With an increased number of solutions embedded in the network, there remains an increased risk to the business of cyberattackers finding a way in. This is only going to be exaggerated in an upwards trend as we see the explosion of IoT in the years ahead.

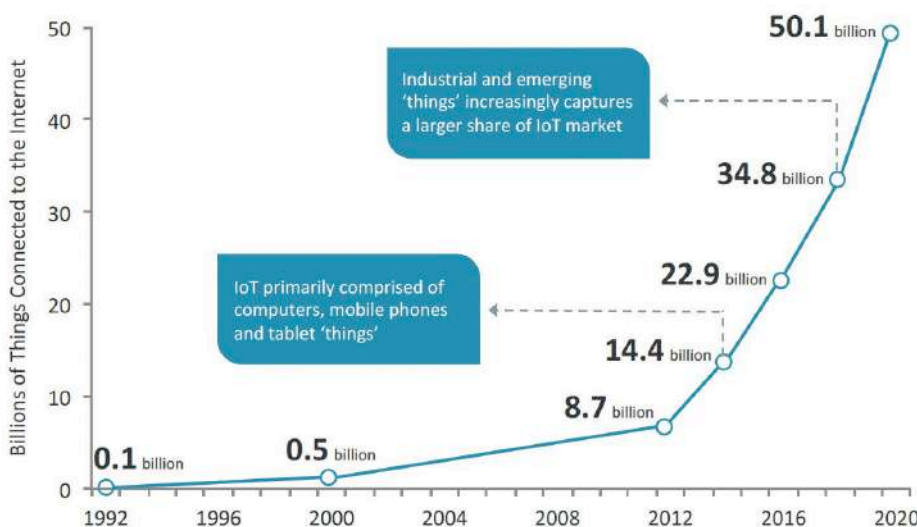
There are expected to be more than 64 billion IoT devices worldwide by 2025. By the end of this year, Gartner predicts that IoT will comprise of over 20 billion connected things. IDC puts this figure closer to 30 billion with an industry value of around \$8.9 trillion. Other studies reveal 127 new IoT devices are connected to the internet every second.

IoT is supposed to give us a smarter way of connecting and integrating devices to make life easier. What we see today is not a SMART, simplified and truly interconnected world. Far from it. It's an escalating arms race where cyberattackers rely on the sheer breadth of sensitive data across every smart device that is in use to try and compromise a company's security network and processes. The attack surface has grown exponentially, and the challenge remains as to how to centrally secure and manage every access to an end point device.

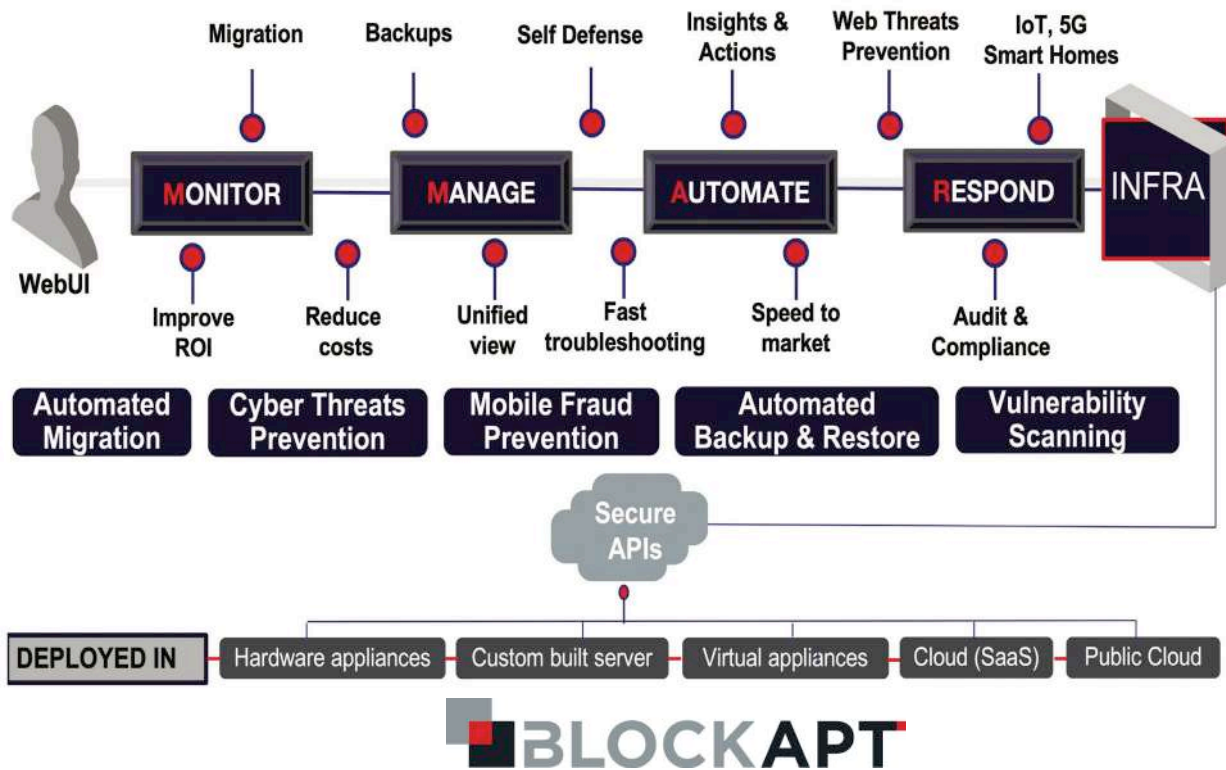
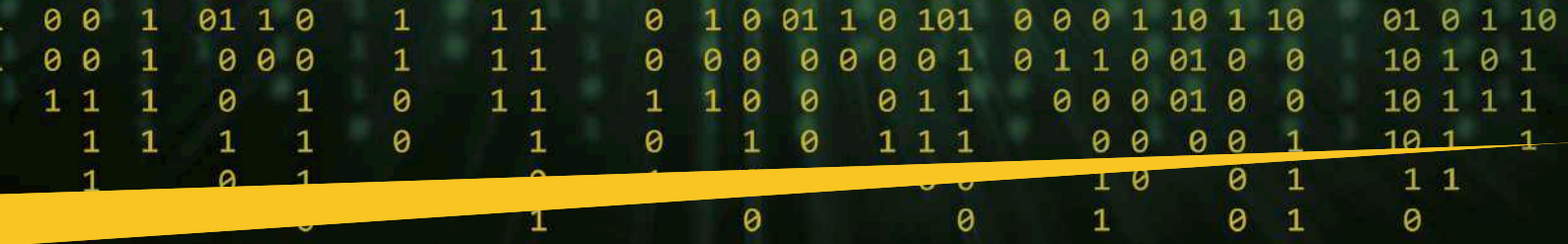
Another challenge which has effectively been forced onto businesses with the COVID-19 pandemic has been rolling out full remote working in very tight timescales. BYOD – 'Bring your own device' or is it "Bring your own disaster"? For businesses anxious to take back an element of control over disparate external mobile environments, there needs to be active security ownership across a number of areas including secure set up, professional indemnity liability cover, cyber insurance, etc.

Projecting the 'Things' Behind the Internet of Things

From 2014-2020, IoT grows at an annual compound rate of 23.1% CAGR



Cisco expects even more devices than other companies: 50.1 billion will be activated to the end of this year.



As Yoda aptly says – “Do or do not. There is no try”

The ability to **MONITOR, MANAGE, AUTOMATE AND RESPOND (MMAR)** becomes a crucial framework for businesses large or small to adopt.

Advanced threat intelligence and detection to help monitor and mitigate against advanced persistent threats, a single centralised security management environment enabling a simplified command and control process, a high level of automation triggering notifications, alerts, etc without the need for human intervention helps businesses gear up to preventing cyberattacks in a reactive and preventative way.

The cyberwar of tomorrow will mean businesses will have to deal with automation fighting automation.

With deep integration between security solutions on premise or the cloud, businesses need to reduce the complexity of their security infrastructure by having an advanced approach where an expert system doesn't just identify a threat, it has the ability to take action by blocking incoming threats and those of persistent repeat offenders. Time is and will be even more so critical as the levels of automation used by cyberattackers gets more sophisticated – an intelligent, advanced, automated system

will be much quicker to detect, take action and prevent cyberattacks than rely on humans to perform the same actions.

To do this requires threat intelligence transfer across traditional security solutions like firewalls through to web and email gateways. Open source API enables a deeper level of integration – one that can be woven into a single and robust security blanket to ensure an advanced prevention approach is at the heart of any businesses' defence infrastructure.

To be resilient against current and future cyberattacks, companies will have to be prepared for a more simplified, centralised security and automated management system with a multi layered defence approach that is preventative in nature.

So the statement 'Complexity is the enemy of security' still stands true across different scenarios.

Disparate security solutions and tools working in isolation protecting traditional security access points across businesses are not enough in today's world of cybercrime.

Having a better integrated and automated security approach is mission critical to defend against the broad cyberattack surface we face.

Sometimes the phrase 'Less is more' really does ring true – it's also about intelligently acknowledging timing for when quality over quantity works best. ■



Focus - Cybersecurity Trends

Welcome robots! But no fear: man is something else.

VIP interview with Luciano Floridi, Oxford University.



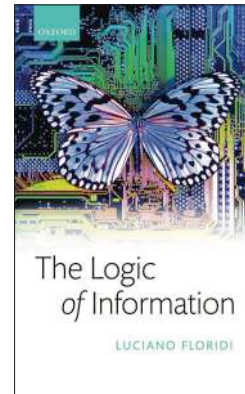
Author: Massimiliano Cannata

We realise the dimension of the infosphere, in which real and virtual are categories that mix inseparably. For this reason, no reflection on ethics applied to the development of technologies can be adequate if we do not strive to recover a systemic gaze, which must embrace all that exists, the natural environment as well as the digital universe.

According to Luciano Floridi, "there are not so many parallel ethics according to convenience rather, as great thinkers taught us, since the antiquity, from Plato to Aristotle to St. Thomas, there is ethics, a discipline whose

task it is to enucleate universal principles and values". In relation to fears and false convictions that have always accompanied innovation, the scholar points out: "we must not fear the spread of AI and sophisticated instruments such as robots, which remain at

the service of man and not vice versa. The world of signification, of articulated language, as well as the ability to solve problems with creativity, are prerogatives of human intelligence, which, unlike machines, does not collapse vertically when faced with a situation never experienced before. Individuals are, in fact, able to take the "step sideways", the horse's move made possible by the plasticity of our brain, not replicable in any laboratory". As a demonstration of the urgency of this issue, an interdisciplinary Commission at the European level is committed to providing an ethical framework on design, development, use of AI and to define the guidelines to be used by the industrial world to choose the directions of the development of digital businesses.

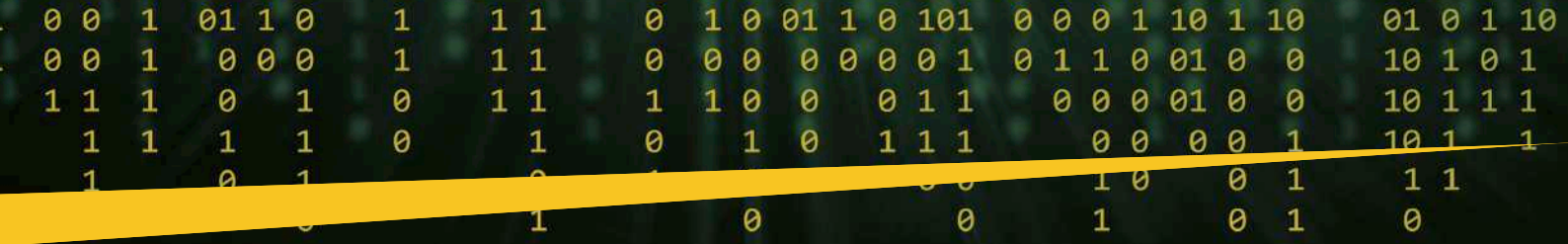


BIO

Professor of Information Philosophy and Ethics at Oxford University, Luciano Floridi directs the Digital Ethics Lab of the Oxford Internet Institute, the Data Ethics Research Group of the Alan Turing Institute and the Ethics Advisory Board of the European Medical Information Framework. Expert in information philosophy - a discipline of which he is considered as the founder -, computer ethics, data ethics, information ethics and technology philosophy, he is also a member of Google's advisory board on the "right to forget".

Professor, the message that comes from many of your writings is marked by a rational optimism that bodes well: man must relate with balance and measure to the technological apparatus, his moral and intellectual sovereignty being not in question. Starting from this assumption, in order to better understand the relationship between ethics and digital society, I would like you to dwell first of all on the definition of infosphere, a term you introduced in the nineties and that you widely discussed in your essay The Fourth Revolution. Could you explain what this is about?

Sounds like a good place to start. The concept of the *infosphere* implies, in fact, environmental considerations, which are essential if we want to talk about ethics in the contemporary world. The new generations spend more and more time connected in a hybrid space situated between online and offline, between analog and digital. Much has been written about this,



but the definition “infosphere” has aroused interest because it takes a “leap” forward. Let me give you a concrete example. Our modern kitchens are no longer like grandma’s ones, they are in fact built around traditional functional tools, from the electric oven to pots and pans, but also with electronic and digital objects. We live in a hybrid world, we have the pots, but also the electronic clock, the microwave oven, the grill to make roasted meat, the electric oven and the sponge to wash dishes together with *Alexa*. The world is made by this mix, based on the interaction of different objects. The old idea that you went into cyberspace to connect and then you disconnected to return “to earth” is now outdated, this is precisely the *infosphere*.

The digital environment is generating relationship possibilities, unthinkable in the past, opening a new chapter in the man-machine relationship. What can we expect for the immediate future?

In the past there were no processes of interaction and symbiosis with objects such as those we are experiencing. The disorientation felt by many citizens is therefore very understandable. However, we must remember that the technological tools we have at our disposal are programmed to solve specific problems, they are not particularly intelligent as we believe. We have objects that are able to learn, process data, improve their performance and, most importantly, are partially autonomous. I always use an example to make myself understood: the home thermostat is a bit “smart”, meaning it is intelligent in the sense that once set it makes me find the rooms I live in at the temperature I prefer, and at the right time, and it is also an “autonomous” tool in the sense that it knows how to optimise consumption by adjusting the on/off alternation. In the past, humans have experienced interactions with artifacts which were not autonomous at all, nor even less interactive. This can help us to understand very well the nature of the epochal change we are experiencing.

Do these “hybridised” ecosystems, which you described very well, pose any risks?

I would emphasise a few “families” of problems, which encompass a multiplicity of issues. The first part of the analysis concerns the enormous production of data related to the functioning of these sophisticated digital tools, a data that has an impact on our privacy. Another very important aspect concerns the ability, characterising robots and so-called intelligent machines, to act with a relative autonomy. But the ability to choose, act, ponder, make decisions, but also to change one’s mind or to solve a problem never encountered before is the prerogative of the individual human as a thinking being. It is clear that by placing this category of interactive and autonomous objects on the market we can create contrasts that have to do with our preferences and choices. Let’s enter, therefore, into the field of values, where the discourse becomes very delicate. It is not just a thermostat that perhaps, in order to save money, makes me find my house cold, but much more demanding and serious choices, in which the machine can be interpolated by conditioning the free will of the individual, for example by denying me a loan at the bank.

The surprising actuality of classical thinkers

Autonomy, criteria of choice, values, are the categories that classical ethics, from Plato to Aristotle, to mention only the greatest, had examined. Ancient issues that return to the present day, as demonstrated

by the work that an interdisciplinary commission of experts is carrying out on behalf of the EU. On which topics are you working on?

The group of which I take part together with 51 other experts has three very precise macro-objectives: to provide an ethical framework on the design, development and use of AI, to define an evaluation platform for AI products in order to meet ethical requirements, to develop guidelines that can serve the industrial world to guide the development of digital businesses and AI. These are all crucial issues because making correctly oriented and targeted investments. In addition to increasing the well-being of companies, this can have a very important impact on the design of social policies.



What must a machine have to meet ethical requirements?

A first requirement concerns safety standards, which no longer correspond to the logic of the old industrial system. Let’s think of *the air bag*: today all the cars must have one or more of them, meeting very precise criteria. The same applies to the design of robots, which must be consistent with socially valid criteria of use. Finally, there is the evaluation of processes and products which, before their production process, must pass the test of congruence between the definition of strategic choices, business development needs and compliance with ethical codes.

The transformations taking place are increasingly affecting skills and organisational structures. In Europe, is the social and economic context ready to make the most of the opportunities generated by the “fourth revolution”?

Your question cannot be answered unambiguously. There are dynamic and very advanced areas, in the South as well as in the North of Europe, sometimes located in unsuspected areas, which are getting very well equipped. Other realities maintain an attitude between fearful and riotous; they understand the usefulness of innovation, but they are afraid to face the change. This attitude is very widespread by the SMEs, which often do not have the necessary resources to invest in research



and innovation. This is a mistake that many governments often make as well. The “false saving” of today will force even higher adjustment spending tomorrow, with all the consequences to face.

Skilled individuals and machines

This as far as the business/enterprise topic is concerned, but how will individuals have to behave in front of wise machines which will soon know more than we do?

Let's clear the field of false convictions. Precisely because they are machines, we are talking about devices that are highly focused, as I said before, on solving specific problems. The washing machine can't even do the dishes, the little robot that cuts the grass doesn't brush the carpets. We do not feed science fiction. The elasticity, the ability to set priorities, to change a path in an original way belongs only to the human beings. Our intelligence does not collapse vertically when faced with a situation never experienced in the past. My electric coffee pot stops if the energy is lacking, while a human does not stop, he finds another solution and goes on. This flexibility that has no limits is a connotation of the plasticity of our brain, impossible to replicate in the laboratory. To put it in philosophical terms, it is because we are disconnected from the world that we are able to be intelligent, while the digital is successful only if it is well glued to the specific problems it has to solve.

So many unfounded fears?

I would say yes, because the world of intelligence and signification, as well as the richness of man's articulated language, up to the most intimate vibrations linked to his emotionality, will never be undermined by any machine.

Speaking of emotions. Many scholars argue that feelings and affectivity are also made of algorithms. Does that mean we'll fall in love with a robot if it looks at us with “sweet eyes”?

At least since the earliest days of the Greek mythology, humans have fallen in love with artifacts. Pygmalion falls in love with a statue that becomes real. As children, we played with toy soldiers believing that they were real: we started authentic battles, with emotions and suffering. The human being is made to create projections. We think of Apollo and Daphne, the metamorphosis of the nymph transformed into laurel. The man in love creates with his imagination dreamlike scenarios that dissolve to recreate themselves immediately afterwards. But be careful not to confuse reality with imagination, for instance living with the projections that we are continually generating on the human with the robot.



In your volume on the “Fourth digital revolution”, the chapter dedicated to ethics comes towards the end of the book, linked to the concept of digital environmentalism. For which reason?

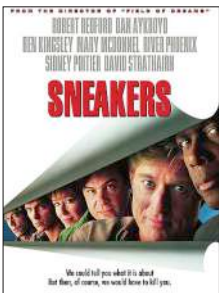
Because it is essential to consider the systemic aspects of dealing with such a vast and complex issue. We talk often about ethics of objects, of AI, of health, of enterprise, it is an arbitrary fragmentation. Ethics is an all-encompassing concept. I would like, therefore, to examine everything that concerns the digital universe, a way too important sphere to be relegated to closed circles dealt by super experts. The Greek culture applied the principles of ethics to the whole being, without fragmentation, is still topical.

In our conversation, the relevance of philosophy has been called into question several times. The renowned Professor Giuseppe Cambiano just wrote a brilliant essay, Sette ragioni per amare la filosofia (Seven reasons to love philosophy) listing the reasons for loving a discipline that seemed to be in crisis until a few years ago. “Asking questions, using words, searching for answers, appreciating disagreements, opening boundaries, understanding other times and other worlds” are the reasons why we must return to philosophical speculation. Do you share Cambiano's vision?

The reasons well explained by the great historian of philosophy can certainly be shared, but I would add a definition that is decisive for me: philosophy is above all *conceptual design*, this is an aspect of its eternity. It creates, articulates and manipulates ideas and theories, interpretations and points of view, to give meaning to the world around us, and to our individual and social lives. Popper said: all life is about solving problems, I would say that all life is about identifying new avenues of inquiry to go further, to move the frontier of knowledge into unexplored territories. This is what I mean by *conceptual design*, this is the human being, who “Pirandello-style” stirs up “the armory of the spinning wheel”, urging his intelligence to find meaningful answers to the eternal dilemmas that from the most remote times stir the consciousness of the living humans at all latitudes. ■



There's a war out there



With this very phrase, the hacker Cosmo, played by the excellent Ben Kingsley, marks one of the most pregnant scenes of the movie "Sneakers" (1992). In the movie, we see a struggle to take possession of the SETEC Astronomy device, a device capable of decoding all cryptographic systems. Agent Bishop, Robert Redford, retrieves the device and during the last verbal confrontation with Cosmo, the latter gives us this maxim "There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information!"

This movie, whose viewing I recommend, was certainly way ahead of its production year, dealing with some very

BIO

Nicola Sotira is General Director of the Global Cyber Security Center of Poste Italiane and Information Security Manager in Poste Italiane. He is in the field of information security for over 20 years with experience in different international companies. In the previous experience, Nicola Sotira was sales Director UC&C & Security Practices in Westcon Group Italy and VP Sales Italy in Clavister AB. Professor at the Master in Network Security of La Sapienza University since 2005, Member of the Association for Computing Machinery since 2004. Promoter of technological innovation, he collaborated with several startups in Italy and abroad. Member of "Italia Startup" since 2014, he advises the conception and the development of several mobile services. Nicola is also a member of the Oracle Security Council.

Author: Nicola Sotira

actual issues: if you read the daily chronicles of these days, you will discover that the film anticipates many of the issues every journalist or researcher is facing today. Encrochat, for instance, is a company providing end-to-end encryption solutions to ensure the anonymity and security of its users. The Android terminals, made available by the company, are modified in their hardware to prevent intrusions in the GPS and video camera of the device. However, the system also guarantees criminal organizations a "secure" management of their traffic with a ZERO risk of being intercepted. Police decide to spoil the party, by compromising the system and deciphering the communications running through it. The results are on many press releases: "...the operation led to the arrest of 60 suspects, the seizure of large quantities of drugs together with the dismantling of 19 drug processing laboratories".

But what happened in April in Israel? We are not talking about COVID, but about the national water system that has been attacked, presumably by Iran,



The Eskol Water Filtration Plant, Northern Israel ©The Times of Israel

trying to increase the levels of chlorine in the water flowing to the residential areas, a cyber attack hence targeting civilians.

Anonymous Israeli sources have reported to the newspapers that the attackers have violated the software in charge of managing the pumps by masking the traffic passing through American and European servers in order

to make it more difficult to attribute the attack.

And as you can imagine, it did not take long to witness a reaction. On May 9th, all the maritime traffic at the Iranian terminal at Shahid Rajae's Iranian harbor had been inexplicably blocked.

All the computers that regulated the flow of ships, trucks and goods went into a lockdown at the same time, creating countless problems to the navigation channels and to the road network leading to the facility. As a result of the analysis of this attack, Iranian experts have acknowledged that they were victims of a computer intrusion that knocked out their IT system. The port was



The Rajae port © IFP News

the victim of a cyber-attack attributed to Israel.

There is a war out there, a digital war that is being fought on the data stockpiles and on the whole digital ecosystem, an ecosystem that is now becoming fundamental for the competitive development of any country, as the pandemic has shown us.

An ecosystem that is still fragile and needs to be made more and more resilient. Because this time, it is not those who have the most bullets who will win the war... ■

The Israeli CERT system

VIP interview with Rahav Shalom Revivo, founder of Israel's Cyber-Fintech Innovation Lab



Rahav Shalom Revivo

Author: Nicola Sotira



The National Financial CERT is responsible for offering a value-added cyber security to the financial ecosystem - through cyber threat intelligence activities at national and international level, with 24/7 available incident handling teams that can support such organisations in case of need, but also by issuing recommendations on how to mitigate threats.

The focus of the National Financial CERT is to secure the "end to end" of all financial processes identified as fundamental to the functioning of the financial ecosystem, such as: cash flow, credit card transactions and much more. The status and resilience of financial processes determine the definition of priorities and the very financial ecosystem itself.

Nicola Sotira: *The "cyber" scenario is constantly growing and organisations should be increasingly prepared to face new threats. In this context, what is the role of a modern CERT, particularly in the financial sector? Which are its priorities?*

Rahav Shalom Revivo: In Israel, we have a National Financial CERT that is part of the Israeli National CERT.



Nicola Sotira: *Preventive activities play an important role. Could information sharing improve the resilience of financial services? Are you working in this direction?*

Rahav Shalom Revivo: The key to success is to be prepared for any danger that may occur. Therefore, in addition to cybersecurity drills for specialist teams, the Ministry of Finance is promoting cyber resilience exercises for financial leadership. Just a year and a half ago we conducted an exercise in which the Minister of Finance, the Manager of Israel's Central Bank, all financial regulators and representatives of the private market participated, responding together to scenarios of dramatic cyber attacks with impacts on the financial ecosystem and their consequent need to make the necessary financial decisions.

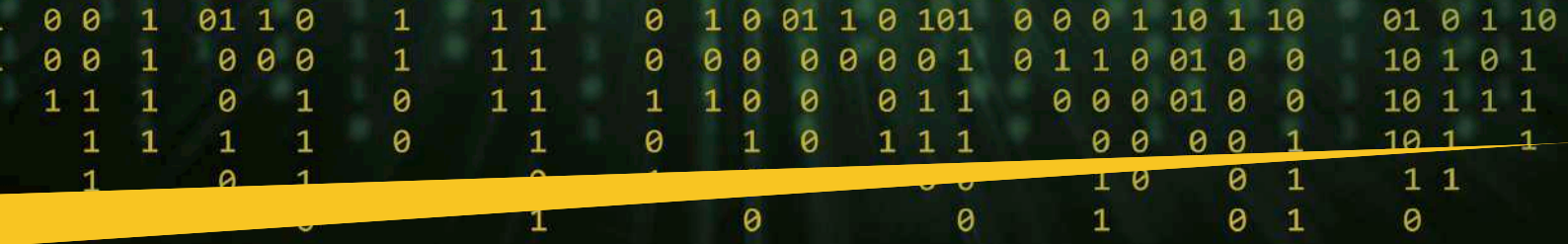
In addition, the Financial CERT provides various recommendations to financial institutions on how to protect themselves. The recommendations range from reporting a specific vulnerability, domain or IP address to be blocked, to identifying new attack methods, vectors, etc.

It is at the latitude of the financial institutions themselves to decide whether or not to follow a specific recommendation. The interesting thing about the Israeli National Financial CERT is that we are not a regulator.

BIO

Rahav Shalom Revivo is the founder of the Cyber-Fintech Innovation Lab within the Israeli Ministry of Finance, the first initiative in the world using government resources and data to promote Cyber and Fintech start-ups with an open innovation platform. Rahav is part of the Israeli National Financial CERT and has over 20 years of experience in coordinating research and development teams, with a focus on Cyber, Fintech, DevOps and Cloud solutions. She is also an expert in designing, building and delivering business solutions for IT organisations. Rahav is also actively working to promote the role of women in the technology sector internationally and nationally. In 2019, Rahav was listed by Lattice80* among the world's top 100 women in the Fintech industry.

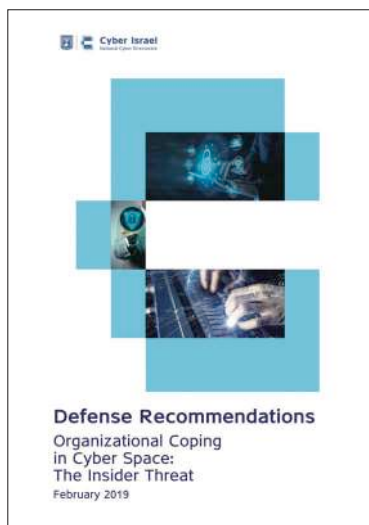
*(<https://www.lattice80.com/top-100-women-in-fintech-2019/>)



Therefore, the cooperation of financial institutions with us is completely voluntary. However, 100% of banks, 100% of credit card companies and all large and medium-sized insurance companies are linked to the Financial CERT and benefit of its services and report incidents.

Nicola Sotira: The human factor is changing from a vulnerable point to the first line of defence against cyber attacks. Is your CERT investing in awareness and training?

Rahav Shalom Revivo: It is true that one of the weakest links in cyber security protection is the human factor. The user is deceived and induced to click a link or open a malicious email, plug unscanned USB keys in a laptop, but the risk can also be posed by an unhappy employee who could become an internal threat. The Israeli National CERT is working directly with the public, creating awareness. The Financial CERT cooperates directly with CISOs and SOCs. It is the responsibility of CISOs to educate and even test the employees of a whole company.



The Israeli National CERT is working directly with the public, creating awareness. The Financial CERT cooperates directly with CISOs and SOCs. It is the responsibility of CISOs to educate and even test the employees of a whole company.

Let's take the risk from another angle. As we focus on end-to-end financial processes, we want to make sure that each of the links they contain is protected, which means that not only financial institutions should be protected, but also the third-party providers who are

themselves part of these processes. That is why we have a specific unit within the Ministry of Finance that focuses on addressing cybersecurity in the financial supply chain and is working with the most critical suppliers who are involved in critical end-to-end financial processes, executing regular surveys on cybersecurity and giving them recommendations to follow in order to ensure they are more resilient.

 **Ministry of Finance**

Cyber Security & Continuity Guidance Unit for the Financial Supply Chain

Nicola Sotira : What is the role of new technologies such as artificial intelligence, machine learning, blockchain, 5G? Can these tools really help a CERT in its strategic operational tactical activities?

Rahav Shalom Revivo: The National CERT and the Financial CERT are using new technologies such as blockchain, AI and so on, in order to protect the financial ecosystem and the Israeli IT sphere in general, both through "self-developed" products and through the use of new released products.

Nicola Sotira: Innovation is everywhere. How do you participate in innovation?

Rahav Shalom Revivo: Absolutely, innovation is everywhere, and as a country regularly investing in it, we wanted to leverage the unique data

and expertise we have at the Financial CERT to promote fintech and cyber startups and help Israel to become a leading 'fintech nation' exactly as it is already known as a *cyber nation*. That's why we launched the Fintech



- Cyber Innovation lab program. This private-sector lab uses government data from the cyber-financial sector for fintech and cyber startups enabling them to develop, test and demonstrate their own products with an even stronger connection to security and "live" events. We are the first country in the world to provide this data to industry and this activity is seen as a natural evolution of the skills we have acquired. We want the private sector to have such expertise for its own needs and requirements. That is why we have published a competition which will close in mid-November: hence, the laboratory should be up and running in 2020.



Nicola Sotira: How can a real collaboration between financial institutions be improved? GCSEC has created the CERT STAR initiative, a programme of technical-operational meetings dedicated to CERT analysts and operators to improve their collaboration and skills. Do you have similar initiatives?

Rahav Shalom Revivo: We believe that sharing information is one of the key tools to become more resilient. That is why the Israeli National Financial CERT is actively investing in this - in addition to regular meetings of its members, we are sharing information not only with the local financial ecosystem (which are our customers), but also with international financial institutions, such as *Poste Italiane*. Such collaborations can make the difference: we are much weaker if we keep being "silo islands" where each one only takes care of its own exclusive territory; cyber attacks are like tsunami waves, they damage everything they encounter on their way. If we remain united, each of us will be better protected. ■

Focus - Cybersecurity Trends

Cyberspace: a domain to control?



Author: Massimo Cappelli

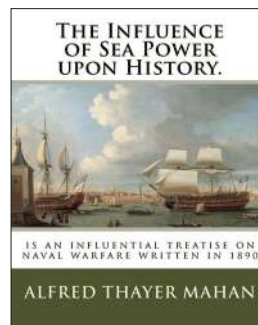
we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea...

The above mentioned appointment reinforced the belief that cyberspace had become another domain of conflict. We have already dealt with this topic in some conferences and also in the newsletter of the GCSEC Foundation. Yet we think it is useful to briefly recall some theories that have influenced nations in the past and that could also apply to cyberspace.



In May 2010, the U.S. Secretary of Defence announced the appointment of General Keith Alexander (former General Director of the NSA) as the first commander of the new U.S. Cyber Command.

In Article 70 of the Warsaw Declaration published in July 2016, NATO affirms that cyberspace is a new field of conflicts "...Now, in Warsaw,

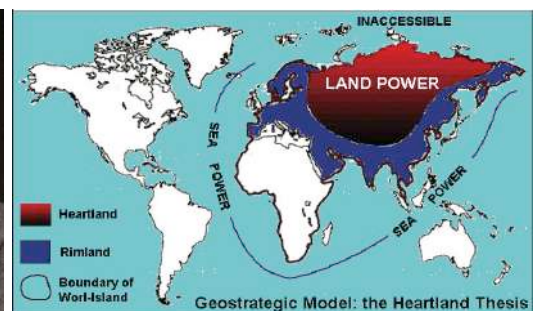


The U.S. Admiral **Alfred T. Mahan** theorised that to dominate the world, it was necessary to prevail on the seas with well-equipped fleets. At the end of the 19th century and the beginning of the 20th century, the governments of the United States, Germany, Japan and the United Kingdom began a heavy campaign of naval reinforcement.

In the early 1900s, a renowned British geographer, **Sir Halford Mackinder**, claimed that there was a pivot area of the world, called *Heartland* ("Heart of the World"), identifiable with the territories of the former Soviet Union. Controlling this area would have allowed the control of the "Island-World",

BIO

Massimo is Operations Planning Manager within the GCSEC (Global Cyber Security Center, Rome). He coordinates, as PMO, the research and education activities of the foundation. Since January 2017, he leads the CERT and Cyber Security of the Poste Italiane within the Information Protection Department. After economic studies, he obtained PhD in "Goeconomics, Geopolitics and Geohistory of border regions" focus on Critical Infrastructure Protection Programme and a Master in "Intelligence and Security Studies". In the previous experience, he assumed the role of Associate Expert in Risk Resilience and Assurance in Booz & Company and Booz Allen Hamilton. He also acted as consultant in several think tanks, for industrial groups as well as for the NATO.

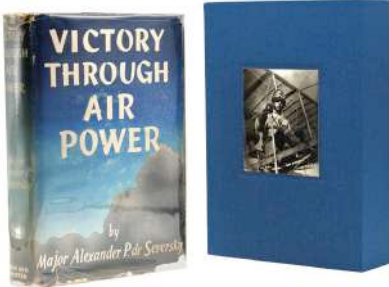


as this was an area inaccessible to naval fleets. Mackinder's theory was also taken up by Nicholas Spykman. Spykman claimed, however, that it was much more important to take control of the *Rimland*, the region that encompasses the *Heartland*. Controlling the *Rimland* allowed to control the *Heartland* and therefore the whole world.

US President Truman was influenced by both theories and used a *containment* strategy towards the Soviet Union.

However, geopolitical theories are heavily influenced by technological development. Advances in aeronautics and missile technology and, more

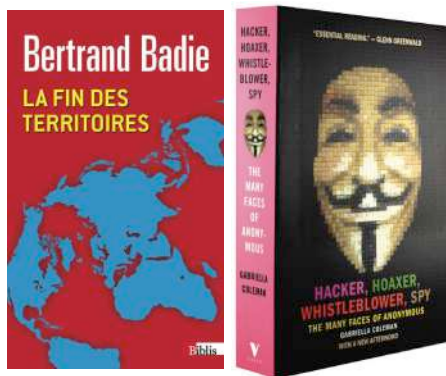
than other developments, the advent of the nuclear era, have led to new theories. Yet, the role of supremacy remained at the roots of all the theories.



Already in 1942, the Russian pilot **Alexander P. de Seversky** had highlighted the importance of air dominance to take control of the world. Therefore, he divided the world into two great circumferences whose centre is represented by the American and Soviet industrial poles and whose radius is defined by the range

reachable by the bombers available at the time. The disintegration of the Soviet bloc challenged the theories of the past and changed the cards on the table. At the end of the Cold War, although borders had already begun to falter as a reference for the control of the world, we witnessed the emergence of new considerations in which politico-geographic limits began to have less and less relevance.

Bertrand Badie expressed this concept by observing wars and protests in different geographical areas where flags of different nationalities waved



together, united by religious ideologies or other triggers. The increasingly widespread and present communication surrounding us has brought to light affinities between different peoples but also their common problems. The propagation of ideas has found new vital lymph with the increasingly massive spread of the internet.

Gabriella Coleman, an anthropologist, has observed this phenomenon by studying the *Anonymous* movement. The *"We are Anonymous"* movement best expresses the shift to new realities. This is a movement that is diverse in terms of religion, nationalities, and ethnicities or social backgrounds, yet fed by the same motivation whether it is the *"Arab Spring"* or the *"war against Multinationals"* or the revolt against government agencies. From time to time, its participants vary according to the motivation, so it can be considered as a movement, even if never the same and always different.

The rise of the Internet hence added a new conflict zone, cyberspace, which joined the old terrestrial, maritime, air and space domains.

The geopolitical theories of the past foresaw the control of a determinate physical space to control the world. That may also be true in this case. If so, we would have to observe cyberspace to understand who is dominating it. Digital space is virtual, but its creation and development is still based on physical and logical assets from which it cannot free itself. Therefore, if we were to hypothesize who is winning the *Digital War* we would have to understand who holds the majority of the digital *"tools"* to declare who has the supremacy. This is not so simple because we are talking about a multitude of public and private actors that develop every day virtual *"spaces"* from where they can provide services or sell products.

If we had to apply the theories of the past, we could start by verifying the penetration rate of certain technologies compared to others, as well as their 'nationality'. This would give us an idea of how different nations are present in the world. Just as an example, we have looked at some statistics. The exercise is purely illustrative and has no scientific basis. The same sources consulted have not been compared, nor has the reliability of the source or the reliability of the news been verified. Despite this, the results of this first research are clear and we do not think they differ much from the reality delivered by a long scientifically-made study.

Let's start with the operating systems. The OS that dominate the market are those of Microsoft (USA) with a market share of 80%, followed by Mac OS (USA) with a percentage around 16-17%. The geographical distribution is impressive, especially for Windows, reaching even countries such as Russia.



On mobile operating systems, the predominance is always American, with Android (USA) situated over 70% and iOS (USA) over 25%. The same domination is valid for U.S. based social media, where Facebook (USA) dominates and stands out over the others with 62%, while in second place we find Twitter (USA) with 14%. If we look at the search engines, Google (USA) is ahead with 92%, followed by Bing (USA) with about 2%.

If you switch to server or cloud services, the numbers are always extremely in favour of the United States. In the Server world, according to the data found on Statista for the first half of 2019, 55% of the market is held by US

Focus - Cybersecurity Trends

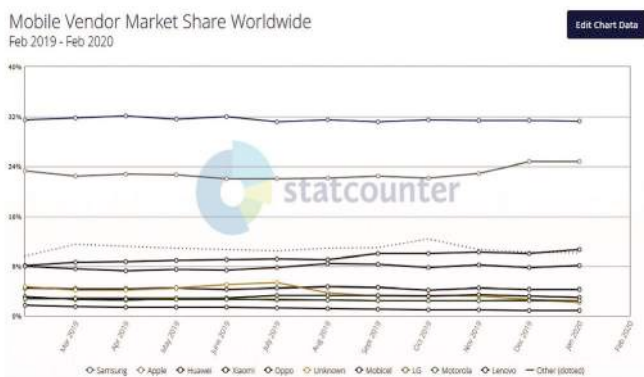
companies (Dell, HPE, IBM, Lenovo, Oracle, Cisco), while the share of Huawei (China) is around 5.4%. In the Cloud world, Amazon AWS (USA), Microsoft Azure (USA) and Google Cloud (USA) hold 56% of the market while the Alibaba Cloud (China) gathers only 5.4%.

Worldwide cloud infrastructure spending and annual growth
Canalys estimates: Q4 2018

Vendor	Q4 2018 (US\$ billion)	Q4 2018 Market share	Q4 2017 (US\$ billion)	Q4 2017 Market share	Annual growth
AWS	7.3	32.3%	5.0	32.2%	+46.3%
Microsoft Azure	3.7	16.5%	2.1	13.7%	+75.9%
Google Cloud	2.2	9.5%	1.2	7.6%	+81.7%
Alibaba Cloud	1.0	4.2%	0.6	3.5%	+73.8%
IBM Cloud	0.8	3.6%	0.6	4.2%	+27.6%
Others	7.7	33.8%	6.1	38.9%	+26.7%
Total	22.7	100.0%	15.6	100.0%	+45.6%

Source: Canalys Cloud Channels Analysis, February 2019

These data comparisons could be done for all types of devices or applications to see their market share and geographical distribution. If we move for example to the mobile market, Samsung (South Korea) has a market share of about 32%, followed by Apple (USA).



On the website www.shodan.io, known to all cyber security staff, you can enter names of specific models of IOT devices in order to understand their geographical and numerical distribution, obviously for those that are reachable via the net.

This overview does not take into account the IoT market and the spread of 5G, which could also partially change the national percentages, mainly by increasing China's share.

A further consideration must also be given to the raw materials used to produce the chips, such as silicon.

As resources are limited, a supply race is underway. In this case we are no more in the virtual but in the physical world. The recovery of these resources through recycling management systems will also be extremely important.

Alas, this is a key issue on which there is not much awareness in the EU, at this very moment.

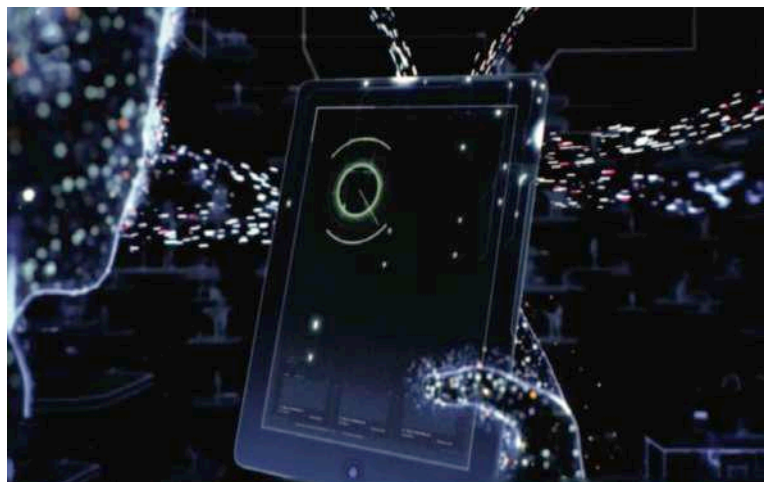
We should also keep in mind that most of the manufacturing of products made with the above mentioned elements take place in Asia and therefore the possibility that the integrity of the product will be compromised is a very serious option. Static and dynamic analyses on individual devices are expensive and often lack analysts capable of doing so, in addition to the fact that it is not feasible for all devices, especially those used by end users. The ownership of these assets is mostly private. They are companies and citizens who use most of the above assets. Gus Coldebella, during a speech in 2019, recalled that 85% of US critical infrastructures are privately owned.

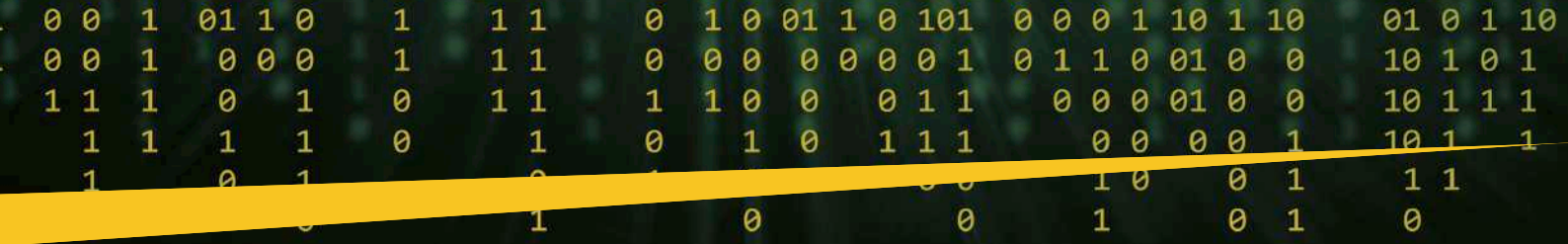
Companies in different countries are outsourcing their data to foreign cloud services. This is also happening for operators of essential services, posing a serious problem in all States because the first line of defence against potential attacks are precisely the private companies, often not adequately supported by governments. Governments often focus on defining or implementing industry regulations instead of operationally supporting companies.

Let us resume and draw scenarios on what has been said so far:

Some geopolitical theories leaned towards controlling certain domains to control the world. Technology and the disintegration of the Western and Soviet blocs led to a change of the global landscape. The advent of the Internet was *disruptive*. The cyberspace is a space without boundaries where public and private provide services of any kind. US digital products are predominant compared to other countries. China could narrow the gap with both the implementation of 5G worldwide and thanks to its massive production of IoTs, which are also distributed worldwide and whose security is often very weak. Europe is not a power in this domain, it is a technology user, and as far as the production of hardware and software is concerned our continent can in no way be compared with China and the USA.

Currently, cyberspace is a perfect field for espionage activities. There have been attacks aimed at compromising or disrupting services, for example in Iran and Ukraine. The real battle, however, is the one devoted to gathering information. Once, such information was written on paper documents, now it travels in the form of data. In fact, a huge part of the "Advanced Persistent Threats" mainly target data and information concentrators, such as social networks or cloud services. Spying is less risky, hiding behind a keyboard





and using anonymous connection services or compromised servers. The spy game has never stopped but in some ways it has become easier and cheaper.

What would happen in case of a world war?

Superpowers could become more aggressive and thus exploit private assets for their own purposes. The principles of TRUST, TRANSPARENCY and SECURITY would be overshadowed. The primary objective would be to dominate the adversary, take control of its infrastructure, carry out attacks bringing the hostile country to its knees. Thanks to the Internet, this could be done without destroying critical infrastructure, but making it temporarily unusable.

To do so, it would be enough for private companies to send official packages to update their technologies, but in the same time able to install backdoors, download ransomware, change control parameters and so on. Cloud service providers could deny access to customers in the area affected by the conflict, blocking almost all essential services. Owners of search engines or social networks could inject false news and manipulate public opinion. Of course, any CEO who would allow this kind of action would be a fool. It would be a commercial suicide, unless his behaviour is imposed for State reasons of *force majeure*: war.



In this latter case, a few considerations to keep in mind:

- ▶ United States 1917, Japan 1938, United Kingdom 1939, the “National Mobilization Laws” forced strategic private industries in their respective countries to come under state control through a nationalisation law.
- ▶ February 2010, the People’s Republic of China issued the “National Defence Mobilization Law”, in which basically the National People’s Congress Standing Committee approved special measures to supervise and control key Chinese industries and areas.

In case of war or necessity, nations can take advantage of their private companies for national interest purposes.

The underground warfare that is being fought is to collect information and collect tools that can pierce any platforms. As Andrea Zapparoli Manzoni, Executive Director of Crowdefense, said in an interview, 87% of *0 day exploitable vulnerabilities* are still considered *0 day*. It means that they have not been made public. An average of 1 out of 20 vulnerabilities is

published worldwide, letting many doors wide open to criminals or State actions.

And there, of course, we find governments, private analysts, as well as companies, looking for the “unknown” *0 days* that can be used for attacks. The greater diffusion of some technologies compared to others represents a two-faced medal. On the one hand they are potential exploitable weapons in case of war, on the other hand they represent very large attack surfaces that could contain critical vulnerabilities also exploitable by the enemy.

Each country has the task of identifying its essential services – we must insist here: services, not operators!



Each service is based on a chain of physical and virtual assets. Once the services and chains have been identified, nations should simulate stress-tests on them, assuming compromises, lack of delivery, a.s.o. This should allow the creation of impact scenarios useful to design and build precise resilience and continuity plans. This work should be done by assuming an essential attitude towards any foreign vendor: the lack of TRUST - at least until contrary is proven.

We need to put ourselves, daily, in the worst case scenario: only then we will understand which improvements we need to make to your “country-system” resilient to shockwaves and their catastrophic impacts. ■

▶ Alfred T. Mahan: “The influence of Sea Power upon History”; “The Interest of America in Sea Power

▶ Heartland figure: <https://birminghamwarstudies.wordpress.com/2012/06/04/215/>

▶ Alexander P. de Seversky: “Victory Through Air Power”

▶ Bertrand Badie: “The End of Territories”

The West is no more

Author: Olivier Kempf



The original article, reserved for subscribers, has just recently been published in the bimonthly LA VIGIE (n. 146, 10th of July 2020 p. 4-6). For more information: www.lettrevigie.com

Our warmest thanks go to Olivier Kempf for his kindness and for the permission given to reproduce, translate and publish this article exclusively in the different language editions of Cybersecurity Trends.



The West was, at the same time, a civilisation, a way of thinking marked by doubt and science, a world domination and a geopolitical device focused on the alliance between Europe and America. But both America and Europe are in deep disarray while the ties between the two sides of the Atlantic inexorably unravel. The West is no longer, if not as a remnant of an ancient but already extinct world. Let us become aware of this in order to build a new system.

The reader of our strategic letter "La Vigie" is aware of our mistrust towards the word 'Occident'. We use it, of course, but by default and always try to find another word instead. Indeed, this very West, which seems to go without saying, has become an outdated geopolitical category that misleads us and causes many mistakes. Instead of imitating Spengler and talking about the decline or the end of the West, let us simply note that the West no longer exists. It is simply, at the end.

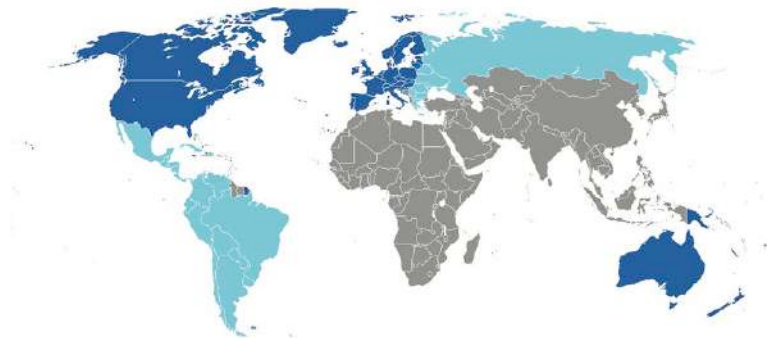
What was the West?

Like all polysemic terms, the West has many meanings. In a remarkable little book, Roger-Pol Droit tried his hand at this genealogy. The West has first of all a cultural and almost philosophical root: it belongs both to the Greco-Roman world (both Antiquity but also its philosophers, its laws, its conception of politics and already a certain geographical extension of the northern Mediterranean) and to the Judeo-Christian world, insisting then on the religious substratum of our culture and notably on Christianity, according to Catholic, Orthodox or Protestant obedience. Judaism is cited as much for its historical antiquity as for its presence in Europe, while Islam is not mentioned in this "Jewish-Christian" category.

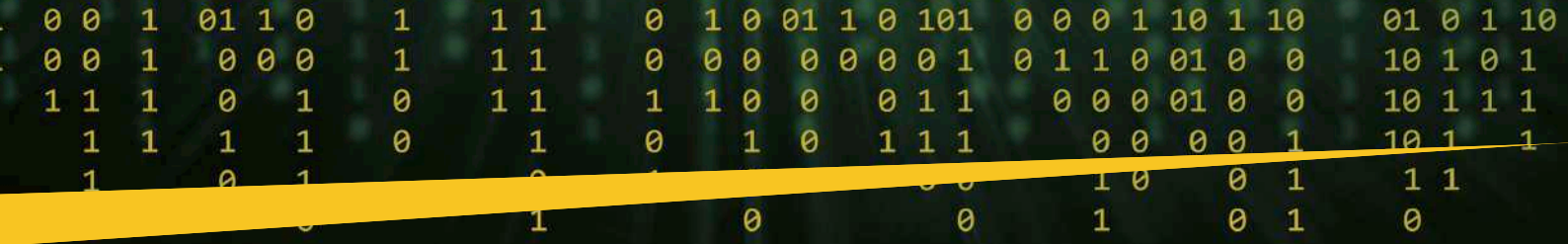
If we want to find a common point between these two meanings, let us mention the three Romans: the one of Italy, which alludes to both the Empire and the Papacy, but also the one Byzantium and finally the one of Moscow, the third Rome. The West would find its source in this civilisational area stretching from the Mediterranean to the North Pole, from the Atlantic to the borders of Asia: what has been designated a time as Christianity and soon after as Europe.

BIO

After a military career where, in addition to operations, he was involved in international affairs and transformation, General (ret.) Olivier Kempf advises companies and organizations on digital strategy and cybersecurity issues (Truchements consultants). Author of "Introduction à la cyberstratégie" (Economica, 2015), he is publishing director of La Vigie, a strategic synthesis company he founded in 2014, which publishes a bimonthly newsletter and writes various studies for its clients.



The western world according to Samuel P. Huntington's 1996 Clash of Civilizations © Wikipedia



The time of Empires

But just as *“Rome is no longer in Rome”* (in *Sertorius*, by Corneille) the West is no longer in Europe or, more exactly, it has no longer been reduced to Europe. Indeed, what has been called modern times begins with a double invention: that of printing and that of the American continent. In this way, the West will take on two new dimensions: first of all, geographically, it will extend to a continent, America, according to several manifestations: who does not see that Latin America has little to do with North America and especially with the United States? But beyond this first colonisation (of settlement, it should be noted), another colonisation takes off first in the 18th century and even more surely in the 19th century: then Europe (and at the end of the period, the United States) takes “possession” of the world according to a first globalisation which was a westernisation.

This time of empires gave the West a universal domination that still persists today. The footprint is so strong that it explains many contemporary phenomena.

A way of thinking

But in addition to this taking possession of the world, with the American relay, modern times are also seeing the development of a new intellectual approach to things and to the world. It certainly goes back to ancient philosophy and its medieval evolutions (quarrel of the Universals between realism and nominalism) but with the Renaissance, religious concerns found new paths: Protestantism, of course, but also a new relationship to the world, to science, to reason, which was to lead to the Enlightenment of the eighteenth century and then to the Auguste Comte and the positivism of the nineteenth century. For if there is one intellectual trait common to the modern West, it is that of doubt and questioning. It is not simply the premises of the scientific method but a criterion of the Western man. This is perhaps what will remain of the West, once it has disappeared geopolitically. Because the West has also created the scientific method and therefore a relationship to science and technology.



The Westerner is the one who designs, manufactures and disposes of tools, machines and other artificial objects: this way is so widespread, including in other civilisations, especially in the Far East (look at Japan, Taiwan or China) that it is no longer exclusive. However, it is so permeated by it that it relativises everything to the point of excess. From now on, the West is the one that gets drunk by denigrating itself, in a masochistic relationship from which it draws its supreme pride and what it believes to be its superiority over the world.

Liberal in essence

From this relationship to the world comes a “liberal” conception in every sense of the word: political as well as economic and moral (or more precisely, in terms of morals). This systemic tolerance has given rise to democratic regimes, but also to liberal economic systems and social organisations that are still the common feature of many Western regimes. It should be pointed out here that this is not only a “white” world, which is often equated with the West: the West has traditionally included Europe and America and former white colonies (Canada, Australia, South Africa). But in the post-war period, Japan was assimilated to the West thanks to the motive that it had a political and economic system similar to its Atlantic counterparts.

An Atlantic West

The fact remains that the matrix of this West with Greco-Roman, Christian, scientific and liberal roots is geographically concentrated around the Atlantic and in particular the alliance between the countries of Europe and those of North America: much has been said about the passage of power between old Europe and America, which was the history of the 20th century and which became institutionalised in the Atlantic Alliance. We are talking here about the political tool (and not the military organisation that is NATO). But is it by chance that many voices raised recently to point out the current uselessness of the Alliance? Recent frictions between France and



“
What we are currently experiencing is the brain death of NATO... You have no coordination whatsoever of strategic decision-making between the United States and its NATO allies. None.
President Emmanuel Macron speaking to The Economist
”
Heslon 34

Turkey have seen Paris remind us that the Allied silence confirmed the “brain death” evoked last November by President Macron. Yet, symbolically, the death of the Alliance confirms that there is no longer a West.

The Island-America

To the dismay of many Europeans who have always believed in the unbreakable bond of the American alliance, President Trump is showing a new path, already initiated by his predecessors. Whether Trump is re-elected or not, American disinterest in Europe is



enduring. Europe is neither a problem (it is China) nor a solution. For D. Trump, the solution lies in questioning a certain form of globalisation and multilateralism. *Make America great again* was his campaign slogan: it has to be said that America is more isolated than ever, that it no longer convinces by its power and that it appears singularly divided, in a very worrying way.



President Trump at the 2018 NATO summit © IUVMPress

A lost Europe

As for Europe, one does not need to be a great analyst to note its disarray and deep disunity, despite the stiff certainties of many "Brussellists", convinced that it is the beacon of History. Here again, we must take care and to distinguish the EU from Europe, as well as to note that the current European institutions are not really satisfactory, to the point that Brexit sounds the death knell of a certain method. The new Commission would like to be seen as

geopolitical, a word that has become chic but whose political manifestations are not seen. What should we say to America? to Russia? to China? to Africa? and quite simply, what should we say to the people of Europe? Let us note that we have few answers to these five questions, other than to repeat that the EU is a unique experience and that we live there better than anywhere else - which is true, but a little short for founding a political project.

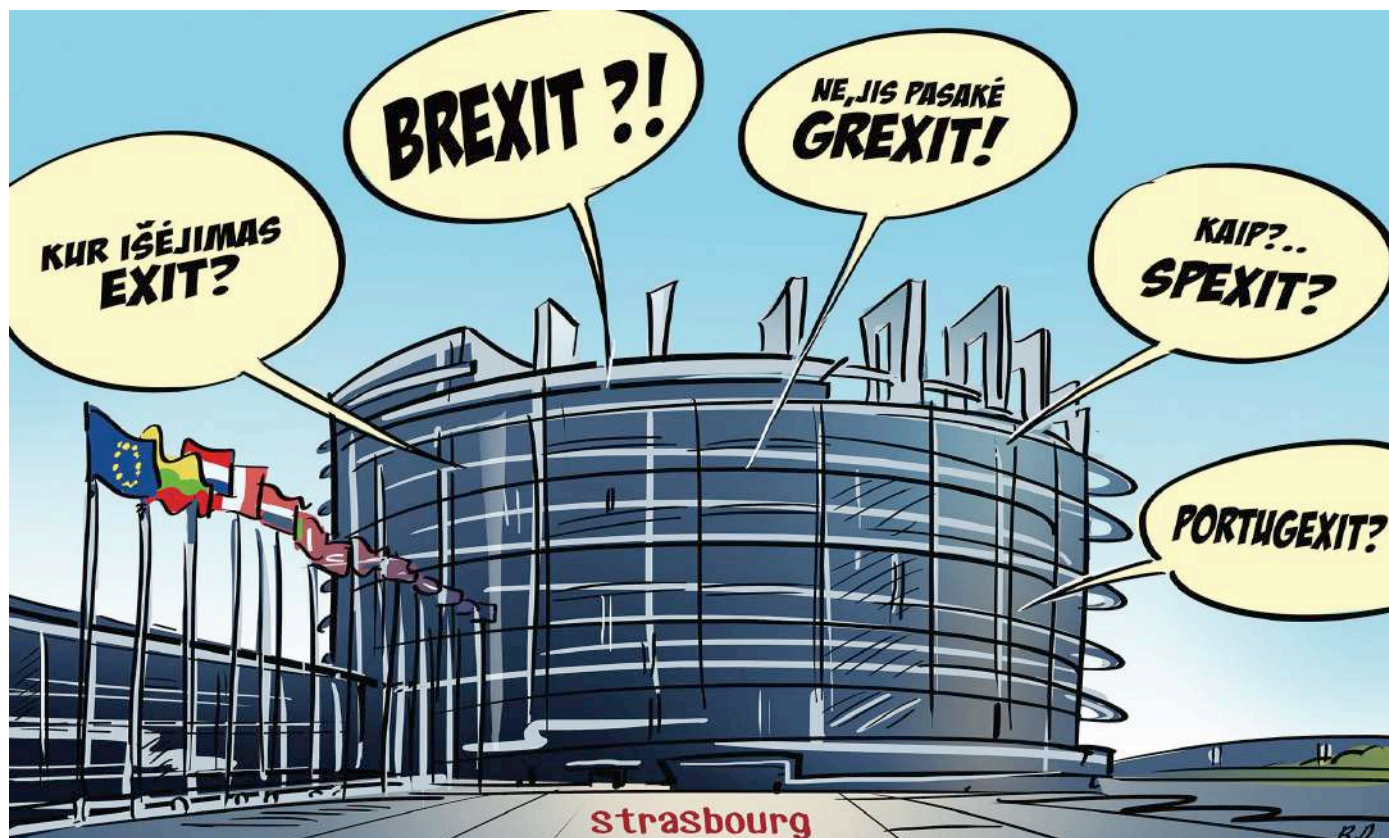
The West is no longer

In the mid-2000s, analysts were concerned about the transatlantic rift. This geomorphological fault at the bottom of the ocean symbolised two destinies drifting apart. The rift has since widened and the West appears to be a remnant: this optical phenomenon that continues to mark the eyes while the lightning flash that caused it has disappeared. The West is a remanence, a memory in the minds of many leaders who cannot separate themselves from it, but also in the eyes of others. Deep down, the West lingers more surely in the eyes of its adversaries (Chinese, Russians, Muslims, Africans) who see it weakened and take pride in standing up against it, while they are only facing a ghost.

The West is no more. The observation is simple, even if it still shocks. Yet it is the primary geopolitical reality of our contemporary world. Very few want to see it, and yet the Brexit and Trump have only accelerated an elder trend, characteristic of our 21st century.

The West is no longer, if not still, in dreams and looks, in memories and words. It is no longer a geopolitical reality. It is no longer that formidable world order-maker that made it possible to discuss in a bipolar or multipolar approach.

The West is no more. We have to take it as a challenge to imagine other ways to defend our interests. The West is no more. ■



Exclusive VIP Interview with General Anton Rog,

General Director of the National Cyberint Center
within the Romanian Intelligence services (SRI),
Romania



Author: Laurent Chrzanovski



BIO

Brigadier General Anton Rog is General Director of the National CYBERINT Centre of the Romanian Intelligence Service (SRI). The CYBERINT Centre is the responsible institution for a 24/7 proactive detecting, analyze and countering malware against systems and networks critical for Romania's national security. Within the SRI, Anton Rog previously held several technical development positions including software and systems design. He also worked as a deputy director inside the Central IT&C Department of the SRI. He is active with the academic community as Associate Professor at DRESMARA (Regional Department of Studies For the Management of Defense Resources) in Brasov. Anton Rog graduated from the University of Bucharest in 1998 with a B.S. in computer science and has achieved in 2011 at DRESMARA a postgraduate diploma in "Program and Project Management." He received the the "Order Manhood and Faith » award (Knight) in 2014 and the "Order of Military Virtue" (Knight) in 2005, by two different Presidents of Romania.

- **About you.** After years of dedication to projecting, developing, ensuring the good functionality of IT&C systems – you reached the position of Deputy Head of the Central IT&C department of the SRI – you passed "to the other side of the line", i.e. to defend and protect IT&C systems. What motivated you to take the decision to make this "switch", quite rare within IT specialists?

It is true that I worked in Romanian Intelligence Service (SRI) for over 20 years until the beginning of 2017 when I worked in an area with several and diverse



technical initiatives. I did not choose to "change sides" in the vast digital area, but the SRI management considered at that time, I was a good candidate for taking over the management of the National CYBERINT Center, the position being available to fill following the retirement of my predecessor. Although I felt that my profile, based on development and creativity is not compatible with the specific work needed within cybersecurity, in reality it turned out that I quickly succeeded in assimilating and integrating with the team. Therefore, I can say I enjoyed a "wildcard" from the SRI, which I tried to valorise giving my best.

Focus - Cybersecurity Trends

Pay-per-service. Contrary to most of the EU states, your services defend the whole country as a duty without any compensation for your job. To be more precise, if the Romanian Central State still has few e-services, municipalities like Sibiu provide to citizens total access to many delicate documents (taxation, cadaster, familiar situation, etc.) and propose online payment for taxes, services, fines etc. In France, such a country could opt between paying the ANSSI (National Agency for the Security of Information Systems) or a private company for its security. In Romania, we already find the same situation for the transportation of important artifacts within different museums: to pay the escort of the transportation to the Jandarmeria, to choose one of the state-agreed private security companies. **What do you think about this situation and its applicability in Romania, with its pluses and minuses?**



Indeed, in Romania not all life events enjoy a good online implementation - birth, marriage, etc. - this implementation being an ongoing process, but the payment of taxes is done online in several cities in Romania, not only in Sibiu, this group including obviously the capital, Bucharest. Regarding the comparison with the French model, I consider that each EU Member State defines its own legislation. In Romania, there is



a single point for payment of taxes, www.ghiseul.ro. The site is managed by the Romanian Agency for Digital Agenda and supported by the Electronic Payments Association of Romania. The most important aspect in this case is that eventual fees and commission are not charged to the taxpayers opting for the site www.ghiseul.ro. As a consequence, this new service gathers about half a million active users who can pay their taxes with no commission fees in real time.

Real attributions vs. political attributions: in recent congresses, **you have shown successful and proof-solid attributions of attacks**, on the contrary of all the mostly political attributions we can read on mainstream media worldwide. **Do you think that serious EU media will once be mature enough to diffuse only examples like yours** or will they continue to be neglected under the tons of "immediate attributions" providing excellent "breaking news"? **What could be done to encourage the media visibility of real cases with months of work behind?**

Both attribution types are equally important: the technical as well as the political one, the second being built on the first. The National CYBERINT Center



is the main actor in the realisation of technical attributions concerning cyber attacks supported by state actors. In our country, a special mechanism has been created, under the signature of the President of Romania, to allow us to take part in international initiatives of the "blame and shame" type, which do have a major media impact. As an example, in 2018, I was part of such an international endeavor when facing the wave of attacks of the APT28 campaign, together with the initiator states - the UK and the US followed by other member states of the European Union. In my opinion, it is important to ensure a media coverage encompassing political attributions based on technical expertise because only in this case, can a huge impact be expected. Once these cyber attacks are discovered and attributed to the author by most State victims, a joint and collaborative effort will certainly become the object of a substantial international media coverage.

Until five years ago, most of EU State agencies like yours were regularly speaking of the successful use of "honeypots". **This term has now fallen into oblivion.** Is it because it is a general basic practice to try to distract at least ad

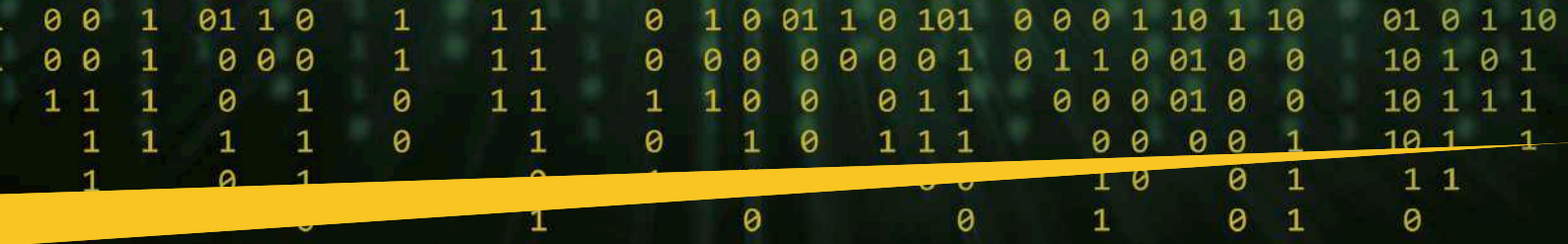
minimam the "bad guys" attention or, on the contrary, because technologies allow attackers to recognise them too easily?

Within the evolution of the cybersecurity phenomena, "honeypots" played and still play their role, but cannot be considered solutions fitting every type of cyber attacks. When discussing state attacks, the malware used is extremely complex and able in many cases to detect such "honeypots". An area in which this solution produces results is the classic cybercrime aimed at obtaining financial benefits by cyber-fraud means.

Honeypots



- Honeypots are filled with fabricated information
- Any accesses to a honeypot trigger monitors and event loggers
- An attack against a honeypot is made to seem successful



Retaliation and proactivity: last year, Swiss citizens voted massively in favour of letting the cantonal polices and your homologue, the FedPol, to create, under a prosecutor's control, fake business profiles on social media and any other useful tools to watch and intervene at the early stages of fraud, economic espionage or sabotage operations. For years, your colleagues in Netherlands and India have the legal right to retaliate in case of attacks. Major powers do it systematically, through their agencies or via privateers. What do you think about this situation? **Should it be an asset for a more cyber-secure Romania to have those rights or would it just increase the amount of men and techniques needed to perform those tasks without a justified result?**

I believe that such instruments can support proactively and very efficiently threat prevention in cyberspace and can be of help in the investigation of some incidents that have already occurred. Unfortunately, in Romania, we do not have a law to regulate cyber security and defense, which could allow players to use such highly useful tools. However, international law, applied also in Romania, allows the use of progressive retaliatory measures in case of cyber attacks. In this frame, proving the link between a cybernetic actor and a state actor holds a special importance because only the achievement of these conditions can allow the provisions of international law to be applied.

In a public-private collaboration perspective, which are your projects and wishes for the years to come, for a more secure Romania. What has been recently achieved and what remains to be done?

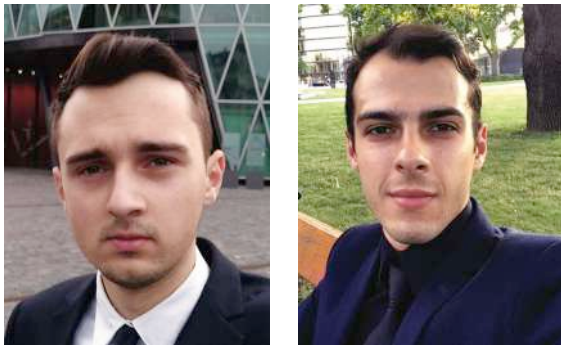
Among the main perspectives that the National CYBERINT Center plans to carry out as public-private partnership, I would like to mention the strengthening of university programs in the 21 universities that agreed to start Postgraduate in-depth study programs on cyber security (of short duration or even a Masters courses including the commitment of our pilot project devoted to introducing concepts of



cybersecurity and cyber hygiene in the national high school curriculum in the Colleges with IT specialisations. Also, another goal is to increase the quality of national exercises by providing a constant number of players and observers – an example being the national cybersecurity exercise, CyDEX – but also to consolidate national conferences on cyber security, as for instance the international conference “Strategic Partnership Romania-US cyber security” and the “cybersecurity dialogues -Romania” congress organised in Sibiu. On the legislative level, it is extremely important to implement at a more accelerated pace the provisions of NIS Directive, which will increase the safety of IT services and essential services operators; it is also vital to create a solid market for cybersecurity in Romania. Last but not least, at an institutional level, I think we should create a hub for the exchange of information between the main actors responsible for cybersecurity within the diverse Romanian public institutions, which can be built following and adapting the models established in other countries, such as the USA, UK or Israel. ■



Facial recognition and defence industry



Authors: Daniel Leu & Ștefan Dorneanu

"Terrorism has become the systematic weapon of a war that knows no borders or seldom has a face."

Jacques Chirac

In the age of globalisation, terrorism is becoming an increasingly widespread threat to state security. This type of threat often comes without a uniform, operating through non-state agents whose effectiveness is inversely proportional to the degree of readiness of states.

The context in which a state must protect itself today has changed greatly in the last 30 years. The battles are now mainly fought behind the curtain on several levels simultaneously with a lot of attention falling on the war on terror. A state, as much as it needs good cooperation with its strategic allies, also needs to keep a strong focus on developing its own defensive capabilities.

BIO

Daniel Leu is a cyber security analyst with more than 4 years of experience in the regulatory technology and anti fraud field. He is part of the team that won the "Threat Security" category in the Patriotfest 2019 defense innovation competition by focusing on the use of facial recognition technology to further security capabilities.

In the light of the increasing frequency of terrorist attacks throughout Europe, it is worth noting the increase in the government's efforts to identify and implement unique methods of monitoring and prevention through concepts such as facial detection and recognition.



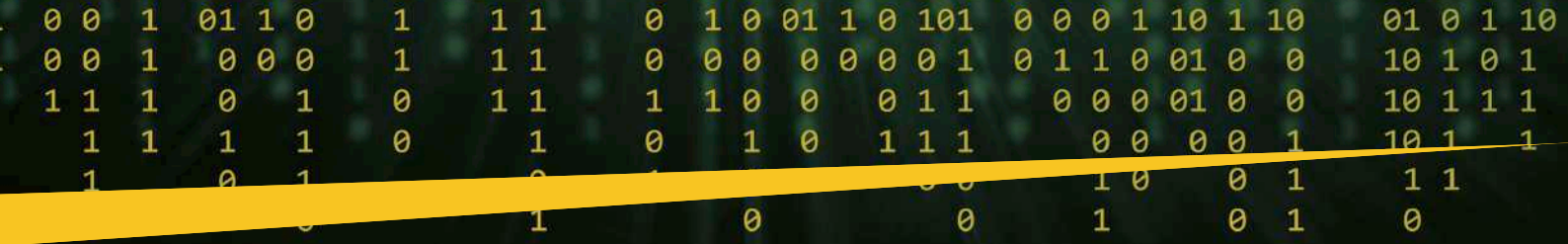
The technological development of the last 20 years allows us today to implement solutions that seemed impossible at the beginning of the millennium. Due to the increase in the processing power available, we can now work more efficiently with unstructured data thus making methodologies such as object detection and pattern recognition more accessible.

BIO

Ștefan Dorneanu is working as a forensic intelligence analyst with a background in regulatory technology and computer science. Passionate about technology and driven by the desire to always improve his skills, in 2019 was part of the team that won the "Threat Security" category in the Patriotfest competition with a project using facial recognition technology applied in the security field.

The use of this type of technology increases the operational capacity of law enforcement agencies by delegating tasks that would normally require the allocation of a large number of human resources and would be vulnerable to human error, to systems specialised in carrying out those activities with a certain degree of independence, thus providing the opportunity to allocate human resources as efficiently as possible.

Pattern recognition in unstructured data can also be used to identify the spread of "fake news" in the online environment. This term has been widely



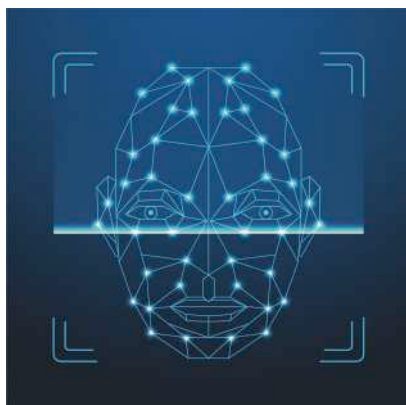
used in recent years and has come to the attention of defence agencies because of the ease by which topics that influence public opinion can be spun in a perspective that serves the interests of threat actors seeking destabilisation. This modus operandi was mass-mediated during the 2016 presidential election and led to measures to reduce its spread around the globe.

More about facial recognition

By facial recognition we mean the transposition of an individual's face that exists in an image or a video frame into an encoding that can be later understood and classified by a pre-configured device. We can describe this process in 3 steps:

1. Detection step: the device detects the faces in the frame.
2. Calculation step: An encoding is calculated for each face in the frame based on a specific algorithm.
3. Control step: Each encoding obtained in step 2 is compared to a Watchlist style database that contains pre-calculated encodings of known threat actors.
4. Feedback step: Following the control process, the system will display whether the person in the analysis is known or not.

Because these operations are performed in real time, a control system based on this methodology can drastically increase the detection rate of suspects at checkpoints, leading to a higher degree of threat prevention.



SCAR portable facial recognition system

Using the concepts presented above, I developed together with my colleague Ștefan Dorneanu for the 2019 edition of the Patriotfest contest, the Security Control and Active Response - SCAR device.

The aim of the project was to develop a portable device capable of analysing face telemetry and to provide, in real time, feedback on the degree of risk of people exposed to the analysis.

The device was designed to be attached to a pair of glasses, consisting of a display that transmits feedback to the wearer and a camera.

Given the speed and accuracy of the data flow transmitted by the device to the carrier, we believe that the use of such a device at security checkpoints can drastically increase the operational efficiency.

To exemplify the operational flow of the product we will refer to the following scenario:

We visualise the scenario of a rock music concert with 3 access points where the crowd can pass the routine security check. This routine control itself is often ineffective due to the large number of people that agents have to process. We imagine the unfavorable case in which a threat actor wants to launch an attack on the location.

Our prevention strategy proposes the equipping of a number of agents, strategically placed at each control point, with the SCAR system. Through the system, agents will monitor the flow of people in real time, applying facial recognition algorithms to all people who fall within the range of the device. In the event of a positive response according to the list of persons provided by law enforcement, the control teams at the rock concert will be able to take the necessary preventive measures to ensure the safety of the event.

We consider that by implementing a preventive-defensive approach, we can considerably reduce the risk of a terrorist attack.

Defense industry and Patriotfest initiative

The last decades have shown an increase in the variety of threats and this tells us that we must keep active the mission of constantly innovating the way a state protects its people.

This direction is also followed by the Patriotfest contest which started in 2017 in order to encourage creativity and new ideas in the field of security. The defence structures in Romania collaborated in order to organise the contest and in 2020, in its 4th edition, the stage of the contest has presented projects belonging to the fields of quantum physics, artificial intelligence or neural mapping.

For us, Patriotfest meant the possibility of bringing together our knowledge in the technical field with the need for innovation in the field of security. The experience gained by participating in this competition has brought us renewed insight into the latest technology trends and conviction that progress can only be achieved through innovation.

Many questions whose answers we seek far abroad can be answered right here through our national innovational capabilities. We had the pleasure of meeting many people with the desire to make a difference, open to new ideas and innovation, but especially proud to have the opportunity to do so in their country. ■





VIP interview with Rick McElroy, Head of Cyber Strategy, Carbon Black



Author: Elena Mena Agresti

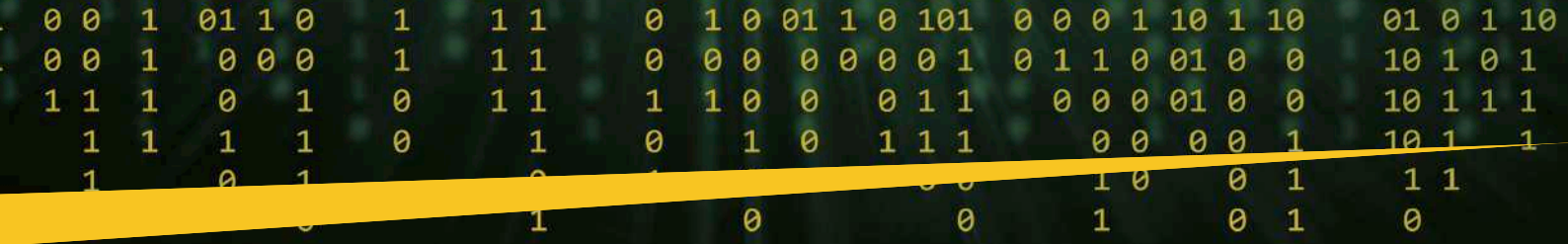
What scenario should cyber security experts prepare for?

Certainly more automation, artificial intelligence and tools will be needed to provide complete visibility of complex and evolving networks. Resource efficiency will become the watchword as companies aim to maximise

BIO

Rick McElroy, Head of Security Strategy for Carbon Black, has more than 15 years of information security experience in educating and supporting organisations in reducing their risk exposure and addressing difficult security challenges. He has held security positions at the U.S. Department of Defense and in various industries including retail, insurance, entertainment, cloud computing and higher education. McElroy's experience ranges from performing penetration tests to defining and conducting security programs. It is certified (CISSP), CISM, CRISC. As a U.S. Marine, McElroy's work included physical security and counter-terrorism services. A fierce defender of privacy and security, requiring education and innovation to be the keys to improving the security landscape, McElroy is president of the Securing Our eCity Foundation's annual Securing Our eCity Foundation CyberFest program, a San Diego event dedicated to public and private sector security education and IT professionals and corporate executives on security realities.





teams' ability to detect and mitigate threats and invest intelligently in the tools that enable their teams to build on growing trust and manage proactive cyber defense.

According to the results of our second regional report on cyber threats, companies are adapting to the 'new normality' of continuous and sophisticated cyber attacks. Increased awareness of external threats and compliance risks has also prompted companies to become more proactive in managing cyber risks as they see the financial and reputational impacts of violations.

As the cyber-piracy defense industry continues to mature, companies are becoming more aware of the tools at their disposal and the tactics they can use to fight cyber attacks. We believe that this growing confidence is indicative of a shift in power in favor of *cyber defenders*, who are taking a more proactive approach to *Threat Hunting* and threat neutralisation than in the past.

The area has increased exponentially but it is good to distinguish between producers and consumers.

If it is true that producers are increasingly prepared and ready, consumers are not, and for this very reason it is necessary to start thinking about a *shared security* policy. A security that must necessarily evaluate all areas, especially for realities that have difficulty in understanding computer security.

It emerges, in fact, a generation gap in which today the older generations find themselves outside the logic of computer security and computer *best practices* to defend themselves.

I believe that in only 40 years, we will arrive at a fully mature generation that can best approach this *digital transformation*.

Can new technologies support the activities of security teams?

The blockchain is certainly a new technology that can guarantee enormous advantages. One of these is the guarantee of individual node

certificates. However, it is not, in my view, applicable to all sectors. Some sectors must continue to work in the direction with which they are working by implementing security technologies such as IDS, IPS, SIEM etc. One example of a successful application that needs to be brought to light is certainly the application of the blockchain to SWIFT systems. Although the perimeter of such a system is complex, the blockchain could play an important role in ensuring its security.

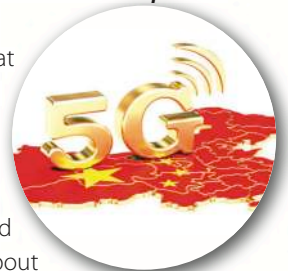
Artificial Intelligence and Machine Learning are revolutionary tools for cyber security as 5G represents the future of communications.

Our research reveals considerable security profession concerns about digital transformation projects and the implementation of 5G will affect their risk position.

There's a lot of talk about 5G and relationships with China. What do you think?

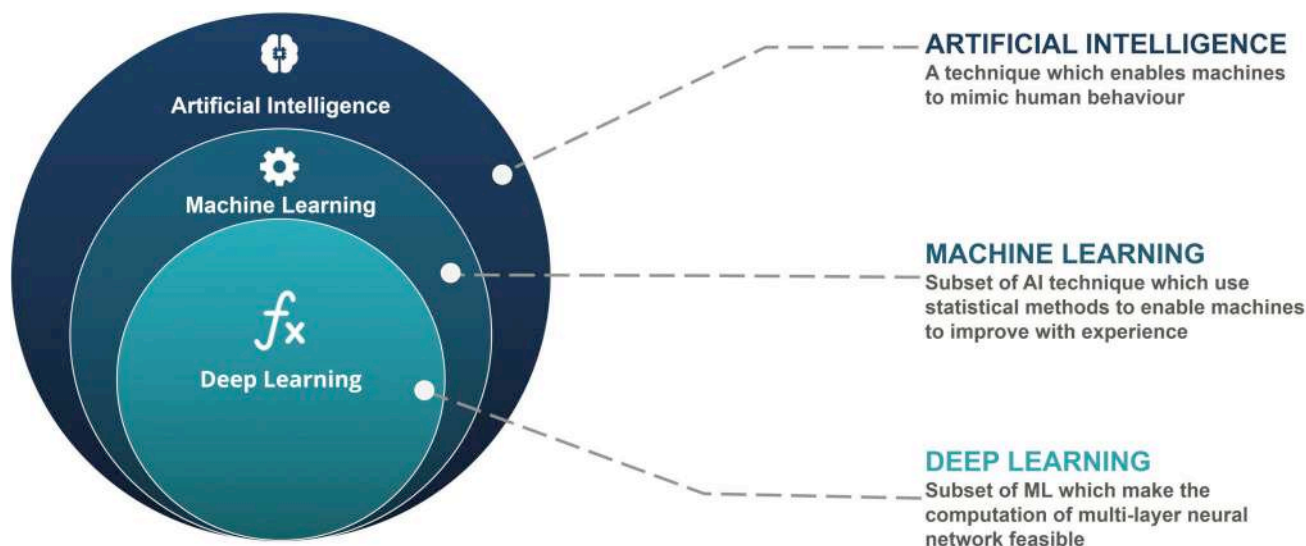
It is pointed out by many that 5G technologies have much lower costs and may pose a threat to Western countries. However, if one takes as a fact the fear of being spied on and not being able to do anything about

it given the origin of the technologies implemented in the infrastructure, it is necessary to act in another way. It is of fundamental importance to have a closer monitoring and defence which takes into account that there is a problem upstream, namely the technologies





Focus - Cybersecurity Trends



provided. Two-factor authentication or other methods of authentication are certainly one of the elements that can help us. I would like to add that 5G, as well as representing the future of communications, plays a very important and difficult to predict geopolitical role. Much depends on the will of individual states and the political decisions they take in their own systems.

He called Artificial Intelligence and Machine Learning revolutionary tools. But what is man's role?

Artificial Intelligence and Machine Learning obviously offer a lot of room for improvement in data analysis but we must not forget that every day the biggest computer security companies are confronted with other equally "human" subjects.

It is precisely the human aspect that is fundamental. Studying the trends, behaviours and dynamics that man puts in place to overcome the barriers of protection provided is the key to success. Artificial Intelligence and Machine Learning can help us in this sense, especially for all those "abnormal" phenomena that you probably do not think about but that exist. I repeat, the man and the attackers will always be in the center. Look at an AI machine. It's great to be able to sleep and not drive but it's good to think that there is a man behind it!



A topic of strong discussion is the relationship between endpoints and cyber insurance.

A car must be designed and built to be safe because it is tempting that the consumer may make mistakes. That is why companies must always be ready to face any kind of threat.

In the event of a successful cyber attack, however, I find it particularly complex to demonstrate the ineffectiveness of an applied security solution. This is because there are

always new forms of attack and it is difficult to identify the type of attack and damage, legally speaking. To this we must add that insurance and cyber insurance have not defined a standard or a framework of pre-established compensation schemes or typified cases such as car accidents. We know that, given an event, a collision for example, the insurance will cover the damage if the conditions laid down in the contract are met. Contractualise all events, and therefore the damage that can result from a cyberattack is complex.

What if the attacker is a government actor? The latest cyber-insurances have a leniency clause for government attacks. How could we ever prove that the attack was launched by one government rather than another?

Digital privacy and ethics are constantly evolving issues. Much information in the past was considered more sensitive than it is today. Do you think it will still be relevant in the future or not?

It is essential to have a constructive approach to privacy and learn to behave according to privacy. When I told my son that the government was probably tapping his phone, my son didn't even blink, as if he didn't care. When I asked him to show me his private messages, his photos, his Instagram profile, then he got excited and said no.



This is a summary of how we live with privacy today. You have to be aware that it is a very important element regardless of who the interlocutor is. Cambridge Analytics was a classic example. It had impacted individuals, companies and elections of a nation.

On the technological side, it is very important to be able to approach this theme by design and by default. The systems also face new regulations, international and European to guarantee the personal data – a key fundamental prospect.

Talking about ethics nowadays is important and fundamental. I believe that we will see an evolution of the humanistic figures in technology and information technology. While the computer scientist has a direct approach to technology, to the problem, to the solution of the problem, the humanist evaluates other factors, even moral ones, which necessarily have to be taken into consideration. It will be complex to manage the scenario that awaits us, for example giving priority to the choices that a machine based on Artificial Intelligence will have to make and for this reason it needs the support of the thinking man. ■

Technology and law must ally for good digital governance

VIP interview with Antonello Soro, President of the Special Warrant Authority for Personal Data Protection (Italy)



Author: Massimiliano Cannata

“In 2019, cybercrime grew by 17% worldwide compared to 2018: a year already defined, as the worst ever for the cybersecurity domain. Experts have drawn worrying forecasts on possible risks and trends for 2020, outlining a horizon of increasingly sophisticated attacks”.

BIO

President of the Warrant Authority since 19th June 2012, Antonello Soro was Vice President of the European Privacy Warrants (WP art. 29) from 26th November 2014 to 12th December 2016. He was mayor of Nuoro and regional counsellor of Sardinia and in 1994 he was elected deputy. From 1998 to 2001 he was President of the Parliamentary Group “Popolari e Democratici - L’Ulivo”, from 2007 to 2009 President of the Group of the Democratic Party of the Chamber. He was a member of various parliamentary bodies from 1994 to 2012, when he resigned for incompatibility as a member of parliament following his appointment to the Warrant Authority. He has presented, as first signatory, numerous legislative proposals, including the one on deontological rules relating to the processing of personal data, even if acquired through interception, in the context of journalistic activity and the one on the rules of discipline governing the legislative process.

President Soro, this is the message that has come from the 14th European Data Protection Day. What scenarios should we prepare for?

The security of the cyber dimension is constantly exposed to increasingly “hybrid” threats, generating a sort of permanent cyber guerrilla. In the last few months, the Post & Communications Police has brought to light what would appear to be the most serious attack on institutional databases realised so far, with *phishing* techniques allowing access to information systems among the most relevant for the State and the nation, from which data could be extracted for being sold to investigative entities or debt collection agencies. It is an emblematic fact which says a lot about the evolutionary trends of the *cybercrime* phenomenon which requires, in order to be contained, competence, timeliness and an immediate capacity of response.

Much is about the relationship between Cybersecurity and geopolitics. How do you see this delicate pair?

Cyber attacks have also become means of war engineering. Just think of the recent events in the Middle East, a foretaste of what will be the paradigm of military confrontation in the coming years: armed drones and cyber attacks are used as real weapons, but endowed with an extraordinarily greater power. Cybernetics is the dimension where the dynamics of conflicts, evident or latent, between States and between subjects, operated through data and information systems, are increasingly moving. On the other hand, we are talking about the only dimension of security and defence which basically lacks an adequate framework of international law. An effective

Focus - Cybersecurity Trends



strategy of prevention of cybernetic risks presupposes, in fact, the awareness of the factors on which action and reaction are based, respectively, technology and law.

The law must be at the service of humans, but is too often forgotten...

The law is the only resource capable of putting technology at the service of humans, of freedom, of security. On the other hand, an alliance between technology and law would be desirable: it could represent the apex of a democratic and far-sighted response to the new threats posed by digital technology, threats fortunately counterbalanced by the extraordinary potential of these two means. This presupposes, first of all, the maximum balance between the disciplines responsible for governing the relationship between freedom and the dark side of technology, i.e. data protection and cybersecurity.

Is it correct to define cybersecurity as the other side of Privacy, as you recently mentioned in a public debate?

Between data protection and cybersecurity protection there is an undoubtedly complex relationship, which, full of antagonisms as well as unexpected synergies, says



a lot about a society in which the irrepressible exhibition of one's private life reflects a deep crisis of trust and social cohesion. Those elements in the past, led to the fundamentals of a very different perception of security and of freedom. In this regard, it must be remembered that cybersecurity protection has legitimised incisive limitations of privacy, in the name of the fight against threats which are immanent as they are hard to define, hence countered with the use of often massive investigative tools. *Social and signal intelligence, strategic surveillance, data mining*: these are only some of the forms that prevention actions can assume, extending its range of intervention each second, as our hyper-connected societies feeds the net with continuous information flows.

Cybersecurity as a human right



Many debates and essays have been dedicated to the relationship between democracy and data power. From the point of view of democratic balances, how should the relationship between security and privacy protection be balanced?

The power of technology and the characteristics of the increasingly evolving cyber threat imply an increase of the spectrum of investigative actions. This, as you point out rightly in your question, can only have effects in terms of democratic freedoms and balances. We have to think that, in our

country, the operators keep, every day, about 5 billion records of telephone and web traffic for law enforcement purposes. Within such a gigantic mass of data, it is certainly not easy to find the useful few. To put it another way: if we spread the haystack out too much, can it still be reasonable to think that we can find the needle?

The collaboration of the Warrant Authority with the DIS (Information System for the Security of the Italian Republic) is certainly an important point on the data protection front. Can you explain in what sense?

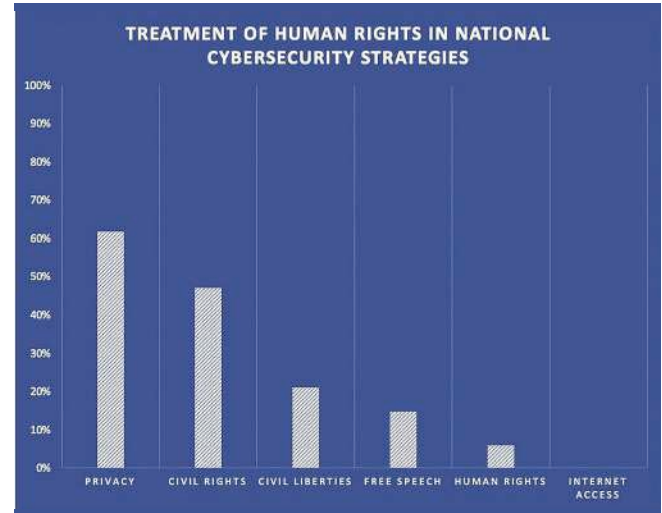
The protocol of intent, signed with the DIS in 2013, was dictated by the precise need to define a parallelism between an extension of the powers of the different State Bodies and a corresponding upgrade of the Warrant Authority's functions. As a demonstration of the delicacy of the problem, even the European legislator took action, establishing a significant symmetry between data protection and *cybersecurity*, which is evident in the definition of some institutions that have to deal with the GDPR regulation, the NIS Directive and national regulations on *cybersecurity*.

From one of your speeches, it emerged clearly how Cybersecurity must be considered as a human right in the network society, the latter being a space which recalls the inviolable rights of expression, movement, participation, relationship. Is this a correct interpretation?

It is correct when one considers that in an economy and a society based on data, protecting data means protecting individuals and the community at the same time. In the context of a digital society in which each object of daily use can represent an entry point for potential cyber attacks and in which, therefore, the sources of risk daily multiply out of any proportion, it is essential to make the protection of data, systems and infrastructures a top-priority objective of public policies, because protection of the individuals as well as national security depends on it.

The growing complexity of systems generates, in fact, vulnerabilities exploited for cyberattacks that can paralyse essential public service networks, institutional communication channels of primary importance, with a very strong impact on public life. In the *"surveillance capitalism"*, in particular, the risks are even higher if we consider that threats, as in the case of terrorism, are no longer predictable, having a "shadow" and constantly evolving character. The defence becomes more and more asymmetrical also because the chains, more and more complex, on which the information

flows are articulated, present a growing multiplicity of weaknesses.



Treatment of Human Rights in national Cybersecurity Strategies, © Scott Shackelford, Should Cybersecurity Be a Human Right? Columbia Law School

In this perspective, the cyberspace becomes a common good. What does this mean in concrete terms?

The synergies characterising the relationship between data protection and cybersecurity, as much as I have tried to explain in this conversation, are not only normative, but they are at a deeper and more structural level, because they both tend to protect digital reality, data and systems being considered not as isolated items, but within their mutual inferences. For this reason, cybersecurity has been defined as a common good, and protection it offers benefits to everyone, precisely because it concerns a reality, the digital one, based on the interdependence of data, systems and subjects.

The importance of democratically sustainable innovation

Can the geopolitical intelligence of data and the rush towards technological hegemony, which many states have put in place, determine a change in the political and economic equilibrium at world level?

The question is complex and involves several levels of analysis. Remaining with the theme of this interview, it is necessary to underline how strict is the net security dependency of those who manage the various hubs and "channels". This brings us, in fact, to understand the theme of *"digital sovereignty"*, to be declined not in a nationalistic-autarchic key, but rather in the perspective of a *governance of the digital dimension*, which is, today, the expression of a legal and political identity. To

Focus - Cybersecurity Trends

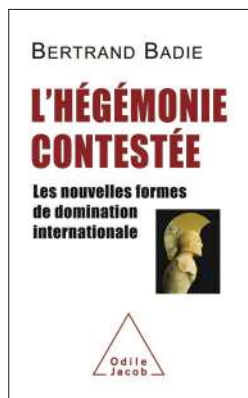
synthesise: since the threats are global, I believe that the objective must be the overall assumption of public responsibility with respect to an interest, such as cybersecurity, on which the independence of a country depends in the first place, and which must increasingly be declined in a supranational way, shifting its horizon, just as it has been made for data protection, from a national to a European perspective, at least.



The French political academic Bertrand Badie in a famous essay talks about the end of the territories and the decline of the famous Leviathan by Hobbes. In a somehow unpredictable way, don't you think that the danger of a "digital neo-imperialism" based on the control of data and information, allied with a different conception of sovereignty, you mentioned earlier, is making its way?



In an area as "non-physic" as the net, sovereignty must be declined in new forms, less linked to the traditional criterion of territoriality and more attentive, instead, to the capacity of States to really protect the rights and a same democratic form, to face all new illiberal pressures. In this sense, the manipulation of personal data, even by foreign States, imply significant risks on national sovereignty and on the essential political choices which determine the democratic exercise.



The *Cambridge Analytica* affair, to cite a case which is certainly striking, has shown how the so-called "micro-targeting" based on the profiling of citizens and on the consequent electoral propaganda, creating "human-targets" according to a specific type of voter drawn up by an algorithm, can heavily condition the process of the formation of a consensus, an action manageable by foreign powers to obtain the electoral result they desired.

The stronger and stronger competition for technological hegemony hides, today, a very close connection with geopolitical dynamics, which can

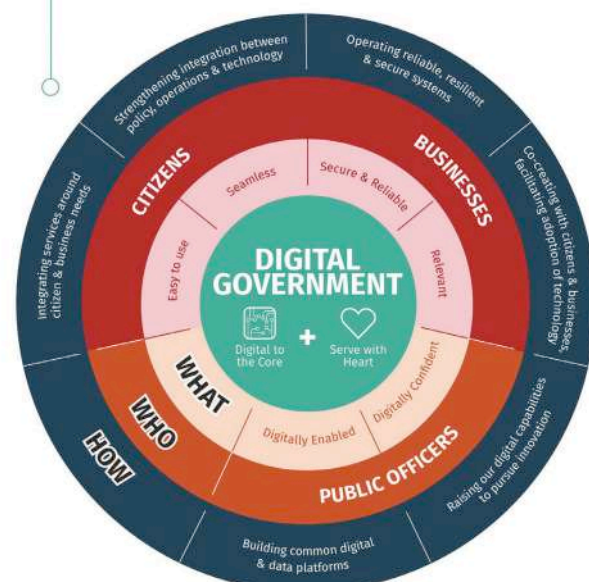
imply, in a decisive way, national security structures. The risk of a "digital neo-imperialism" to which you referred has been highlighted by the concern expressed by the Parliamentary Committee for the Security of the Republic, for whom this case appears to be an evident weakness within a Nation's legitimate needs of cybersecurity, which is increasingly bypassed by the overwhelming force of commercial interests of some actors that act as dominators, and succeed effectively to limit the freedom of the internet users and even, sometimes, the full sovereign democratic exercise of a State.

Where is Europe, in this complex game of global digital governance?

Europe has made data protection a factor of identity, rediscovering there, at a time when isolationist and division pressures are re-emerging, the very federal aspiration, so hampered in other fields, that the GDPR marked a real transatlantic gap in the management of the relationship between technology and rights, economy and freedom. This unifying vocation, which is often, unfortunately, hidden in other fields, has made it possible to overcome the peculiarities that often deprive the law of its necessary long term vision, and has allowed this discipline to become the most advanced front of a digital governance, able to move towards a real constitution dedicated to the algorithms, a topic many other regulators (including non-European ones) have started to work on.

Looking ahead, I think that it will be more necessary than ever to update the political agenda, putting at its very center ideas and projects on how to govern the digital society, in order to guarantee rights and freedoms of citizens in this new dimension of life. In this field, at this moment, data protection is to be considered an indispensable compass. ■

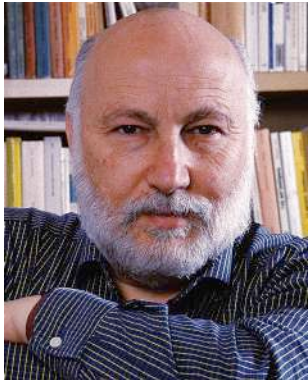
DIGITAL GOVERNMENT BLUEPRINT



Digital Governance: The concept developed by Singapore

Where to start again

VIP interview with Domenico De Masi.



Author: Massimiliano Cannata

The “prophecy” of Bill Gates

In 2005, Bill Gates prophesied: not a bomb will kill us, but a virus. COVID-19 came like a raging wind, wiping out everything. A crash test for Western civilization. How did the country react in its darkest hours?

It has to be said that rational and positive reactions have fortunately prevailed over irrational and negative ones; in reality it is as if we were taking part in a great seminar that confronts us with an unprecedented case and forces us to reason and meditate.

What are we learning from this moment of forced “collective training”?

Many, many things. First of all, that the world is globalised and it takes nothing for a virus propagated by a Chinese bat to reach our homes. That it is not possible to create borders, that every rigid closure is only artificial and psychotic, and that as a consequence sovereignists are outdated, they are the fruit of old thought legacies belonging to the nineteenth century, a century dominated by nation-states. We are, moreover, learning that skills are indispensable, as one cannot, without preparation, move in the complexity of the present. The exact sciences will not be as infallible as great thinkers had already told us, from Popper onwards, but they are exact enough to guide our behaviours.

The time for a mass mental and psychological reset could not have been more abrupt. What can we expect in the coming months?

We changed our lives by decrees because we accepted the assumptions which led to the strategy of rigour. Initially, some believed themselves to be immune, then the gravity of the situation “convinced” even those “super men” as well as the more sceptics. There is a profound mutation of many attitudes which are part of our DNA. For example, we are finally realising that decisions are a complex fact, and that when faced with new facts one can be wrong. The result is that a part of the country is learning to be tolerant towards mistakes, which are inevitable when you have the responsibility to decide while being in conditions of total uncertainty, such as the pandemic we are experiencing in these months. The signs of such a profound upheaval are bound to last.

Our relationship with technological instruments is also undergoing significant changes, with what consequences?

The forced solitude led us to reflect on the concept of living together, and what sociologists call *primary groups* became important: family, close friends, neighbours. Until yesterday, we were accustomed to being familiar only with *secondary groups*: colleagues, customers, suppliers, acquaintances

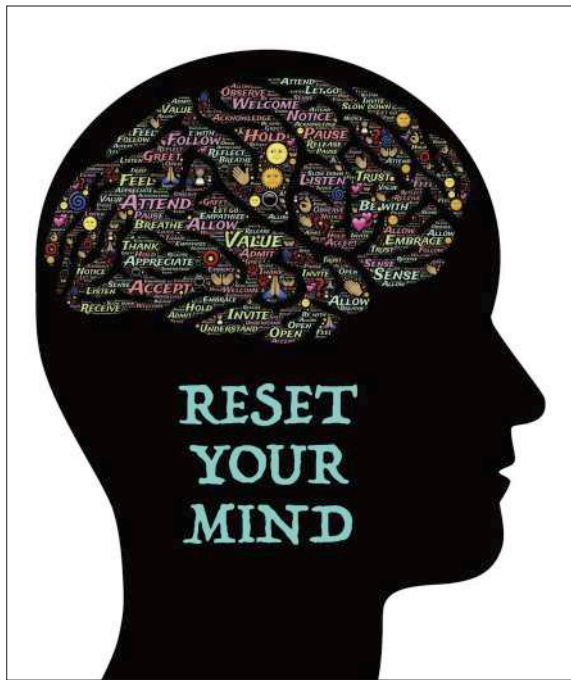
We have learned to inhabit the void

“Never before in human history had we witnessed a choral experiment of this proportion. Almost 70 million Italians made a “break”, finding themselves at war against an invisible enemy. Collective lifestyles, habits and customs, in the short span of a few days, have been modified. Rich and poor, young and old, all sealed at home, in a dimension where space and time have changed their meaning.

As such, speed, cars, the great icons of industrial society are no longer part of us, as if they no longer belong to us, and in the meantime we are learning to inhabit the emptiness of a city and to regain ties with our primary groups : the family, the closest relatives, the neighbors and, finally, we are beginning to listen to elder people again...”

BIO

Domenico De Masi, Professor Emeritus of Sociology of Work at the University “La Sapienza” of Rome, has seen and studied revolutions in every corner of the globe. He sees a different crisis we are facing - the transformations that have come alongside social processes and productive organisations. The key is how to “look beyond” in order to try to understand where we are going.



in the broadest sense, we spent more time with the people to whom we addressed with “Mister” than with the ones we just called “dear”. Now the world seems to be turned upside down, the centrality of the human factor and of conviviality returned, even if they cannot be cultivated through physical encounters. We dealt that through information technology, we learned to discover it, as you mentioned in your question, and its precious usefulness. Apocalyptic believers are always inclined to condemn innovative instruments, but today, after condemning the net, we all became great fans of it. Another important aspect: we are rediscovering the value of authentic communication, which must be as reliable as possible. It is better to stick to what the radio and TV say, without dwelling on the many fake news. Traditional media is having singular revenge on new media, a fact which was unthinkable until recently. But the picture of the upheaval is not yet complete.

What are you referring to?

To the importance of young people in this game: the digital natives have the advantage of being familiar with computer science, they know how to tele-play, tele-study, without too many problems they are continuing to “hang out” with friends and to carry out their activities, to go virtually to school, even if the gates of the institutes are closed. But I would not underestimate the unexpected strength of the elderly, who teach us many things...

Don't you think that this category of people, over the years, has been and continues to be the most penalised and disadvantaged, because they are increasingly isolated and particularly exposed to contagion?

The fact that this category lives in a condition of fragility is undeniable. This is the reason why we must not let the

elderly lack our affection and attention. But it must be said that they are also more independent, and are used to stay at home, playing sedentary games. Thanks to a long life experience, they are, moreover, showing wisdom and balance when facing a challenge. But there is another component we have to get used to: living in the emptiness of cities.

The “emptiness” of historical centres

A shock to be added to other traumas. How long will it take to return to normal?

Nobody’s got the answer in a pocket, not even the experts are unbalancing for a date or a month. One thing is certain: while we are at home we feel protected, we are in the place we have always known, then we put our nose out the door and we have an unprecedented view, we are projected into the unknown, in a context we have never seen, at least in this form. All this involves new psychological reactions that we do not know and that we can only hypothesise for the moment.



In this scenario full with fears and uncertainties, even the dimension of time has totally changed. Nothing looks the same as before. What is the sociologist’s reflection on this?

I agree. We have gone from a frenetic life, played on many fronts: home, work, friends, colleagues, theatre, cinema to a single dimension of life enclosed within the walls of our home, in houses that, no matter how big



they are, seal us up and act as a prison. In a prison, you know, time dilates, the movements that filled our days are no more there to enrich our day. It is like speed, and the cars, the great icons of industrial society, no longer belong to our lives. To be short: I live in the very central *Corso Vittorio Emanuele* in Rome, it is usually impossible to cross the street except on the strips and when traffic lights are green. In the last period I have been able to take some very short walks on the “central white line”, which in normal conditions is as unthinkable as dangerous. But not only the conception of time changes: together with it the perception of space is modified. It seemed to us that it was unlimited, we used to travel everywhere by any means, suffering the scarcity of a time full of commitments, things to do, appointments. In this “fenced-in space”, time is enough and even too much, it is now up to us to know how to fill it with meaning and signification.

Agile work can change the company



Let's try to dwell on the production organisations, which have always been the subject of your studies. What should entrepreneurs and managers learn from this lesson?

Companies are "discovering" the importance of tele-working. I talked about this subject for the first time in a book of 1991 on the basis of studies carried out as early as the mid-eighties of the last century. Well: ten million Italians are working from home, without any harm in the field of productivity. Better late than never, one might say.

Is what is happening to be interpreted as a sort of new deal for the corporate world?

I'd be more cautious. I am convinced that only in a first moment, pressed by the emergency, entrepreneurs will allow more employees work from home, but after the crisis, most of the bosses will try to regain their archaic power, they will come back physically, hindering in fact any practice of distant working.

Can the trade unions play a role in order that we will not go back to "used" habits?

As long as you change your mind. I don't think that the large organisations of our country, which have many employees, are yet ready to adopt flexible and agile working solutions. I'm not very optimistic because I believe that the human heart has stronger persistent inhabits than the brain, and I'm afraid for this reason that the ancient habits will regain their rights, after "the night". Let us remember that behind the traditional vertical organisational schemes, there are as many as two hundred years of industrial society, the experience of this disease, on the other hand, is only a few months old. This imbalance, at least in the short term appears unbridgeable.

Europe's weakness and the "necessary state"

Europe has appeared fragmented and surprised in the face of the emergency. It has closed its borders, while its ruling classes have only stammered answers, weak and often contradictory. Will the old continent emerge weaker or stronger from this experience?

Some European states will understand, others will keep on reactionary positions. This affair has made it clear that we need a stronger State and a stronger Europe. Just as the State must prevail over the regions, Europe must prevail over States in times of emergency. We have mocked the writings of Latouche and those who preached a serene de-growth. Now, it has happened, a Chinese bat has inflicted to us what we could have been planning since a long time.

Certainly a new phase is opening for capitalism, something that had not happened even after 9/11. Does that mean the shock is more serious this time?

9/11 actually changed almost nothing for us. We saw it 6,000 km away from us, the concern was relative. Even during this epidemic, at first, we thought of something far away, aimed to develop into an indefinite "elsewhere". Many of us thought that like an earthquake or a tsunami it would remain a distant event. But the virus moved and so very quickly it reached us...

In your last paper (Lo Stato Necessario) you affirm the necessity of a return of the State, after years of exasperated liberalism. In light of the health emergency, what is the basic message of this research?

Current events rend the message even easier. How would have we coped to this dramatic situation without public health, both thanks to the professional scientific contribution and of the level of security and expertise that experts have passed to the political ruling class in order to prevent non-sense quickly taken decisions?

The present need for a State, though certainly not an intrusive one, is emerging at every stage of the crisis we are experiencing. Let us take the reactions of the regions which thought themselves as being most immune to any economic collapse, because they were richer and more organised. Let me give you a concrete example: between Lombardy and Campania, the gross domestic



product is three to one, reason why Lombardy felt above any risk and any possible economic fluctuation. Thus the richest regions, also by virtue of a constitutional design providing them a broader autonomy, have made their own health care decisions. This model does not work.

However, the health emergency has made it clear that it is much more effective and advantageous to go back to the central State, without any ego and further local wishes of "freedom". In these circumstances, there is a need for a State that decides quickly, coherently and firmly, to protect everyone, from the economically weaker regions, to those territorial realities that are considered stronger and therefore independent or even autonomous. ■

Focus - Cybersecurity Trends

Memory and Identity are strong values that we must cultivate in the digital society: they tell us who we are and where we come from

VIP interview with Pietro Jarre



Author: Massimiliano Cannata



'Sloweb' is a term that evokes slowness. Was Sloweb born to call for a return to reflection in times more devoted to superficiality and instinctive reactions?

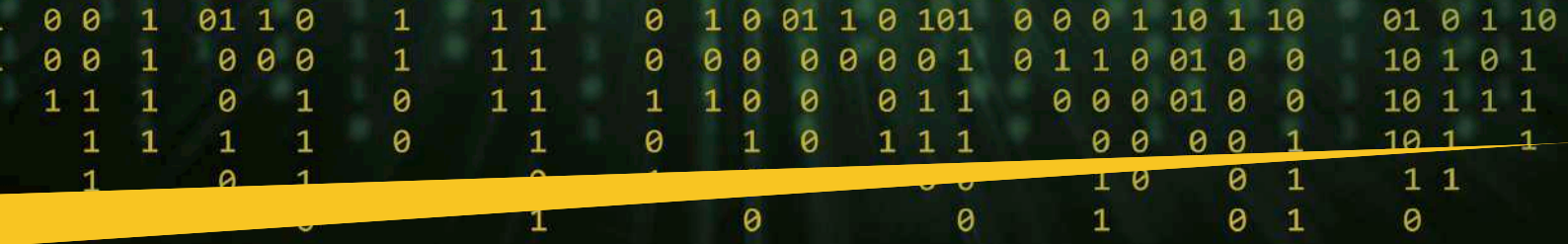
Your reading is correct. Slow allows us the right to think well and in-depth. With Sloweb, says Mario Perini, a

BIO

Pietro Jarre, 63 year-old, is an engineer, founder of Sloweb and creator of eMemory and eLegacy. He promotes the web services of informEtics, digital education events, publications and cultural initiatives on responsible and conscious use of the web. In this interview, Jarre shows the great potential, but also the huge risks associated with the use of the web. Knowledge of history, respect for diversity, awareness are key terms that today's humans must care for and practice, in order not to transform oneself from "Homo Sapiens Sapiens" to "Homo Stupidus Stupidus", to recall the title of a recent book by Vittorino Andreoli.

psychoanalyst, *today's human must regain the right to use a slow and thoughtful mind that deals with fast technology.* We are losing the ability to reflect, and, like slightly foolish fishes, we are distracted by the thousand shiny objects that swirl around us. The very phase of attention - which precedes reflection - is compromised, reduced to a few minutes at best. I realise myself that I find it hard to read 10 - 20 pages of a book without ever interrupting myself, take a look at my smartphone, do something else. More specifically, it should be pointed out that the name of our Association is derived from *Slowfood*, but also from *Slowmedicine*, which advocates the cause of a sober, respectful and just medicine. When deciding which logo to adopt for "Sloweb" we decided not to use animals and similar symbols, and rather to simply write "Sloweb" in italics as if it were written with pen and ink by a student of another time, who wrote slowly and thought carefully, and while he is thinking he grows...

Very beautiful, this image that evokes the tension of a growth towards a direction that we do not always know. The activity of your Association is based on two key values: ethics and responsibility. How do these concepts, which have a long philosophical tradition behind them, be declined in the digital age?



For some time I used the words “responsible use” and “conscious use” of the web without reflecting that they are two different branches from a common root, ethics: companies must be induced to a responsible use of the web, which means an ethical use, for example not to produce addictive software, and not to steal information from their users. Who should lead them in this direction? The citizens and the institutions of the State. Users, for their part, must have – or be induced and guided to – a conscious and ethical use. As for sex education, when using the web, they must be aware of risks and opportunities, dangers and pleasures. Today, there is a lot of talks about web ethics around the topic of *privacy*, but I think it is no longer possible to postpone the discussion and actions on the topic of *inequality*. Is it ethical to produce, offer, spread, a product that gathers an unlimited accumulation of the money of many in the hands of a few?

The web has an extraordinary ability to penetrate every social group, offering opportunities and some risks that are not small, yet it is sold everywhere and with few instructions for use, not like cigarettes that are sold at a high price to adults over 18 and only in special shops with and bear, not by hazard, the coat of arms of the State Monopolies.

Navigating: an exercise not easy and full of risks

Today surfing is hard: it's full of many dead fishes is the quote of the cartoon illustrating the cover of the volume. Could you explain this metaphor?

In 2017, with Federico Bottino, we asked Francesco Tullio Altan for a cartoon that could illustrate the book and, with his incredible kindness, he gave us that of the little man who pronounces precisely this sentence. You can surf the net, and it's more and more difficult to find good stuff, it's full of small dirty things, distractions and dead fishes. In my opinion his “dead fishes” represent the fake news, the garbage in general. Think of the pyramid

OGGI NAVIGARE È DURA:
È PIENO DI PESCI MORTI.



“Today navigating is hard, it's full of dead fishes.”

of knowledge, which has wisdom at its top, at the pure “data” at its base. Well, there are those who do not see that the net is every day, more and more full of “data”, almost always not validated and not made to last, almost always of little value, and in all this there is a growing imbalance with lots of gossip, little reflection, no wisdom: like an iceberg whose base pushes upwards, one day the pyramid will turn over, and the top of knowledge will be crushed by big data, with a great stench of rottenness everywhere, exactly as the one of many dead fishes.

Words are also important for innovators. “Language is our world” could be said paraphrasing a famous Wittgenstein statement. Does the glossary you publish in the volume evoke this purpose?

Of course. Words have different meanings for different speakers, which shows how difficult it is to build something good together, let alone innovation. Let me give you a simple example: the internet is a physical network made of cables, pylons, plastic cards and pieces made with almost all the elements on Mendeleev's Periodic Table. The web IS NOT. *Internet is not ethereal, the web is*, says Giovanna Giordano, co-founder of *Sloweb*. Internet consumes materials, electricity, its use implies producing carbon dioxide... And let's point it out clearly: with an increasing growth of 15 - 20% per year, the ICT produces already today more CO2 than the whole aviation industry. We cannot say “internet” meaning “the web” and vice versa. Yes, words are important.

The value of memory

This is an essential linguistic specification, because in fact the two terms are almost always used as synonyms. I would now like to touch on another theme with you, that of memory and digital heritage, important missions for Sloweb, decisive in a society crushed by the present. What kind of work are you doing on this delicate terrain?

At *Sloweb* some of us are dedicated to digital education (not just digital literacy), others to methods of including disadvantaged groups by teaching them a - conscious - use of the web. With Alessandro Macagno and others I devote myself to the themes of memory and digital heritage through professional experience and personal history. In these fields, we make treasure of the experiences and ideas of specialists in psychology, teachers, historians and archivists, and especially of *eMemory* and *eLegacy* users and of the HR, ICT, marketing and strategy managers of the companies we interact with every day.

eMemory and *eLegacy* are the platforms we have created to help families, communities and companies to select memories and documents that matter, to enhance

Focus - Cybersecurity Trends

them, to protect them in non-profiled environments, to define their destiny in order to safely pass them on. *Homo sapiens* is here because he has been able to stop hunting and gathering, and to talk, around a fire, about risks and opportunities, teaching the young people of the tribe what the future can bring, and how to face it. I don't say anything we don't know, but today too many of us don't realise and don't fight the fact that improper use of digital technologies leads to a waste of time, reflection, stories, and therefore, very soon, a loss of identity and memory.

What are the dangers of this drift?

We tend to delegate everything we need to remember to our smartphones, and the age at which *dementia* begins is lowered... and between memory and history losses, we find perhaps how humanity will disappear. Without knowing who we are, without knowing how to face the risks of all times, because no one in the evening will tell us more about the wolf and the three little pigs and when grandmother made bread for the following week and for the whole village.

And nobody selects what is important. I have 10 photos of my grandmother, and these are enough to tell her extraordinary story of courage through the 20th century. I have 100 of my mother. I risk, if I don't select them and continue to enhance their collection, to leave 100'000 photos to my grandson - and what will he do with them?

He'll throw them away, because I won't have left him - in reality - anything at all. Digital inheritance is a theme that is overbearingly emerging among us: we leave what we don't want and we don't leave what matters, including even passwords for bitcoins sometimes! A great chaos, which requires legal guidance - currently existing with the implementation of GDPR - and IT tools - which we are preparing before others will use them.

Memory is a great heritage, mortified by a process of removal and a rampant ignorance of history that cannot leave us indifferent. What is your assessment of this?

On memory, and the importance of saving what matters to grow well, I will tell you a little story. Two years ago, with Alberto Trivero, we had 500 shoe boxes made with the eMemory brand, in a beautiful orange colour, as a gift for the first users. Some of them are left over, and when I meet a grandfather or a mother I give them one or two, explaining that they are the *memory boxes* and they are to be used like this: we teach children to take into account, appreciate and value small elements - a photograph, a doggy or a puppet, their first drawing, that particular photo - of their life. Before us, adults, then together with them, then themselves alone will open the box from time to time, to save there a card, a stone, a postcard (!).



They will know who they are better, they will have traces of themselves and they will have learned to keep them. When they reach the age of 20 and possibly leave the family house, they will be able to take with them from the box what they need, to remember who they are, where they come from, and how far they can go.

At the age of 20, they already will have changed 5 or 10 smartphones, and lost the faces and small hearts drawn by their first loves, as well as an infinite quantity of gigabytes of images, all in bulk.

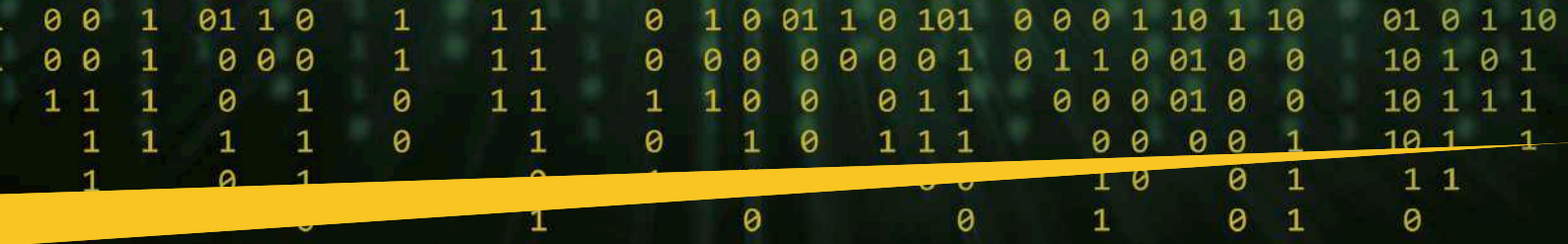
You have created what the Greeks called a *koinè* of scholars, intellectuals and tomorrow young people to reflect on a great phenomenon like the Net. Are we still speaking about the proposal of a constitution for the Internet, which represents the largest public space that mankind has ever had from the origin of history to today?

If three years ago I thought as an engineer that all this had a lot to do with technology, more and more I am realising that it has to do with *rights, politics, philosophy, ethics*; and let's not forget that today, computer scientists are the technicians who enter more deeply into our soul, and they, the computer scientists, have not studied neither theology, nor psychology, nor the rudiments of basic ethics as did doctors or engineers. They do not have a professional register, they answer only to themselves. So it happens that too many of them think that *what is technically feasible is automatically lawful!* And we see the results. As for a constitution, I can say that I come from years of global experience aimed at making corporate social responsibility evolve in a few multinationals as well as contributing to the standards and guidelines adopted at United Nations level, hence I can only agree.

A digital human rights declaration is needed

Among jurists, there is a debate on the reality of the Internet and on what is called the "protection of the electronic body". Surely this terminology is right, in the light of the evolution of recent years, don't you think?

Yes, of course, and I would add, thinking about the we, that in this field we have an *urgent need* for a *Universal Declaration of Human Rights* (including the environmental, social and economic impact of the digital world). And I would also add that Europe has a specific responsibility and opportunity in this regard, thanks to GDPR which - let's say by the way -



many North American people envy us. To develop the *eLegacy* software we worked closely with lawyers and law-makers - Pietro Calorio and Alessandro D'Arminio Monforte - and took full advantage of the GDPR, which offers very wide possibilities. With *eLegacy*, you recognise your digital presence as your face in a mirror, and thanks to GDPR you can unsubscribe, delete and customise your accounts, fix what MUST happen in case you get sick or die: what you leave, what you DO NOT leave, your rights, now and forever.

I would end with a more general question. Security and freedom are antinomic concepts that always marked human history and, in particular, underline the delicate relationship between the individual and the instruments of technology. Is it possible to achieve a virtuous balance in this essential bipolarity?

More generally, excuse me, this is a question for others, for science philosophers... Perhaps you want to refer to the technological development in the field of war and its benefits in terms of security and freedom? In the last decades the world has been "safer and freer" for many (not all) perhaps also thanks to the development of certain technological tools? Yes, maybe

so, but I do not feel like giving the answer in definitive terms, and I do not forget that in reality Imperial Japan surrendered to Russia and its infantrymen, not to the American atomic bombs. There are many myths on these issues which allows me to have a couple of "side" observations.

The first: today we are being spied all the time; this certainly makes us less free, but many believe that this is the *price for security* – the Talibans have prepared the ground well, by the way. I do not agree, and I tremble to think how many times in history we have already seen - and we shall see again - that not the information, but the hand that handled it, caused destruction. If today we are freer thanks to digital spies, we should ask the students in Hong Kong why they moved to Telegram, built by the exiled Durov, abandoning American social networks. We should ask the victims of the next holocaust, which will take place thanks to the big data in hours rather than days or years: the Jewish holocaust took years, the Rwanda one resulted in the loss of half a million people in only 100 days. It's not hard to see that with the use of advanced digital technologies, the next genocide will start and end in a few hours. They will find within a tenth of a second children, parents and friends - and with a few strokes of fake news everything will be forgotten after ten "tweets" and four "likes".

The second: today mothers have magnificent leashes, short and long, golden and light, to keep their little ones on a string. Mothers say that they are *safer*, and parents are "safe" or rather "reassured". Are the children freer? Do they go where they want, transgress and learn? No, nobody peels one's knees anymore. Children stay on a leash (wished by their parents) and security is paid for with the currency of the children's freedom. But what does all this entail? That the children grow up in a protected environment, they always have food and shelter at their fingertips, no one talks to them about bad things that could happen, they don't have experience in handling exhibitionists, thieves and street crooks, in fact they never go there at all, they go from a car to a screen, and... they just don't grow up.

When they grow up, it's scary to think they won't truly know how to make a decision without being manipulated - be it a political one, be it to have a child, be it to say NO - and even less will they know how to fight a war, be in solidarity with others, enjoy helping others, grow up in true friendship between human beings, in the *tribe*.

I would like to end stressing that this bad use of technology will accompany and accelerate a serious involution of human capabilities in general. Even on the web freedom is conquered, it can not be received as a gift. The same goes for security. I trust that young people will be able to conquer the first and the second.

Sloweb

MANIFESTO

Sloweb is a non-profit association established to promote the responsible use of information technologies and devices, and of the web and Internet applications in general. Sloweb activities include education, information and combating any improper public or private use of the internet and the web.

Sloweb asserts that the web is an extraordinary vehicle for knowledge, memories and quality information sharing. Sloweb acknowledges the endless opportunities and the huge potential that digital technologies offer, also in facilitating the inclusion of challenged or disabled individuals.

Sloweb recognizes that the use of information technologies involves a deep interference with the irrational, emotional and unconscious side of human nature. Besides the opportunities, risks and social phenomena exist that must be carefully assessed and in specific cases challenged.

Sloweb is also committed to protecting human fundamental rights for the ecological use of personal digital data: reduce, select, protect, own and delete for ever, managing your own digital heritage

All the above is essential to make the web safer, free and beneficial for everyone.

Focus - Cybersecurity Trends

Towards the advent of “informEthics”: The second edition of the Digital Ethics Forum will take place on October 1st.

Next October 1st, the second edition of the **Digital Ethics Forum** (to be held in Italian and English languages with simultaneous translation) will take place, in a streaming version as the protocols impose in this “strange” era of pandemic.” Pietro Jarre, founder of Sloweb, motivates the importance of this 2nd edition as “the events of the last period led us to look critically at the use of technologies and to focus our study on online behaviours in the public and private sectors, in order to understand how this affects our choices and inhabits. The aim of the initiative is to provide participants with new theoretical and practical tools to move ethically and consciously when using of digital tools. Deepening the themes of web ethics - from production, to distribution, to the use of software products and hardware technologies - we aim to address the “frontier issues” concerning the digital universe, in the belief that the time is has come to engage in a real fight for a fair and sustainable technological development”.



ORGANIZER *Sloweb*

The two-day programme (1st and 2nd October 2020) will be focused on issues related to the development of the information society from an ethical and political points of view, in order to observe the newly progressing dynamics of works, set in their more general context of cities that are changing in their urban configurations, in the logics of living, in the use of their very squares, places of relationships and centres of gravity of a physical community life. During the second day, two strategic strands for the future of the nation-system will be tackled: education and health, with the main objective of identifying the evolutionary paths that can take our boats out of the “sand banks” of this unprecedented crisis. “Sustainability means durability, propensity to dialogue with the stake holders, something that cannot be achieved without an ethical approach to every business”.

The importance of plural thinking for an ethical breakthrough

A counter-reaction movement must find its way, this is the message that will come from the days of the DEF and their will to reaffirm the strength of a plural thought in this delicate phase of transition to new digital forms. The

very concept of the business models is called into question. The real model is not to accumulate profits without rules, but to create the premises for a creation of added-values capable of determining positive external reactions within the communities of reference of the companies and their physical and geographical context.



In particular, there is a term of value, too neglected: the reasonableness which must inform all actors in the supply chain: from those who design sophisticated software to those who are often unscrupulous when placing them on the market. “A video game can create addiction to the point of inducing children to practice gambling. Without wanting to retrace the old paths of the “apocalyptic” or systematic detractors of development, I believe that some particular phenomena, already in place, should make us understand once and for all that not all aspects related to the overbearing development of technology tools can be tolerated by society. Just as we prohibit the rape or sale of minors, I don’t see why we can’t lift our shields to counteract the crimes which abound within the net, reflecting every human turpitude”.

“The New Alliance”

What Jarre invokes is a collective duty, which must move public institutions as well as managers and professionals.

The DEF days will certainly be useful to create a “koiné” of good will experts, ready to boost the reasons of a “digital humanism” inspired by values, and able to open up the way for others. It means to respect everybody in every moment of life, family, work, and more generally within the society. It is not about cultivating yet another utopia, but to lay the foundations for the advent of *informethics*, Jarre’s recently created neologism.

In fact, there is a need to start a new season, exactly the one preached by Ilya Prigogine – Nobel Prize winner for chemistry – in his 1979 book “The New Alliance”. There, the renowned scholar hoped for a profound metamorphosis of the hierarchy of knowledge, which would lead to a close collaboration between the exact sciences and the humanistic sciences, beyond prejudices or fenced divisions. Only under this condition, which unfortunately is still not met more than 40 years later after the publication of the essay, the human will be able to return to the centre, abandoning the sin of pride which led us exploiting the planet limitless and dragging us into the abyss we are experiencing.

Progress has to be guided towards ever higher goals for the civilization of rights, which represent a mobile frontier to be boosted continuously, if we want to respond to increasingly pressing and sophisticated historical, social and environmental needs. ■

Humanist manifesto for a “slow digital”



Author: Laurent Chrzanovski

There's nothing “*smart*” about what many people would like us to do. In this journal, many authors have repeatedly raised an alarm call about the harmful effects of digital dependencies.

We observed that specialists of all disciplines vigorously denounce the fraud of the “*smart everything*”, from “*Homo stupidus stupidus*” by the psychiatrist Vittorino Andreoli, via the various recent volumes of renowned philosophers such as - for example - Giorgio Agamben, Slavoj Zizek, Michel Onfray, to the volume by Shoshanna Zuboff dedicated to



“*The Era of Surveillance Capitalism*”, a milestone for any further study in the digital field, whether it's led by the “GAFAM” or not.

BIO

Historian and Archaeologist, free thinker, Laurent is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/ editor of 32 archaeological books, of more than 150 scientific articles and of as many general-public articles. In the frame of cybersecurity, Laurent is member and contractual consultant of the ITU roster of experts. He founded and manages the yearly “Cybersecurity Dialogues” PPP Congresses (Romania, Italy, Switzerland), organized in partnership with the highest international and national authorities . In the same spirit and with the same partnerships, he is co-founder and redactor-in-chief of the first cybersecurity awareness quarterly journal, *Cybersecurity Trends*, published in Romanian language since 2015, with English and in Italian versions since 2017. His main domains of study are focused on the relationship between the human behaviours and the digital world as well as the assurance of finding the right balance between security and privacy for the e-citizens.

COVID-19, politics and money:

But the COVID-19 pandemic changed many minds. A virus that was supposed to generate a perfectly manageable mini-crisis. Instead, we found ourselves in the middle of a “war” thanks to the lexicon used by the State propaganda and the measures taken by governments and politicians, duly escorted by various lobbyists from the pharmaceutical, digital and agro-alimentary world. To convince us, governments and their special crisis management bodies have relied heavily on various spokespersons, all of them top experts of great prestige.

The latter, for their parti-pris and the systematic refusal to question themselves and to debate with their colleagues who did not have the same opinions, have literally erased for a long time any public credibility of the so-called “scientific

Focus - Cybersecurity Trends

authority" as a legitimate "counter-power", an irreparable damage in the short and medium term, as former General Olivier Kempf has just written in the latest issue of the strategic magazine "La Vigie".

Well aware that we will have to cohabit with COVID-19 for at least a year, if not more, we absolutely do not deny the fundamental usefulness of individual responsibility measures, but we do not accept the doxa of "nothing will be the same as before", imposing a forced march to digitisation, Mao-style.

On the contrary, we reject it, in every aspect, because it leads to the total loss of the human being's own humanity, which is based on real relationships and does not pass through screens and other keyboard 'amusements'.

Unfortunately we realise that those who do not share the nefarious thought of the "all smart" bump into a united front of politicians, GAFAM representatives, ultraliberal think-tanks and citizens who do not have the necessary digital culture to understand that they will lose any rights within the already existing algorithms, which do allow a real personal and intimate espionage, 24/7/365, going far beyond the prophetic novel written by Orwell.

The author of the present lines, like others in this magazine, is one who works everywhere, with numerous air travel and nights away from home, to fulfill professional commitments and to meet, debate and talk freely about things that can neither be written nor discussed in a "smart" world, i.e. digital security strategies.

Years ago, a small dozen Italian gourmets came up with a brilliant concept that generated a global movement: "slow food". Let's stop eating badly, quickly, and go back to taking time and enjoying the authentic taste of traditional foods and recipes.

We have long practiced this teaching, which we have extended to good sleep and *slow digital*. In short, if we travel so much for stimulating and vital encounters, now that we are no longer in our twenties, we cannot afford to eat badly, sleep badly and waste useless time in front of our three "smartphones" and two laptops, a multiplicity of tools made necessary by the restrictions of their different uses, exactly the lifestyle that promotes, with essays of great value, the NGO *Sloweb*, (see the interview of its founder, Pietro Jarre, as well as their next world congress announcement and whereabouts, in this issue).

If we were to summarise the 'smart catastrophe' as we observed way before the appearance of COVID-19, we can quote two anecdotes, one for each of our jobs.

In the academic humanistic world, our youngest students have moved from the 'Wikipedia generation' to the 'Pinterest/Facebook generation', despite a quantic jump in the last five years in digitising an impressive number of articles, journals and scientific books, continent-wide. These

"easy-to-get" and "smart" sources, with their more than approximate content, create additional duties for faculty teachers, having to not only start from zero, but, since the first year of university, to contradict with solid arguments what is proposed, in good faith, by their students.

In the 'cyber' world, it is enough to remember the alarm launched by all the intelligence services of the United States: since more than 80% of the candidates no longer know how to write by hand, handwriting tests were almost eliminated, even if they were vital precisely because they allowed the experts of the forensic units to provide the best information on the various aspects of the character and of the psyche of the "inner being" of the candidates, positive as negative or clearly anomalous...

Under these conditions, repeating our motto "smart = spy", we do not share any proposal of a forced acceleration of the so-called "smart working".

The social consequences of such a change in our *modus vivendi*, with its corollary of *smart cities* and *smart governance*, will be just worthy of the legend set by Slavoj Zizek under an image of the empty streets of Wuhan "the GAFAM dream has come true".

After kindergarten, we'll do everything from home, where we'll study from school to university, we'll work with more or less protected tools, we'll share our lives on zoom, we'll order everything via the internet, we'll find partners via Meetup, and we'll go out just to get some fresh air or eat with friends we met on Facebook. After our extreme unction / last blessing on Vaticanviewer (Imamviewer, Rabbiviewer etc. according to our beliefs) the last thing we'll see on earth will be a screenshot of an episode of a serial on Netflix.

This "smart" life will obviously bring a wide corollary of physical and mental illnesses, as it has been demonstrated by several medical and interdisciplinary studies recently published, among which the gruesome "Meet Susan, the future remote worker" stands out. This is a projection of a woman who has been working from home for 25 years -, a synthesis of a transdisciplinary project made accessible to everyone by the largest multinational recruitment agency, Directly Apply (<https://us.directlyapply.com/future-of-the-remote-worker>).

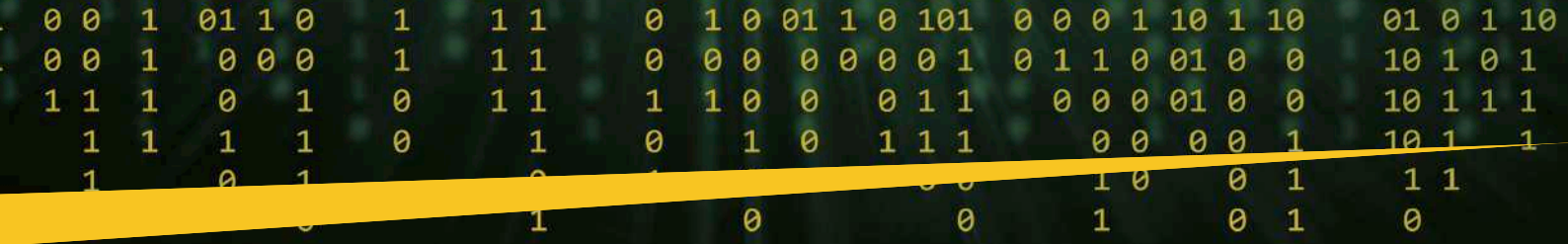
A northern hemisphere with empty towns and villages and sick people at home? We reject it.

Not because we could not go and live in countries of the other hemisphere, where life is beautiful because there is death, where health is enjoyed because there are diseases, where talking to others in the street makes the day rich, and where any work must be well done because if not, you do not eat. But because until today, it is from the northern hemisphere that all our educational, philosophical, religious, moral, ethical, aesthetic and sensorial substratum comes. And we refuse to see this treasure destroyed by a camarilla at the service of the creators - none of them being European - of this concept.

The turning point: private insurances to save the human being against their will

Going back to *smart working*, it won't be able to be adopted quickly. Because exactly at this point, another major cartel enters the game, private professional insurances, now compulsory in the UK and more than half of the EU states. Their rules will put the brakes to the "smart work" self-isolation fanatics.

As a matter of fact, if the number one employment portal in the United States has published the monstrous "Susan", it is precisely because the entire U.S. ecosystem relies on private insurances and lawsuit possibilities. If there are serious professional issues, the company that brokered and made a recruitment






- 

Computer Vision Syndrome
Staring at screens all day can also cause Digital Eye Strain or Computer Vision Syndrome. This results in dry, inflamed and bloodshot eyes, as well as eye irritation, redness and blurred vision. Over time it can also negatively impact your eyesight.
- 

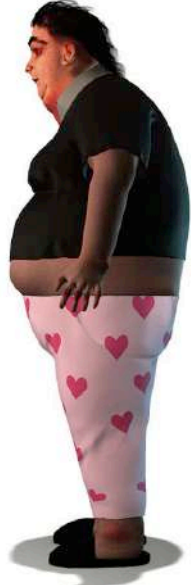
Poor Posture
Lack of physical exercise and too much time spent with poor posture in front of a screen can result in a hyperextended neck, rounded shoulders and a hunchback which will start developing over time. It will work its way from your neck to your hands and back as the strains slowly creates a bend in the neck.
- 


Repetitive Typing Strain
Typing repetitively over long periods of time can lead to repetitive strain injury in your hands and wrists that can significantly worsen and result in poor posture in other parts of the body over time.
- 

Hair Loss
Vitamin D is mostly absorbed from sun exposure, so working indoors all day can leave the body deficient which can cause hair loss and new hair growth can be significantly stunted. Vitamin D deficiency has also been linked to alopecia, an autoimmune condition that can cause bald patches on the scalp.
- 

Dark Circles
Staring at multiple screens while working all day can cause prominent dark circles to form in the skin under your eyes, leaving you looking tired and haggard after prolonged periods.

- Tech Neck**
Working from a device such as a phone or laptop can contribute to the modern term 'text neck'. This results in excessive strain on the neck, a rounded shoulder and often counter strain in different parts of the body such as increased lower back pain and shortened hamstrings.
- Increased Wrinkles**
Wrinkles are a natural part of ageing, however certain habits such as squinting at a screen all day can increase the onset of premature lines forming beneath the surface of the skin, leading to wrinkles such as crows feet or frown lines.
- Obesity**
Long periods of being stuck inside, constant snacking and lack of exercise can lead to an excess body fat accumulating over time. Working from home could potentially lead to a population that is overweight, considerably so in the stomach, thigh and bum areas, as well as your ankles.
- Pale & Dull Skin**
Lacking in Vitamin D and B-12 due to reduced sunlight exposure can result in pale, dull and mainourished looking skin.
- Increased Stress**
Going without human contact for long periods of time can lead to higher levels of the stress hormone cortisol, which raises blood pressure and has harmful effects on physical health. Overworking leads to chronic stress producing high levels of adrenaline and cortisol, associated with chronic health conditions and cardiovascular disease.



- 
- 
- 
- 
- 

“Susan”, with all the pathologies proposed by doctors and psychiatrists, after 25 years of smart working... © us.directlyapply.com

possible - if it had a possible knowledge of those issues - is therefore guilty by association, immediately after the direct employer. In Susan's case, with all the illnesses directly caused by her workstyle, even the recruitment portal, knowing that she would get a "remote working" place, will have to participate in the compensation for damages and interest granted by the U.S. courts, sums of money that are not to be joked about ...

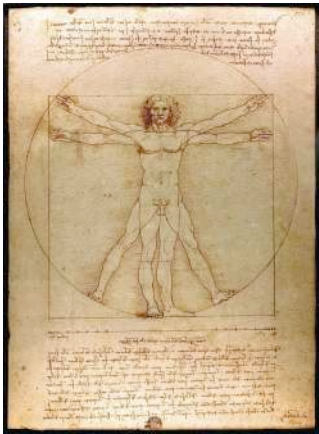
As a Swiss freelancer, we can easily explain why continental countries will either choose total illegality or will have to bear extremely high costs to make legal a job at home that, in the case of employees, public or private, can be done only and exclusively after obtaining the free consent of the worker.

Conclusion

Since humanism, the vocation of man to be one of the most sociable animals on the planet, on the ground and not through interposed screens, is not convincing to any politician fascinated by the digital explosion and, within the

EU, by the huge new 2020-2027 funds dedicated to every EU country's digitisation initiatives.

Therefore, any "smart" acceleration will be truncated by the European fines that will be imposed on the State who will allow its own entities and the private sector



to send home a good part of the employees without the obligation to grant to each of those "self-insulated" the above-mentioned private insurance guarantees.

Focus - Cybersecurity Trends

Instead, we should begin, throughout the whole European continent, to think about correcting the tragic consequences of the accumulation of mis-management and bad administration decisions of the past three decades, before hiding everything under a new miracle carpet whose name seems to have been invented to lure chickens - "smaaaart".

And what about starting to learn how to use with "slow cleverness" technologies, after a careful evaluation of their intrusiveness and security level?

Post-scriptum: stay away from your smartphone as much as you can!

Probably one of the most pertinent researches, explaining the topics we will develop further, was led by a team of the university of Chicago. Bringing some hundreds of students and non graduate citizens into three big classrooms, they were all given the same tests, basic arithmetic / memory questions and general questions requiring some basic intelligence).

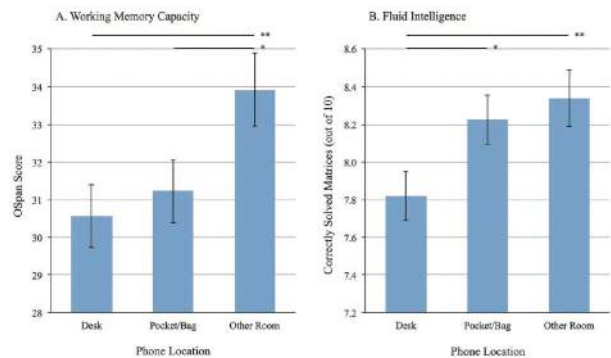
The participants of the first group had their smartphone set at one meter, with interdiction to grab it, the ones of the second group had their smartphone set into their pocket or bag, with interdiction to grab it, and the third was in a room with the smartphone left at a custodian outside. The graphic hereunder left us speechless and needs no comment: within the participants of the first group, the simple view of the smartphone doubled by the incapacity to grab it diminished by almost 1/2 their memory capacity and by 1/3 their "fluid intelligence" in comparison with the participants in the room without their phones.

A business performance disaster

Tolerance at work versus the disponibility of employees to be reached outside workhours turned to be a major mistake. Recently, some of the most renowned general public business magazines dedicated a whole series of articles on the companies' losses due to the time spent by the employees with their smartphone - raising up to 4 hours per day on 8 working hours! (see for instance Akhtar 2019).

An old proposition made by scientists came back: the suggestion to educate employees to dedicate special timeslots ("Zeitgebers") for organizing better their personal and professional lives but this method, in nowadays individualism and lack of biorhythm and discipline hygiene, does not seem to offer quantitative successful results to fight further steps into the employees' addiction to smart tools.

Moreover, recent studies on tomorrow's employees and leaders show a constant degradation from an increasing addiction to smartphones (Arefin, Islam, Mustafi, Islam 2017;



© Ward, Duke, Gneezy, Bos 2017, Figure 1. Experiment 1: effect of randomly assigned phone location condition on available Working Memory Capacity (OSpan Score, panel A) and functional Fluid Intelligence. Participants in the "desk" condition (high salience) displayed the lowest available cognitive capacity; those in the "other room" condition (low salience) displayed the highest available cognitive capacity.

Mosalanejad, Nikbakht, Abdollahifrad, Kalani 2019) and very dangerous effects on several individuals : changes of personality, constant increase of stress and isolation/loneliness, a phenomenon which is much more radical within adults already inserted in the work market (Ellie, Mazmanian 2013) where the smartphone "news flood" chosen by each adult may lead to conflicts with his co-workers because of the radical positions acquired by being fed by chosen "info" sources and social network acquaintances.

It is worth noting that several papers indicated the very poor and contrasting arguments made on this kind of addiction until the most recent years, as most researches were made on employees' self-assessments or statistical samples, few of them being led during a long period of time (on the contrary of the masterpiece study by Tossell, Kortum, Shepard, Rahmati, Zhong 2015). Now, new study standards have been established (Li, Lin 2019), and a Korean university having access in PPP to governmental databases applied with success addiction statistics based on data mining, i.e. on what the persons are using as apps and how many timesthey spend on each (Lee, Han, Pak 2018). ■

Quoted researches:

Akhtar 2019 = Allana Akhtar, Smartphone habits that are getting in the way of your success, in BusinessInsider Apr. 21, 2019 (<https://www.businessinsider.com/smartphone-habits-that-are-ruining-your-productivity-2018-7>)

Arefin, Islam, Mustafi, Islam 2017= Afrin Shamsul Arefin, Rafiqul Islam, Sharmina Afrin, Mohitul Ameen Ahmed Mustafi, Nazrul Islam, impact of smartphone addiction on academic performance of business students: a case study, in: Independent Journal of Management & Production (IJM&P), v. 8:3, 2017 (www.ijmp.jor.br/index.php/ijmp/article/view/629/726)

Ellie, Mazmanian 2013 = Harmon Ellie, Melissa Mazmanian, Stories of the Smartphone in Everyday Discourse: Conflict, Tension and Instability, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York: ACM, 2013 (<https://ellieharmon.com/docs/HarmonMazmanian-SmartphoneStories-CHI2013.pdf>)

Lee, Han, Pak 2018 = MyungSuk Lee, MuMoungCho Han and JuGeon Pak, Analysis of Behavioral Characteristics of Smartphone Addiction Using Data Mining, in Applied Sciences 2018: 8 (<https://www.mdpi.com/2076-3417/8/7/1191/htm>)

Li, Lin 2019 = Li Li, Trisha T. C. Lin, Smartphones at Work: A Qualitative Exploration of Psychological Antecedents and Impacts of Work-Related Smartphone Dependency, in: International Journal of Qualitative Methods Volume 18: 1-12 (2019) (https://www.researchgate.net/publication/330572104_Smartphones_at_Work_A_Qualitative_Exploration_of_Psychological_Antecedents_and_Impacts_of_Work-Related_Smartphone_Dependency)

Tossell, Kortum, Shepard, Rahmati, Zhong 2015 =Chad Tossell, Philip Kortum, Clayton Shepard, Ahmad Rahmati, Lin Zhong, Exploring Smartphone Addiction: Insights from Long-Term Telemetric Behavioral Measures, in International Journal of Interactive Mobile Technologies Volume 9: 2 (2015), pp. 37-45 (<https://online-journals.org/index.php/i-jim/article/view/4300>)

Ward, Duke, Gneezy, Bos 2017 = Adrian F. Ward, Kristen Duke, Ayelet Gneezy, and Maarten W. Bos, Brain Drain: The Mere Presence of One's Own Smartphone Reduces Available Cognitive, in: Journal of the Association for Consumer Research (University of Chicago), Volume 2: 2 (April 2017), « The consumer in a connected world » (<https://www.journals.uchicago.edu/doi/full/10.1086/691462>)

Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power*, Profile Books Ltd, London / Public Affairs, New York 2019.

Review by Laurent Chrzanovski

"Every email we send, every interaction, every emotion we have is sold, controlled, manipulated. Never had human society seen such an enormous concentration of wealth, knowledge and power in so few hands. Haven't you noticed? Read Shoshana Zuboff."

Roberto Saviano, author of *Gomorra*

Since its first UK edition, and mainly the US one in January 2019, edited by the prestigious publisher Public Affairs, Shoshana Zuboff's masterpiece has already entered the pantheon of books that build the cornerstone of a basic understanding of the digital ecosystem that the world uses daily.

Writing a useful review on this real "manual of understanding and survival" is an extremely difficult exercise, since the week following the official launch of the book, the world of research and the media - from the most specialized to the most generalist - have produced a quantity of texts dedicated to Zuboff's in-depth analysis of what's going on.

Before embarking on a real initiatory journey «à la Prévert» - i.e. a choice of the most relevant parts of the book, given the abundance of vital information contained in the volume and the small space reserved for us, we must immediately stress that the author is, as a specialist, a real anomaly in today's world.

Chair of Business Administration (emeritus) and Full Member of the Berkman Center for Internet and Society, at Harvard University, Shoshana Zuboff has never been adept of either annual quickly-delivered volumes nor of small or medium-sized scientific articles.

On the contrary, she focused all her energy into writing only 3 books, all of which becoming, as soon as they appeared, milestones both in the university world and in the field of public success, an extremely rare fact in the academic world: *In the Age of the Smart Machine: The Future of Work and Power* (New York 1988), *The Support Economy: Why Corporations Are Failing Individuals and the Next Episode of Capitalism* (London/New York 2002), and the volume we are dealing with today.

An unparalleled writer and disseminator, Shoshana Zuboff spent a great part of her time explaining her theses and dealing with current issues in the best media for the general public. Interested readers can access many of these essays, interviews and lectures on the author's website: <http://www.shoshanazuboff.com/>.

The question is as simple as Zuboff resumed in a must-read Q&A with French journalist Géraldine Delacroix (1) "We are victims of an unprecedented asymmetry: Surveillance capitalism knows

everything about us, while its operations are designed in such a way that we know nothing about it. It nullifies the fundamental rights associated with individual autonomy, rights essential to the very possibility of a democratic society."

Worse, the semantic definition of the title on the very first page of the book may only leave us frightened and speechless:

Sur-veil-lance Cap-i-tal-ism, n.

1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales

2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification

3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history

4. The foundational framework of a surveillance economy

5. As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth

6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy

7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human

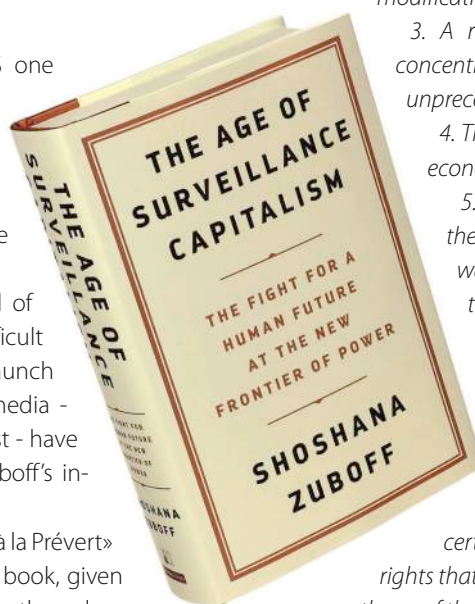
rights that is best understood as a coup from above: an overthrow of the people's sovereignty.

At this point, it is necessary to underline that Shoshana Zuboff was the first woman to be Professor of Economics at Harvard - she hence was the teacher of number of influential businessmen and politicians building the élite of today's USA, and became gradually interested in the digital world since the late eighties.

Therefore, we are not facing here another excellent «whistleblowing book» by ex-insiders such as «*I'm Feeling Lucky: The Confessions of Google Employee Number 59*» by Douglas Stewart (New York, Houghton Mifflin Harcourt, 2011) or the very recent "*Zucked. Waking Up to the Facebook Catastrophe*" by Roger McNamee (New York, HarperCollins, 2019).

On the contrary, we are in front of a university textbook with over 50 pages of bibliographic references, with the enormous advantage - a recipe for its success - of being written with a style talent worthy of an established thriller author. Every sentence, every concept is supported, argued, dissected, making the argument unassailable. And therefore even more serious.

Leaving aside the thousands of methods of behavioural espionage, placing now the "majors" in an almost total possession of our past, present and future existence, which make up the majority of the volume, we will focus on the causes that have led the entire planet to suffer the consequences of this situation.



Biblio - Cybersecurity Trends

The total abandon by European – and first and foremost American – State authorities is explained by the very person that educated so many politicians and CEO's of various sectors during her career: at first, technology and the swift towards data collection was not perceived as a threat. Evolving, it was not understood - neither its dazzling technical capacity for almost daily improvements nor the underlying purposes of the hugest ever data collection made in history -.

By now, the trend being dictated, and implemented by the «majors» with the consent of all those who enter data on the network, it seems no longer being faced with success - especially because of the fear of many political elites to be considered by the citizens as the advocates of an equally intrusive “deep State” similar to the one experienced and denounced by Edward Snowden during his years of work within - or in collaboration with - the NSA.

Zhuboff explains this fact by putting in their context expressions of 2010, considered then as simple demonstrations of ego and not as a clear declaration of total war. The interview of Andy Grove, then CEO of Intel, who declared to the Washington Post, stands out in that year: *“High tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap (...) and so what you want to do is you want to make sure that the government does not get in the way and slow things down”.*

This simple concept – and really illegal besides being immoral – was hugely condemned and faced from the intellectual elites to not a few politicians. Absolutely not caring at all of what “moralists” were saying, the idea was reiterated crystal-clear by the Eric Schmidt, then CEO of Google, in a crystal-clear sentence, impossible not to be misunderstood: *“technology moves so fast that governments really shouldn't try to regulate it because it will change too fast, and any problem will be solved by technology. We'll move much faster than any government”.*

Businessmen, politicians, economists, not having the necessary digital culture and not even disposing of the right advisors to understand what, at that time there, was still possible to regulate somehow by law, chose to do business with those new technologies, in an ultra-liberal way, happy with the new flood of money those various companies and their lobbies brought them.

Today's situation, as Zhuboff explains both in the introduction and in the conclusion, imposes only one way for those who want to be free: exile. One's own home, full of transmitters, already “belongs” to the majors, and therefore even taking refuge in the house is no longer useful. With much bitterness, the digital natives, for whom connectivity should be “a human right” but without surveillance, are carefully portrayed in their disgust for this world.

It is well explained that their freedom, far from being freely connected as they dreamed to, means simply renouncing to exist and to live with a thousand masks. By using special technological means, masks and anti-visual reconnaissance clothings, one can in fact escape to “the eye of God” (of the “majors”). But they are masks (each one's original face) which that cannot be removed, except in

ultra-protected places. It is the new field - fully imitating the military one - of the *art and science of hiding*.

The last pages of the book are a real manifesto for a civil awareness and hope to raise a powerful social movement that would inevitably lead governments to take the necessary political, strategic and legal measures to avoid falling into, as Zhuboff said to Delacroix, *“a reactionary era in which capital is autonomous and individuals are heteronymous; the very possibility of democratic and human development would require the opposite. This gloomy paradox is at the heart of surveillance capitalism: a new type of economy that reinvents us through the prism of its own power”.*

If there is a sacred union on Zuboff's first proposal to save what can be saved: to put the human back at the center of a performing cultural and educational system allowing every citizen to understand the ecosystem in which one lives, on the other proposals we see many debates in Europe.

It is precisely on the point based on the *“American way of life”*, where an individual can make things change and where society can save democracy, that the most massive criticism has been raised, first of all by sociologists but also by various state think tanks.

Our European laws, our freedoms, our citizenships are in fact managed by a social pact, based not only on Rousseau's work of the same name but also on the realities in force, starting with the services that the State must offer us in exchange for our contributions, an axiom introduced by Bismarck and continued until the Second World War, perfectly following a philosophy and a continental legal corpus of Greco-Roman style, the central topic of the world famous book by the Slovenian philosopher Slavoj Zizek *“Like a thief in broad daylight. Power in the Era of Post-Humanity”* (London, Penguin, 2019).

For a European reader, the other “touchy” point of Zuboff's book, is avoiding to mention the falsification and even denial, by the GAFAM, of morality, philosophy, history, biology and sexuality a must in today's United States where every little distortion to “politically correct” triggers a tsunami of protests. This particular behavior of the majors is exactly the subject of one recent essay of the French philosopher Michel Onfray's latest, reviewed below.

To end, we can not but agree with the prophetic sentence. We need synthetic declarations that are institutionalised in new centers of democratic power, expertise, and contest that challenge today's asymmetries of knowledge and power. This quality of collective action will be required if we are finally to replace lawlessness with laws that assert the right to sanctuary and the right to the future tense as essential for effective human life. (ebook version p. 319). If we fail to do that, we will not only be co-responsible of our spied present but, above all, of the totally controlled daily future of the next generations. ■

(1) Author's translation from a paragraph Géraldine Delacroix, *Le capitalisme de surveillance, maître des marionnettes*, Médiapart, 02.03.2019)

**Michel Onfray, *Théorie de la dictature*.
Précédé de *Orwell et l'Empire maastrichtien*,
Paris, Robert Laffont, 2019, 615 pp.**

Review by **Laurent Chrzanovski**

As with almost all of Michel Onfray's works, this essay is still not available to English-speaking readers, as on the contrary to Slavoj Žižek's essays (on the same topic, see the Slovenian philosopher's recent masterpiece, *Like A Thief In Broad Daylight: Power in the Era of Post-Humanity*, Penguin, London 2018), the author's style and his (few) totally France-dedicated book parts are considered by major non-Latin speaking publishing houses as not fit to their readers, while Onfray's texts are widely available into Spanish, Italian or Portuguese. It is somehow sad, as this very book, proposed by the "church-eater" philosopher (his nickname in Italy) is the first to have been acclaimed by the Catholic media, especially for the parts that deal with sexuality and post/trans-humanity,

Continuing the reflection delivered by Shoshanna Zuboff's masterpiece we just summarized, the latest writing from the French philosopher is a vademecum on the current situation of cultural, social, educational, ethical and moral degradation of our continent, whose basis are exactly the infiltration and complete implementation, in Europe, of the "surveillance capitalism" denounced by Zuboff.

Michel Onfray makes a very useful and captivating popularisation attempt, in a simple, clear and provocative style, as for all the other themes vital for the society he deals with.

It is not a "dense" book like those where Onfray deals with history and thoughts of past philosophers, but a manifesto with a deliberately exaggerated style of printing to make every idea better understood: the pages of Orwellian theses, of no more than two paragraphs, are followed by pages, each of those carrying an example or a concrete thought, often of a few lines.

This innovation is also an irony wanted by Onfray, who gives us a book that often looks like a print of individual "tweets", to underline the loss of the culture and of the art of paper-publications reading, denounced in many passages of the volume.

In the long introductory part "*Orwell et l'Empire maastrichtien*", Onfray traces the history of the European Union and denounces its underlying ideology, from the planning stage to the ratification of the Maastricht Treaty.

The frantic hunt for an (ultra) liberal-style single market, the creation of a currency which is independent of the real economic

and political factors of its member-States, and all the critical issues which remained the exclusive prerogative of each single government, are, according to the author, the seeds that have allowed our entire continent to become a sort of bad copy-paste of the United States system: "*in almost a quarter of a century, this "Maastricht state" has become as toxic as the regimes supported by converted former sixty-eight students - who, in this sense, remained faithful to their beliefs: they love political forms that keep people on a leash.*"

The abandonment of the promise of positive exchange between cultures, of a pan-European social, educational and military measures is evident: "*it is even the opposite of the promise that was fulfilled: the galloping impoverishment, the proliferation of racism and anti-Semitism, the participation in the NATO-led wars in the rest of the planet leading to the destruction of the stability in all the Near and Middle East area, the collapse of social protection systems and public services. Never before has a promise been so betrayed.*"

This preface is necessary to understand that the monstrous world, seen within the United States with Zuboff's eye, is already being realized in an even more nefarious, hidden and improving way in a number of increasingly weaker countries united in a system that do not manage anymore the essence of the real power (i.e. a good management of culture, education,

health, defense and average level of individual and productive well-being), all fields remaining an exclusive prerogative of each government.

Different laws, different means, different policies in 26 states have done nothing more, with the help of Europe itself, used as a nice scapegoat but also as a "rescue pretext" of every government speech when it comes to unpopular measures.

From here, Onfray recalls Orwell's thesis, explaining, following each of the Ten Commandments of "1983", that we are already fully experiencing the dictatorial surveillance Orwell himself predicted for 2050.

We therefore resume the terrifian decalogue enabling the exercise of a totalitarian 4.0 dictatorship, managed by a global ultra-minority involving "representatives" and "agents", between politicians, media owners and scientists, in each country.

The first: destroying freedom - thus activating a police of thought, ensuring perpetual surveillance, reporting thought yet unrealised crimes, eliminating loneliness, rejoicing of the obligatory holidays, ruining personal life.

On this point, the naivety and growing dependence of most Europeans on social media and smartphones despairs Onfray. The European man is "*executioner and victim of himself, hammer and anvil of himself, wound and knife of his own flesh.*"

Extending the discourse to totalitarianism 4.0, which gets its vital energy abusing the weaknesses of each of us, he adds: "*This*



Biblio - Cybersecurity Trends

surveillance is the most successful ever, because no totalitarian regime could have hoped for something better than a subject who, thanks to narcissism and selfishness, becomes a self-snitch with jubilation, satisfaction, pleasure and joy! Terence had theorized the Heautontimoroumenos in a piece of the same name, Baudelaire had made a sublime poem of it, the postmodern individual embodies it”.

Continuing, the philosopher adds: “All this information is gathered in a cloud, the famous i-cloud that replaced the angels in the empty sky of the Judeo-Christian God. It is the safe in which we put the misleads we pledge to offer our thieves. We are constantly robbing ourselves for the benefit of those who rob us to make the most of us - the world of the GAFAM”.

The second: impoverishing the language - thus practicing a new language, using ambiguous language, speaking only one language.

When we observe that 200 words are enough to read a USA Today edition, and that the prestigious Le Monde has gone from 10,000 to less than 2,000 words in a decade, accepting and adopting all kind of Anglo-Saxon neologisms, we understand even better the hidden will of this choice, which wants to bring us all to speak “Globish”, a sort of Americanised Esperanto: “The process of language impoverishment is certainly a matter of words, spelling, grammar, neologisms, acronyms, but also rhetoric. Preventing everything that allows one to reason, reflect, think, conceive, speculate, is just as important when one’s project is to make an individual completely uncultured.”

The third: abolishing the truth - spreading false news, erasing the past, producing reality.

Onfray is explicit from the beginning: “When the death of the truth is announced, the lie has its own free boulevard. Thank you Foucault, thank you Deleuze. The generalization of social networks has given a maximum visibility to lies, approximation, fairy tales, propaganda, mystification, legends, fables, intoxication. Logic no longer makes law. Neither does reason. It is the responsibility of the person who denies the lie to prove that it is not a lie. Otherwise, the lie becomes truth.”

In the long chapter, the anecdote the philosopher invented to better explain this case history is funny, if it wasn’t worth to cry: “I declare that I spent the evening with a unicorn who told me about his sex life. My interlocutor doubts. I ask him to prove to me that my statement is false, even if a priori unreasonable. He can’t do that. So I conclude that I’m right, he’s wrong, and as a result, I spent the evening with a unicorn... I can also add that by his doubt, my interlocutor disrespected me, and by doing so he insulted me, a crime that demands and justifies compensation. Otherwise said, I can use all the law codes into and strike at anyone who doubts that I spent the evening with a unicorn... This is where we are in a country which, for half a century, has lost all legitimacy to call itself Cartesian...”

The fourth: suppress history - that is, foment hate, rewrite history, destroy books.

“The erasure of the past leaves a void that must be filled with the rewriting of the past. What happened did not exist, but what never happened existed - that is the goal of the art of building a past that did not take place, of making memories of facts which never happened. Where there was substance, now there is nothing; where there was nothing, now there is substance.”

“With the collapse of traditional morality and the impunity allowed by the anonymity granted by social networks, hate is one of the most common messages. It allows to avoid debates, discussions, exchanges and controversies for the sole benefit of the discredit of a person. The logic of the scapegoat is at the top of the list. However, anyone who is in the grip of hatred, individuals or people, states or nations, no longer thinks. Disconnected from his neural system, he is connected to his neuro-vegetative system. The cortex is fired, the reptilian brain leads the way. Our time is a time of hatred.”

In these two statements, Onfray reaches the last book of the regretted Zygmunt Bauman, Retrotopia (New-York, Wiley, 2017), where the Polish-born sociologist explains the creation and diffusion of State propaganda of a false national history full of glory, and therefore the regret for “golden periods” that never existed but that the governments and parties that make great use of it would like to revive...

The fifth: deny nature - thus deny the laws of nature, impose a hygienism, procreate medically.

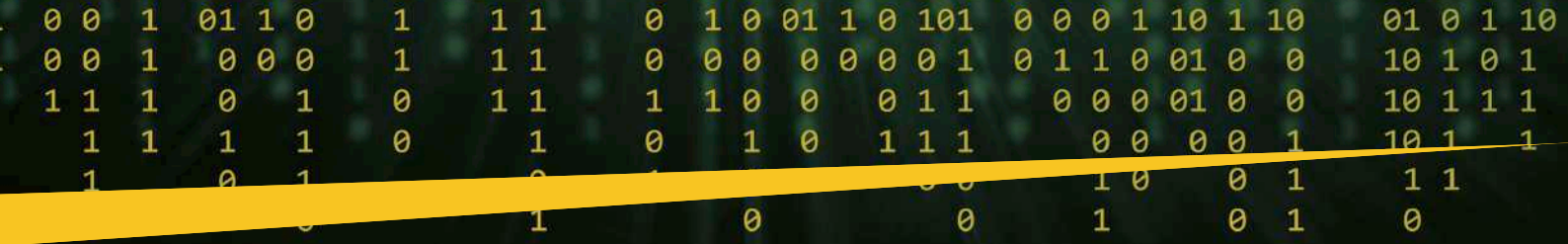
Only one real example, as a total challenge to any millenary Western ethics and morals, illustrates the entire chapter alone: “In its March 30, 2019 edition, the Daily Mail reports that in the Nebraska, a 61-year-old woman gave birth to a baby girl conceived with the sperm of her son and the ovule of the sister of her son’s husband. The mother who gave birth to this child is therefore also her grandmother, but this niece also has her aunt as her mother, which gives her four parents, all in the most perfect incestuous logic, since the mother was inseminated by her child’s semen. If this aunt were also to be a mother, the children would be cousins of half brothers or sisters at the same time.”

And to conclude cynically: “If incestuous logic must be the most progressive sign of progress, one can understand that we do not subscribe to this kind of progress...”

The sixth: artificialise bodies - destroy the pleasure of living, procreate medically, organize sexual frustration.

Just starting from the previous example, Onfray denounces the “political correctness” imposed by GAFAM censorship. The birth of the child provoked many comments, many immediately eliminated by the new planetary “moral censors” because they were judged homophobic or anti-progressive.

In this context, Onfray is perfectly right when he denounces that “If gender and race do not exist, the fight against gender or racial discrimination cannot exist either. Both sexual and natural racial differences do not in fact lead to gender or racial inequalities. Natural difference becomes an inequality in the cultural register only after discrimination has been established between two separate groups and validated by empirical evidence.”



Worse, the fruit of the ambiguous and ambivalent digital society, is to trash any previous morality or ethics by using messages “scientifically” distilled by social media, *“Man is considered outside of natural cycles, seasonal cycles, solar and lunar cycles, cosmic cycles. Son of cement and asphalt, son of cities and cement, he produces libraries and, more recently, digital flows. The question of gender is no longer a question of nature, but of culture.”*

The seventh: ruin culture - reassign places of worship to other uses, industrialise artistic production, lower the education of the people, misinform children, suppress beauty.

Here, Onfray brings a new idea, which actually invades the digital world: *“Nature opposes culture, the first nonsense that prevents us from thinking. The higher would be the first, the smaller would be the other: a natural being would turn out to be rough and simple, if not simplistic and idiotic, if not the cannibal of Montaigne or the good savage of Rousseau. A cultured being is adorned with the feathers of the most beautiful peacock. Culture is not in nature, so it is not found in the countryside, but in cities. It is urban. This petrification of souls, this cementing of intelligences, this asphaltting of reason contribute to the cancellation of nature, which is now considered only in the configuration of urban ecology and in an anthropic way: according to this urban-centric worldview, man remains at the center of nature, he is its master and owner. If the planet is warming up, it is his own fault.”*

According to Onfray, only nature, good and evil that make man suffer are now true culture, allowing to throw literature, art, philosophy and everything that allows to think into oblivion.

The Eighth: Foment wars - therefore: create an enemy, keep wars going on.

Onfray, here, does not surprise strategy experts and comes to support UN reports that armed conflicts - even though many of them are geographically minor - have grown dramatically since the end of the Cold War. And it condemns the deliberate ignorance of conflicts in which there is no monetary interest in the same way that the disproportionate vocabulary and treatment of conflicts where our states are “the good guys” versus all other wars...

“In a world where hatred has been propagated by progressives, progress is to believe that one thinks only when one hates, and, as a consequence, the seek for an enemy is vital: without that one cannot live; it is to maintain sad passions as a viaticum; it is to psychiatry critical thinking and to dirty anyone who does not think in the same way rather than criticize his arguments. It is justifying wars and defending them when they are declared, but condemning them when “others” take the same initiative; it is pretending to be surprised that terrorism presents itself as a response from the weak to the strong; it is praising peace by trading weapons and justifying their use on the battlefields where we are “invited” or on those we created ourselves.”

The ninth: to aspire to the Empire - therefore: to govern with the elites, to practice class urbanism; to administer the opposition, to psycho-analyse all critical thinking, to hide power.

The misdeeds of ‘social class-organised’ urbanism, which can be seen in the French suburbs and their permanent state of decay, serve Onfray to open a global scenario where these real ghettos will become the norm, as *“Property, for example, is no longer in the hands of individuals, but of groups. The mission of the elite, composed of journalists and intellectuals, advertisers and trade unionists, bureaucrats and politicians, sociologists and professors, technicians and scientists, is therefore to perpetuate the confiscation of the goods, wealth and property of individuals in order to entrust them to the hands of groups which, in turn, allow the members of this oligarchy to live a life of maharajas. For this reason, economic inequalities have become permanent.”*

The tenth: erase the human - therefore: dominate through progress, realise the ultimate human.

For Onfray, *“The GAFAM world does not hide its project: to realize the post-human, to overcome man, to end up with this old moon. This also leads to the abolition of civilizations and of the “Divers” dear to Segalen, for the benefit of a united, united, unified world. GAFAM claims an ideology activated by an elite with unlimited money, and therefore absolute power. Every planetary click is a gold coin in their wallet. They attract all kind of scientists and researchers: engineers, IT geeks, biologists, surgeons, cognitive scientists, cyber-activists,, astrophysicists, neurologists, philosophers, sociologists, to create a chimera that unites the biological body and digital flesh.”*

And it is precisely here that Onfray takes the debate far beyond Zuboff: the real para-national danger of the GAFAM, not being controlled by anyone, is to aspire to create a techno-human, asexual and amoral, ideal hybrid society.

Onfray insists precisely on this point because the current phase, the one of brain conditioning through informational intoxication (with its daily-raising extraordinary quantity and its constantly increasingly mediocrity) is already bearing its fruits and that, in the meantime, the *majors* themselves are investing colossal sums in all sciences related to anatomy and nature, having recently succeeded in implanting artificial memories in the brains of rats in laboratories, without any legal obstacle.

Onfray, more than ever, is to be read imperatively. Certainly, his lack of domesticity with languages, therefore his honesty limits the numerous examples chosen to of the country in which he lives, but also to French-translated known and proven facts, mostly American. The ideal companions to this book are hence the more “world-observing” last two volumes, of Slavoj Žižek: as far as the GAFAM are concerned, *“Like a thief in broad daylight. Power in the Era of Post-Humanity”* (London, Penguin, 2019) and for, the tendency to be trans/postsexual: *“Sex and the Failed Absolute”* (London-Oxford, Bloomsbury Academic, 2019). ■



Trends - Cybersecurity Trends

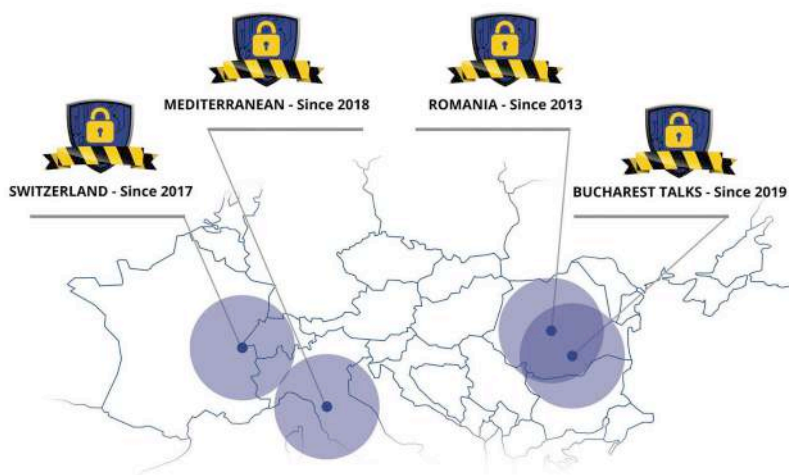


CYBERSECURITY DIALOGUES

www.cybersecurity-dialogues.org

BROUGHT TO YOU BY:

web for your business 
swiss webacademy



www.cybersecurity-dialogues.org

The only platform with it's own quarterly magazine



<https://issuu.com/cybersecuritytrends>



A publication

web for business 
swiss webacademy

edited by:



Copyright:

Copyright © 2020
Swiss WebAcademy and BlockAPT.
All rights reserved.

Redaction:

Laurent Chrzanovski and
Romulus Maier †
(all editions)

For the UK edition:

Raj Meghani

Translation and proofreading:

Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136

ISSN-L 2559 - 6136

Addresses:

Swiss Webacademy - Str. Școala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
14 East Bay Lane,
The Press Centre, Here East,
London. E20 3BS
United Kingdom

www.swissacademy.eu
www.cybersecurity-dialogues.org
www.blockapt.com



**“Mind the Gap:
The Cyber Security Skills Shortage
and Public Policy Interventions”**

A complete study made by GCSEC in collaboration with
Oxford University.
Available free of charge upon registration on: www.gcsec.org



Cyber Security Toolkit for Boards

Cyber security is central to an organisation's health and resilience, which means it's the Board's responsibility.

Managing cyber security is a continuous, iterative process, but broadly speaking there are three overlapping components, summarised below.

For these steps to be effective, you'll also need to get the environment right.

For more information, please visit www.ncsc.gov.uk/collection/board-toolkit



1 Gather information

Get the information you need to make well-informed decisions about the risks you face.

Establish what is important to you.
Find out what your estate looks like.
Identify your vulnerabilities.
Identify what might be of value to an attacker.
Identify who might target you, and how they would do it.

Getting the environment right

Embedding cyber security in your organisation
Cyber security is not just 'good IT' - it must enable an organisation's digital activity to flourish.

Developing a positive cyber security culture
Board members should lead by example to help promote a healthy cyber security culture.

Growing cyber security expertise
As the demand for cyber security professionals grows, you need to plan ahead to ensure your organisation can draw upon the expertise you need.



2 Prioritise your risks

Use this information to understand and prioritise your risks.

Good risk management should go beyond just compliance.

Integrate cyber security into organisational risk management processes.



3 Take steps to manage your risks

Take steps to manage those risks.

Make arrangements with any suppliers, providers or partners to mitigate the risks posed by supply chain attacks.

Implement suitable defences, focused on mitigating your risks.

Have plans in place for when things go wrong.

@ncsc

National Cyber Security Centre

www.ncsc.gov.uk



Stay Safe Online Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.



Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way - perhaps to test their own skills or cause disruption for the sake of it.



Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.



Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.



Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.



Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.

Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.

Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.

Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.



Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password¹), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.



Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.

If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.



Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.