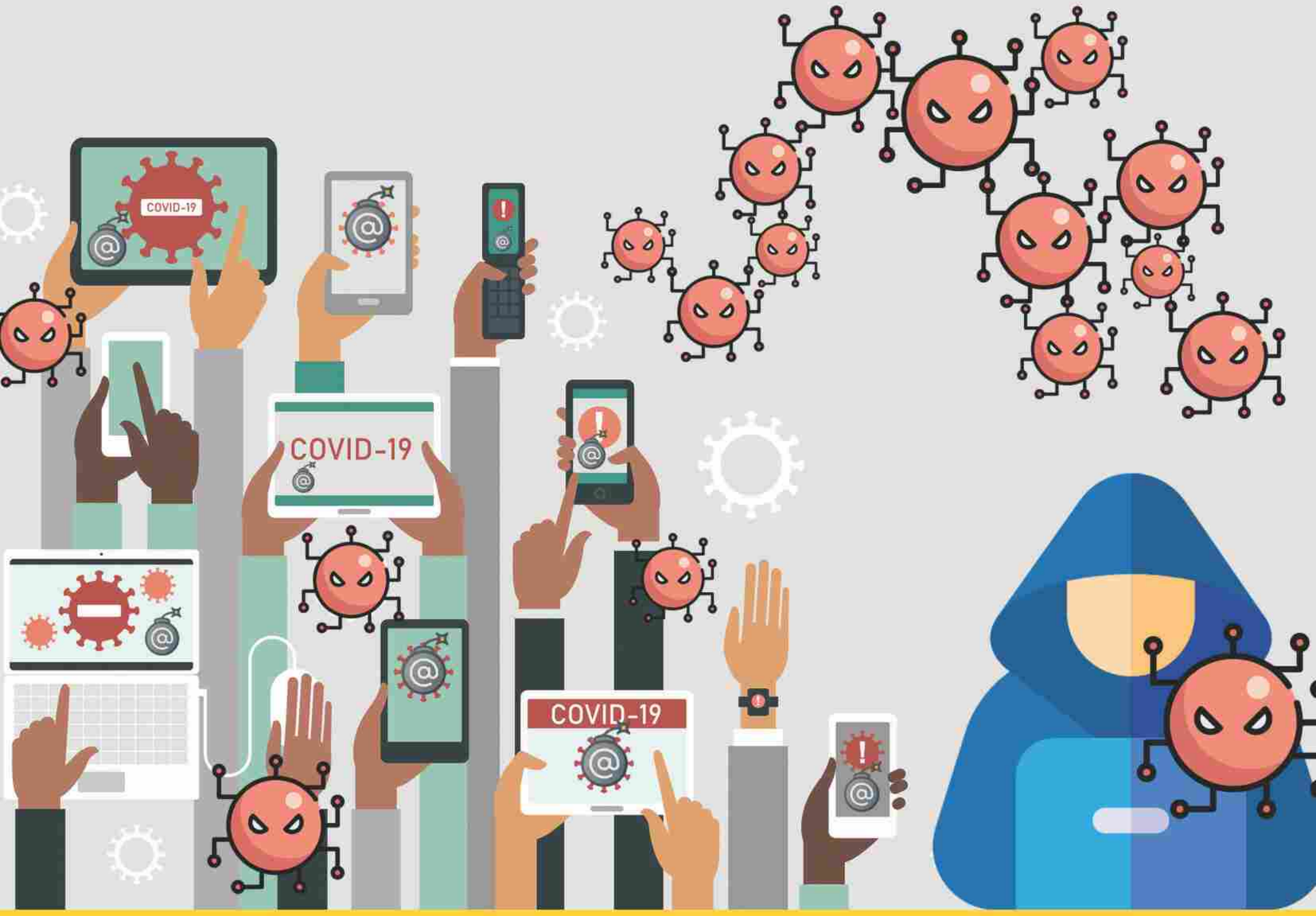
Cybersecurity Trends

Special Edition, April 2020

Ce volume vous est offert par :

MIRAT DI NERIDE
Cyber Sécurité

- **Context and digital consequences**
- **Cyber-defence guide for citizens and businesses**



«Cyber-COVID#19», the hugest wave of cyberattacks in history. PROTECT YOURSELF!

A welcomed publication in the context of an unprecedented wave of cyber attacks

Author: **Patrick Ghion**

As with every European Nation, our country (Switzerland) is coping with a wave of cybercriminal assaults unprecedented in number, scope, diversity and, above all, in the quality of the most dangerous of them.

In addition to phishing and all known forms of digital scams, we observe new generations of *ransomware*, attacks based on new breaches found on the most commonly used systems and software, as well as an impressive number of *zero-days* and accelerated mutations of the known *Advanced Persistent Threats*.

Worse, these attacks now affect not only citizens of all ages and social categories, but also all businesses, from the smallest to the largest, State institutions included. All digital tools used daily, from smartphones to tablets and computers and from servers and to cloud services, are under attack.

For example, one only has to glance at the official statistics of the Confederation to see the scale of the damage: from 14 reports of serious incidents/attacks in the first week of January 2020, the *National Centre for Cybersecurity* recorded more than 170 reports in the first week of April (1), a jump of more than 1700%.

Operational since last year, the Western Switzerland Regional Competence Centre for Fighting Cybercrime is located within the Geneva State Police. The principle stemming from the new Swiss Cyber Protection Strategy is to pool advanced expertise at the inter-cantonal level. This change of paradigm heralds a collaborative era without precedent in the history of Switzerland, where each constituent canton (State) of the Swiss Confederation has its own police and criminal police body with its own cyber unit, which is competent in this area.

In this context, and with the new extra-cantonal responsibilities that now fall to the Geneva Cantonal Police, particular attention is paid to the fundamental importance of public-private partnerships, which we have been multiplying for years with extraordinary results.

As on the whole continent, with our specialized personnel at the front - we are unable to mobilize additional forces to group, concentrate and synthesize the alarms broadcasted to the population and businesses.

In our opinion, this brochure aims to be readable by everyone, as a true digital prevention and defence guide with a clear structure, based on categories of attacks and targets, rendered in a clear synthetic style and doubled by countless online references, is timely.

It is, therefore, our duty and honour to be among the main international partners of this publication, which will be published in three languages.

We would like to thank our long-standing partner, the Swiss Webacademy, organizer of the three international *Cybersecurity Dialogues* congresses as well as the quarterly magazine *Cybersecurity Trends*, for taking this initiative and express our gratitude to all those who have contributed to this special edition, and in particular the journal's Founder and Editor-in-chief, Laurent Chrzanovski, and his team. ■

BIO

Captain Patrick Ghion is Head of the Forensics Section of the Geneva State Police. Patrick has been working for the Geneva State Police for 19 years. Until recently Head of the Computer Crime Unit, Patrick Ghion is now the of the Head of the Forensics Section of Geneva State Criminal Police – constituted by 4 brigades among which the Cybercirme one. Before joining the Law Enforcement Forces, he worked in several Swiss banks and also lived a while as diving instructor in Asia. Father of two kids, his main hobbys are scuba diving and aviation pilot.

(1) www.melani.admin.ch/melani/fr/home/ueber_ncsc/meldeeingang.html

Can we achieve it?

GLOBAL CYBER SECURITY CENTER

Author: **Nicola Sotira**

Today it seems almost "normal" to talk about emergency measures, pandemics, COVID-19; an emergency situation that publicly began to peep out, in Italy, on January 30, when two Chinese tourists were tested positive.

From here the numbers are growing and we will have to get used to seeing everything in a new light. As the MIT report of 17 March also makes very clear, to stop this pandemic we will have to change all our customs, the way we work, exercise, shop, teach, learn, socialize and last but not least, travel.

Could some of these transformations become permanent? Until recently, smart working seemed to belong only to some niches of workers, today it has been adopted on a large scale and to the great satisfaction of companies, especially those operating in the service sector.

We have therefore discovered that it can be done, that our working day can be marked by meetings made thanks to collaborative digital platforms, without affecting the quality of the work to be achieved.

And what will happen to schools, universities? Do we remember the images in the news that offered us overcrowded classrooms and a scarcity of amphitheatres? Almost anachronistic today… and I don't even want to touch the subject of expensive maintenance still to be carried out and/or construction of new learning spaces.

Now, schools have started online sessions and e-learning has been widely adopted. No more crowded classrooms, everyone can follow lessons from home and interact with the teacher via chat or other online means.

The air monitoring stations and the satellites show clearly a huge diminishing of pollution, leading us to reflect on how a different model of economical growth can combine development with environmental sustainability.

Digital is proving to be increasingly relevant and enables us to change the rules of the game, in production, in the life cycle of companies, but also for the management of our leisure in times of imposed reduced real socialization as the current ones.

Not only have we also dematerialized the medical prescriptions, and during this emergency, it is possible to request via email and even via WhatsApp, the delivery of the drugs prescribed by our physician.

We're using Big Data and predictive techniques in the healthcare field, we're talking about using Apps to monitor the spread of the pandemic, we're thinking about enhancing telemedicine implementation and hence, all the endless discussions we had on this topic became real and usable tools in a matter of weeks. In three words: we can do it!

The world has changed many times and this pandemic will change our lives again.

All of us will have to adapt to a new way of living after this experience. But as with all changes, we will have to try hard to keep the positive aspects to make a leap and accelerate a real digital metamorphosis, of course including without any concession all the aspects of security and privacy, the only warrants to have a real improved quality of life.

The best we can hope for is that the depth of this tragedy will not only force all countries to rethink the social issues that have generated inequalities but to implement all useful changes which can continue to be useful beyond this time of emergency. ■

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 alos a member of the Oracle Security Council.

How cybercriminals are exploiting COVID-19, remote working and how to fight back

BLOCKAPT

Author: Marco Essomba

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://www.linkedin.com/in/marcoessomba/
Company website: https://www.blockapt.com

Introduction

Cybercriminals are always on the lookout to exploit well publicised events by using social engineering. The coronavirus (COVID-19) outbreak is a perfect example where cybercriminals are creating sophisticated fraud schemes as a way to trick users into clicking malicious links to download malware by using phishing techniques. Amongst many attack types, phishing continues to pose a significant threat to individuals and organisations of all sizes. They remain a very effective tool used by cybercriminals because it is relatively easy to target millions of users directly via emails, mobile phone text messages and social media using the coronavirus as a call to action.

The coronavirus has forced millions of users to work from home. Many organisations were caught unprepared and had to rush into putting in place remote access solutions that are inadequate and insecure. This poses a significant issue to organisations whereby employees are directly targeted with all sorts of COVID-19 scams with the aim of exploiting remote access software that is vulnerable in gaining unauthorised access to secure systems and sensitive data. More importantly, as more organisations open-up their critical infrastructure to be accessed by their entire remote workforce, cyber attackers will be looking for more ways to break into those systems for malicious gains.

COVID-19 - a sweet spot to attack individuals and SMEs

Cybercriminals will be looking to compromise endpoint devices and steal sensitive information using common attacks techniques such as

phishing, exploiting unpatched software, and using brute force attacks to gain unauthorised access into remote systems. Given the lack of cybersecurity expertise and skills, it is expected SMEs particularly will be caught unprepared. Most will have inadequate solutions to protect their employees against various cyber attacks like phishing. For that reason, the risk to their organisations will be much higher than usual causing significant data theft and could evenly lead to higher costs such as the rise of their cyber insurance.

Boosting cybersecurity to allow remote workforce to continue to work productively from home now becomes even more essential. And given the varied nature of cyber threats that cybercriminals can exploit, it makes sense for organisations to have in place defence-in-depth, by combining device Monitoring, Management, Automation and Response (MMAR) to ensure that threats are discovered & neutralised quickly.

How to fight back and stay safe against COVID-19 related cyber attacks

Given the increase in the number of cyber attacks related to coronavirus employees and organisations will have to step up and become more savvy in defending themselves. Of course, not a single solution can fully protect against the range of cyber attacks that cybercriminals have in their arsenal to maximise their impact. However, enforcing a multi-layer defence strategy is always very effective. This means that deploying various security controls at the network and at the endpoint level is key.

As a first line of defence, enforcing inbound and outbound network traffic security checks is crucial. As a second line of defence, deploying a malware protection at endpoint devices using traditional malware scanning as well as behaviour analysis is a must. That way, even if a system is compromised, the attack can be detected and disrupted before the damage is done. Thirdly, security awareness training plays an important role as part of the overall security strategy of an organisation. By raising awareness, organisations can significantly reduce their risk exposure to phishing attacks. The trade off between security and convenience means that employees will not be able to to consistently detect and avoid targeted and sophisticated phishing attacks, however, training, when combined with a robust overall defence-in-depth security solution, provides the strongest protection to ensure that phishing attacks do not reach employees in the first place.

Moreover, an endpoint protection solution on both the laptop and desktop is key to ensure devices are protected against malware and ransomware. Using multi-factor authentication in all external facing systems is a must. This provides significant resistance against password based attacks which are the most common and also provide a useful deterrent against basic attacks. The following practical tips should be followed whenever working from home:

- Ensure that your laptop or desktop is fitted with the latest antivirus or endpoint protection software
- Be particularly vigilant against phishing attacks related to the coronavirus and remote access software
- Ensure that strong authentication is used when accessing remote access systems and remote video conferences
- Ensure that, where possible, all external facing systems requiring password uses two-factor authentication on top of traditional passwords
- If using an untrusted Internet Service Provider connection such as Internet cafe, use VPNs software to ensure that your Internet traffic is encrypted and protected against eavesdropping.

Conclusion

The coronavirus has forced millions of users to work from home. Cybercriminals are constantly on the lookout for a quick and effective way to compromise systems for malicious gains. Individuals and organisations must step up and become more savvy in defending themselves against various targeted attacks. Regularly patching software, using two-factor authentication, ensuring you have an up to date endpoint protection solution and ongoing security awareness are by far the most effective ways to stay one step ahead of cybercriminals. Finally, defending-in-depth must be part of the overall security arsenal of network and security managers. That is, combining active devices Monitoring, Management, Automation and Response (MMAR) to ensure that threats are discovered & neutralised quickly. ■

For hygiene as necessary in the digital world as it is in the physical world

Author: **Mohamed Saad, President of the Association of Users of Information Systems in Morocco (AUSIM)**

For our first action in partnership with Cybersecurity Trends Magazine, arising from the public-private congresses «Cybersecurity Dialogues», we would have liked to write these few lines by presenting our Association, its achievements, the richness of human exchanges that led to our presence in this volume, among others thanks to our friend and common partner Didier Spella.

BIO

Mohamed Saad is an actor in the world of Information Technologies since 1991. Digital Evangelist; President of AUSIM and Director of the Resources Pole of the Casablanca Stock Exchange, he has operated in the service, industry and banking sectors. In terms of associations, he is a founding member of Isaca-Casablanca, the Moroccan chapter of ISACA, Vice-President of CCAM (Morocco's Club of Business Continuity), member of Project Management Institute. He is a graduate of INSEA and holds an MBA, as well as CISA, PMP, CRISC, ISO 27001 certifications. Mohamed Saad is the author of several articles on IT Governance, IT risks, IT ROI, IT standards and baselines, and many others.

Given the actual circumstances, it is our duty to deal with what is perhaps the most highly mediatized topic since the Second World War, which none of us have lived, of course...

But a war, you say? It is one, as the other would say. This is a health crisis as we never experienced before, and which spreads at the speed of light, confining entire nations, gaining ground and swallowing up billions of dollars in losses... but above all, it is destroying a capital of comfort, pleasure and well-being.

We all have to enable our institutions, first of all, to protect the human being by providing our colleagues with the necessary tools to work at a distance, to stay at home, and to be protected as much as possible from contacts with others.

Secondly, we have to ensure that the activity of the institutions does not stop, through IT tools and other digital devices, to allow the business to survive, as this has an impact on the economy of the entire nation.

Faithful to its actions and good practices, the AUSIM is currently launching Webinars which deal with Business Continuity Plans, including the protection of human health, but also IT security and cybercrime, another scourge which finds a very fertile ground thanks to the proliferation of teleworking.

Digital security will also be addressed as it is a 'relatively new' theme in the way we work, in our culture. It is more urgent today than ever, as the pandemic has opened all doors to cybercriminals, with a global monthly growth of attacks of more than 500% since February, another unprecedented fact. In this context, it is a pleasure for AUSIM to join the collective effort that made this volume possible, published in four languages and intended to provide the greatest number of people with the basic keys of digital understanding, necessary to read and then make good use of the very clear final guide to fight the cyber threats awaiting each of us since the beginning of the pandemic.

Life must go on, firstly by arming ourselves with the health measures necessary to save humanity and, secondly, by creating an atmosphere of mutual aid, firstly between humans but also between institutions.

AUSIM promotes containment as one of the most effective measures to curb this pandemic, as it is the opinion of most experts, researchers and virologists. Thank God, our country took the necessary measures in time to limit and reduce the impact and spread of the virus, but we all, citizens, must show civic-mindedness, responsibility and respect the instructions of the authorities and the control and monitoring institutions.

It is up to each of us, starting from now, to adopt digital hygiene measures to take advantage of this special moment to develop our degree of maturity in cybersecurity, whether it is a matter of our private life, of our professional activities or our public life.

At a time when our thanks go first and foremost to the medical and paramedical personnel and to the agents who watch over the security of citizens, we would like to stress the vital role of all those who work, like the initiators of this magazine, to make tomorrow better.

And it will be better. Inch'Allah. ■

* You can view the entire first Webinar *(AUSIM Webinar: PCA et télétravail pour gérer la crise)* at: http://www.ausimaroc.com/webinar-ausim-pca-et-teletravail-pour-gerer-la-crise/

An unprecedented mobilisation

Cybersecurity Trends

Author: Laurent Chrzanovski, founder and editor-in-chief of Cybersecurity Trends

While preparing, at the end of March, the first of the four 2020 editions of *Cybersecurity Trends Italy**, the idea came to us to share our article and its little cybersecurity guide with many specialists, working in State Institutions, but also private ones, specialized in cyber defence, to collect opinions, advice, data and, *last but not least*, constructive criticism.

All these experts from Romania, Switzerland, France, Morocco, Italy and England, fighting 24/7 on the front line against the pandemic of cyber attacks, a tsunami growing exponentially for more than two months, have been tirelessly helping us, sacrificing in a collective effort of positive disclosure the few free hours they are granted daily.

What followed is in the same logic, but can be seen as one of those little miracles that only the hardest times can bring alive. Observing the lack of communicators to inform the general public more in-depth than through short "alarms" on specific attacks, several Institutions and Professional Associations of the above-mentioned countries asked us to plan, design and publish this present volume, in the languages of the citizens of their respective countries: French, English and Romanian.

Also, on April 6, the directors of all these entities had on their email the formal request necessary to obtain their approval regarding partnerships - and to allow the specialists to write the prefaces and contributions that you can read here. On the same day, the Swiss Embassy in Romania decided to grant its aegis to all three language versions, placed under the High Patronage of His Excellency Arthur Mattli.

Today, 15 April, as we write these lines, all texts have been received and are either in the final stages of translation or already in the process of layout. This unprecedented speed of reaction aligns with the stakes, as the challenge is to save as many jobs as possible through prevention and knowledge, by offering some basic guidelines aimed at protecting companies but also each citizen's private life.

May all partner Institutions and Organizations, all the authors of the texts edited in this volume, as well as the dozens of specialists who assisted us, be thanked here from the deepest part of our heart.

This work is by no means intended to be exhaustive. However, it is intended to provoke as much "food for thought" as possible, thanks to the plurality of points of view that you will discover, but also to motivate further readings through the references leading to in-depth studies available online.

Let's take advantage of this very difficult moment to finally understand digital technology, its indispensable contributions to our daily lives, but also its dangers and the plethora of traps waiting for each of us. Resilience will soon pay off in our fight against the Coronavirus. But a "cyber-resilience", matured by each one of us will pay in the short, medium and long term.

Let's contribute, all together, to stop both the disease and its cohort of digital viruses! ■

**All the volumes, including the newborn n. 1/2020, are available online on the site created ad hoc by the Italian Post Office and GCSEC: www.cybertrends.it/rivista/*

II. How did we get there? On the ground and in our lives.

Forgotten strategic vocabulary

Author: **Olivier Kempf**

The original article, reserved for subscribers, has just been published in the bimonthly LA VIGIE (n. 139, 1st of April 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 in exclusivity this text in the different language editions of Cybersecurity Trends.

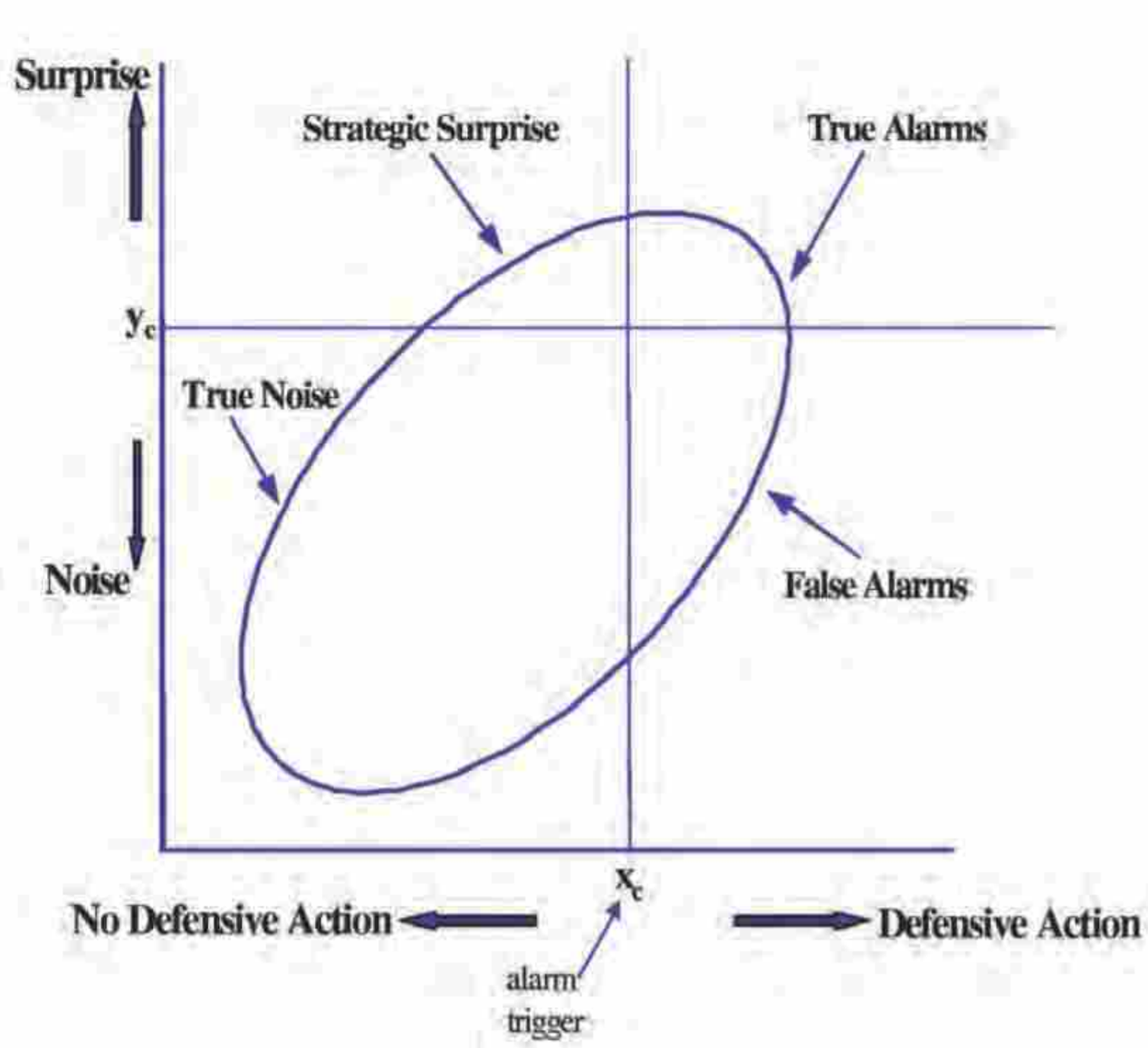
All observers agree: the current pandemic is a breaking point and there will be a before and an after. It is, of course, too early to effectively discern the features of this "after".

However, a few clues are beginning to emerge: let us note with caution that geopolitical affairs are regaining their rights, here and there, with some players taking advantage of the attention mobilized by the victim figures to discreetly relaunch their actions.

We'll come back to that. For now, let us dwell on a large part of the strategic vocabulary that has been forgotten, whether consciously or not, through negligence or change of priorities.

Strategic Surprise

Remember: the term was very much in vogue after the 2001 attacks. At that time, we had all worked on this theme, produced more or less intelligent analyses, and then we moved on to other expressions, adopted, as is often the case, from acronyms invented on the other side of the Atlantic: GWOT, MENA, COIN or A2AD, for example. We promised, we had learned our lesson, we would never be surprised anymore!



The concept of strategic surprise: image © Joseph Lampel, Zur Shapira, Judgmental Errors, Interactive Norms, and the Difficulty of Detecting Strategic Surprises, in Organization Science Vol. 12 No. 5 (2015), fig. 1

In fact, we had anticipated the next strategic surprise by investing heavily in cyber defence. Of course, the Crimea affair in 2013 had alarmed us a little, but tactically one could say: we had then forged the (unconvincing) concept of hybridity.

But we were staying within an agreed framework and brilliant strategists were talking about issues of multi-domain operations.

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.

Without any doubt, these questions are important (insertion of space in strategy, technological developments, collaborative combat) and it is not a question of forgetting them: but they belong to military-strategic theory and not grand strategy.

Yet a concept is relevant if it fits both military strategy (at the strategic, operational or tactical levels) and grand strategy.

The concept of surprise undoubtedly belongs to this category. It should, therefore, be the obsession of the strategist. In this respect, we have to acknowledge that we have failed.

Yet the likelihood of a pandemic was well known. So here comes a new case, a surprise that is not so much a surprise but that, nevertheless… surprised. The 2000s had seen some examples: the SARS above all, but also the H1N1. It was precisely the succession of these two crises that caused the unpreparedness that we are observing.

SARS, in 2003 was a surprise that sparked a great deal of mobilization. The response to H1N1 in 2009 was strong, but the outbreak was less virulent than feared.

A debate ensued about the waste and disproportion of the reaction: this debate should not have taken place because the authorities had reacted in a context of uncertainty and were unaware of the virulence of the threat. Blaming them after the fact for overspending was a non-strategic reaction, worthy of post-match soccer commentators.

The fact remains that we let things go for a decade, which led us to the current situation: as a result, this pandemic appears as a strategic surprise.

It is strategic in terms of its consequences because the other feature of the strategic surprise is not only that it is surprising, but that it is strategic because of its consequences ...

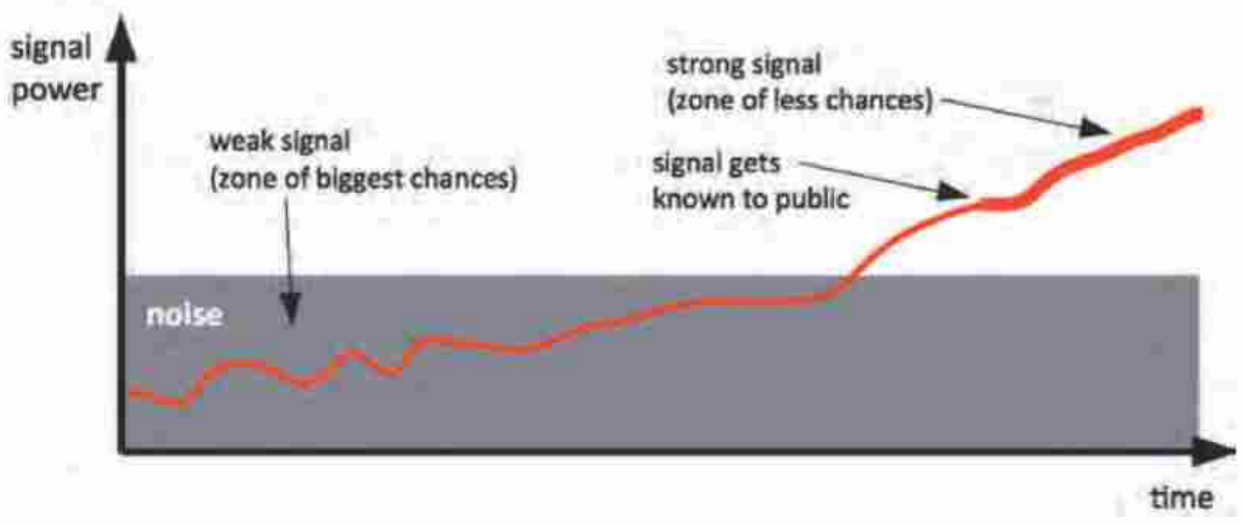
Weak signals

Another term inherited from September 11 is the notion of weak signals. It is not a question of going back on the words of Rumsfeld who, in his time, evoked "unknown unknowns", or even of going back on listening to the intelligence services: information is only worthy in function of the decision-makers ability to listen to it.

But in this case, let us note that the signals were not weak, but strong. Here we recall the criteria outlined in the Pandemic Influenza Response Plan, set out by the SGDSN *(Secrétariat général de la Défense et de la Sécurité nationale)* in 2009: *"The warning signs that may justify the use of this fact sheet are as follows: sudden reporting by concordant sources somewhere in the world of a widespread extending of a disease with a large number of cases of influenza-like illness (more than 100), with suspicion of rapid spread (high contagiousness), with abnormally high mortality and/or clinical or biological severity requiring hospitalization significantly more frequently than for seasonal influenza".*

It was not a question of being a great clerk: as early as February 5, La Vigie reported the virus, more than a month before the government's first measures.

Conclusion: if not only the strong signals are not heard, how much less will the weak ones be: basically, they do not exist.



On the necessity to understand weak signals before loosing the opportunity to counter in time a phenomenon © Robert Eckhoff, Mark Markus, Markus Lassnig, and Sandra Schön, No Outstanding Surprises when Using Social Media as Source for Weak Signals? First Attempt to Discuss the Impact of Social Media Sources to Detect Surprising Weak Signals. In: Proceedings of The Ninth International Conference on Digital Society (ICDS) in Lisbon, Portugal, 2015, fig 1

Strategy of Means

We have discussed the issue of aligning means with ends and paths to follow: it is customary to refer to the strategy of means to designate how to mobilize the industrial apparatus to acquire the resources that armies need.

However, what this crisis teaches us is that a civil strategy also requires a strategy of means.

The analogy is valid in all dimensions: it is necessary to have stocks, here of ammunition and fuel, medical masks, respirators and tests; but it is also necessary to have an industrial strategy to allow manufacturing sovereignty: defence industry in one case, chemical or health industry in the other.

Let us point out here how much the notion of "industrial policy" has been devalued in recent decades: the economic policy of trust in globalization has made those who were moved by it look like sad and retarded minds.

The notion of economic intelligence had regained some favour in the last two or three years, thanks to Donald Trump's radical decisions. There is no doubt that tomorrow the notion of strategic industry will be in vogue.

Defence and innovation

Of course, there's no war against the virus. The formula may pass for a metaphor, but it is hardly acceptable when it comes to using war vocabulary to promote a national mobilization that has not been especially encouraged before.

Incidentally, the calls for "the army", formulated here and there, show to what extent the common imagination has no idea of the residual weakness of military means, the effect of three decades of optimization, as they used to say. The staging of the call for armies worries more than it reassures.

However, there is no doubt that there is a front, that of the hospitals. Let us observe, moreover, the capacity for innovation, with the few available means, the fitting out of emergency intensive care rooms, the manufacture of masks or equipment, the use of emergency medication: one would think, all things being equal, that we are facing the formidable inventiveness of the armies (and of their Health Service) during the First World War.

Snorkeling masks used in French, Belgian and Canadian hospitals © radiocanada

Defence (stopping, braking, control, we used to say) also requires adaptations in the long run.

Freedom of movement

Who doesn't know the three principles of strategy, dear to Foch? One of them is freedom of movement.

With containment, the population is deprived of this freedom of movement: but it is to hinder the freedom of movement of the virus (we could speak of freedom of contagion).

It is curious and paradoxical that our only defensive strategy is to stand still to slow the spread. But the logic is respected: this pandemic has a global dimension due to the exacerbation of the flows caused by globalization. Logically, stopping the flows will make it possible to curb the virus.

Resilience

Resilience: another word that has been very much in vogue, imported by strategists from the psychological world. But while the term originally refers to an individual's ability to overcome hardships, strategists have applied it to collective groups.

We shall note that they were not talking about nations but about "resilient people". The idea was to explain how they would be able to overcome terrorist attacks since it was understood that those wanted to instil fear, change collective opinions and thus achieve new policies.

Curiously enough, this virus (which of course we won't name an enemy) didn't scare anyone at first. On the contrary, it was reduced to a *"grippette"* (small flu), which was not going to prevent us from going to the theatre, as we were advised by the highest authorities.

And then things got worse, and we heard of war and, immediately afterwards, of resilience. For if the French population seems to be less moved than during the 2015 attacks, we can see that it is more deeply affected by the pandemic: in addition to containment, the human toll is already (in France) counted in thousands of deaths.

Certainly, seasonal flu, suicide or alcohol cause many deaths. A cynic would find that, in the end, it would not affect the balance of the country that much, so resilience is assured.

That is not seeing the economic damage that will result in the end. From this point of view, it is much less certain that we can talk about resilience.

The recovery will certainly take much longer.

It is not the *Operation Resilience* (mobilization of military resources against the C-19 in France) which will be enough to cope with it. ■

French soldiers mobilized in the frame of the Opération Résilience © Europe1

This special issue is placed under the aegis of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

It has been realised in partnership with:

Gendarmerie nationale
Une force humaine

Centre de recherche de l'EOGN

POLICE GENÈVE

ROMANIA
CENTRUL NATIONAL CYBERINT
SERVICIUL ROMAN DE INFORMATII

DIRECȚIA DE COMBATERE A CRIMINALITĂȚII ORGANIZATE
I.G.P.R.

CERT-RO

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

GLOBAL CYBER SECURITY CENTER

AUSIM
beyond digital

FIC

CHARENTE-MARITIME CYBER SÉCURITÉ

CYBERSECURITY PUBLIC - PRIVATE DIALOGUES

swiss-cybersecurity.ch

and with the support of:

BLOCKAPT

STANCHION

COVID#19 or when digital security would have much to teach governments about crisis management

Author: **Laurent Chrzanovski**

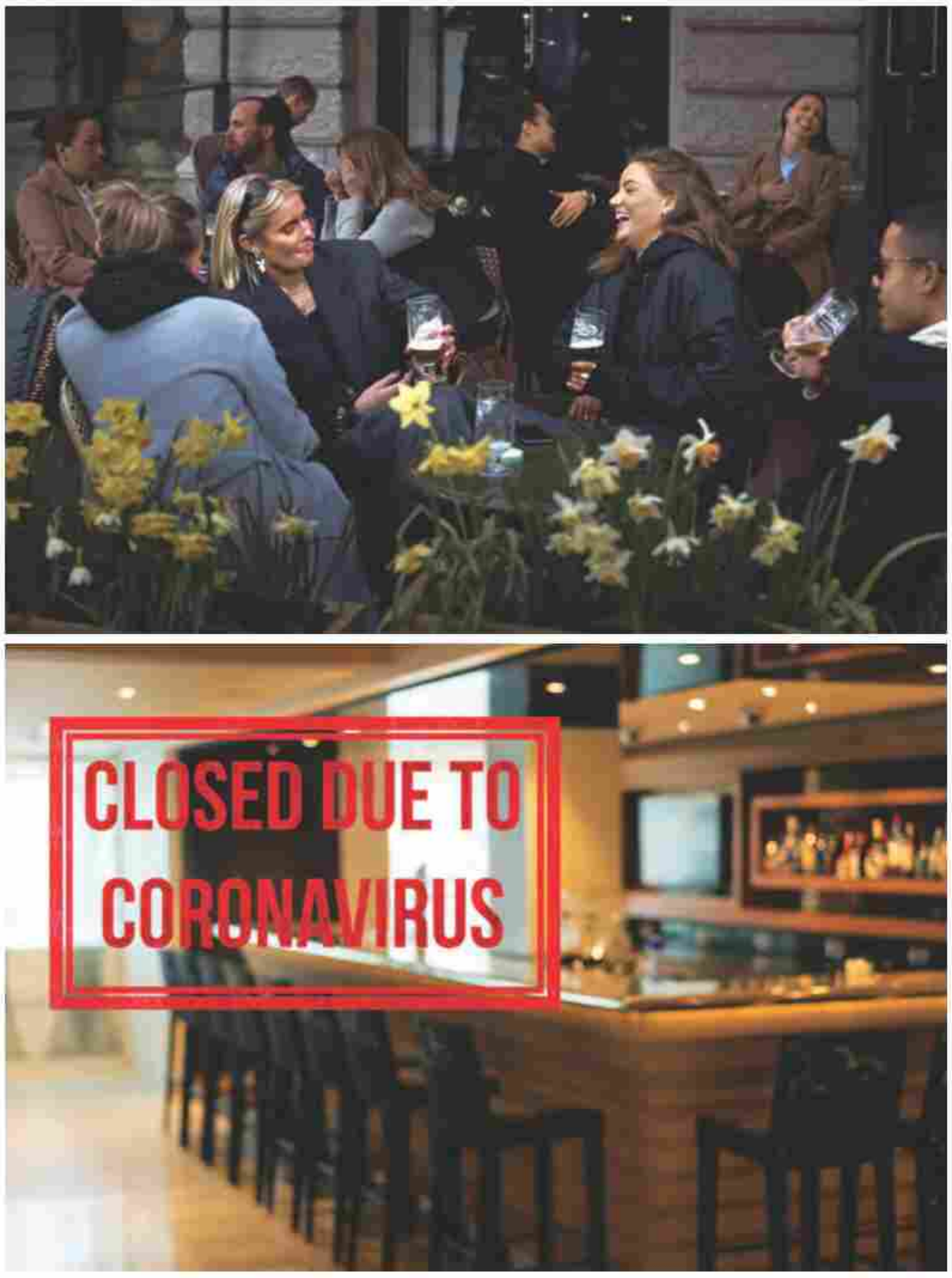
On the ground: the politics of chaos and the "every man for himself" ideology.

The European management of COVID#19 (Coronavirus) is catastrophic: national emergency plans with successive increasingly restrictive measures, like the closure of borders and the isolation of individuals. Such measures bring populations in a state of siege and, sometimes, panic.

All this is magnified by a political cynicism where the emergency translates into a threefold challenge: to effectively combat the expansion of the virus, to make the economy work best, and not lose their share of electoral popularity.

In the «think tanks» of European leaders, where everybody has clear and precise needs, these three fronts are completely conflicting. The result is palpable, we live in a state of chaos where every country applies different emergency laws, health measures and treatments. The current situation was resumed pretty well in the description made by Giorgio Agamben: «*Never before have we witnessed the spectacle, typical of religions in times of crisis, of different and contradictory opinions and prescriptions, ranging from the minority heretical position (also represented by prestigious scientists) of those who deny the seriousness of the phenomenon to the dominant orthodox discourse that affirms it and, however, often radically diverges as to how to deal with it. And, as always in these cases, some experts or self-styled experts manage to secure the monarch's favour, who, as in the times of religious disputes that divided Christianity, takes a party according to his own interests for one current or another and imposes his measures*" (1).

The policy of chaos: Korczowa - Krakovets, border point between Poland and Ukraine, 28 March 2020. In the midst of the COVID#19 crisis, tens of thousands of Ukrainian citizens flock to return to their country before the borders are closed. © Novynarnia.



Un bar in Stockholm and a second, in Chicago, 10th of April. © Getty

BIO

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski 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 books, of more than 150 scientific articles and of as many general-public articles.
In the frame of cybersecurity, Laurent Chrzanovski 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 cyber security 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.

The population is left at the mercy of an explosion of alarmist information and, even worst, of misinformation created by fake news. The state of confusion and general abandonment can be resumed in Noam Chomsky's motto: *"The general population doesn't know what's happening and it doesn't even know that it doesn't know".*

European and international collaboration, the only one that could best face the epidemic, is almost non-existent, as Yuval Noah Harari masterfully pointed out: *"I think the worst thing is the disunity we see in the world, the lack of cooperation, of coordination between different countries. And the lack of trust, both between states and between populations and governments. (...) So what really frightens me is the lack of leadership and cooperation. And what people should realize is that the spread of the epidemic in every single country threatens the whole world, because if it is not contained in time, the virus will evolve. This is perhaps one of the worst scenarios with this type of epidemic: a rapid evolution of the virus."* (2).

Worse still, in countries with closed borders, where one of the public health measures is a full quarantine, we are witnessing a real coup dictated by the inability to identify and isolate outbreaks of the virus on the territory due to a lack of sufficient testing. This induces a psychosis where the relative, the neighbor, the friend, all become suspected cases and a border must be created towards

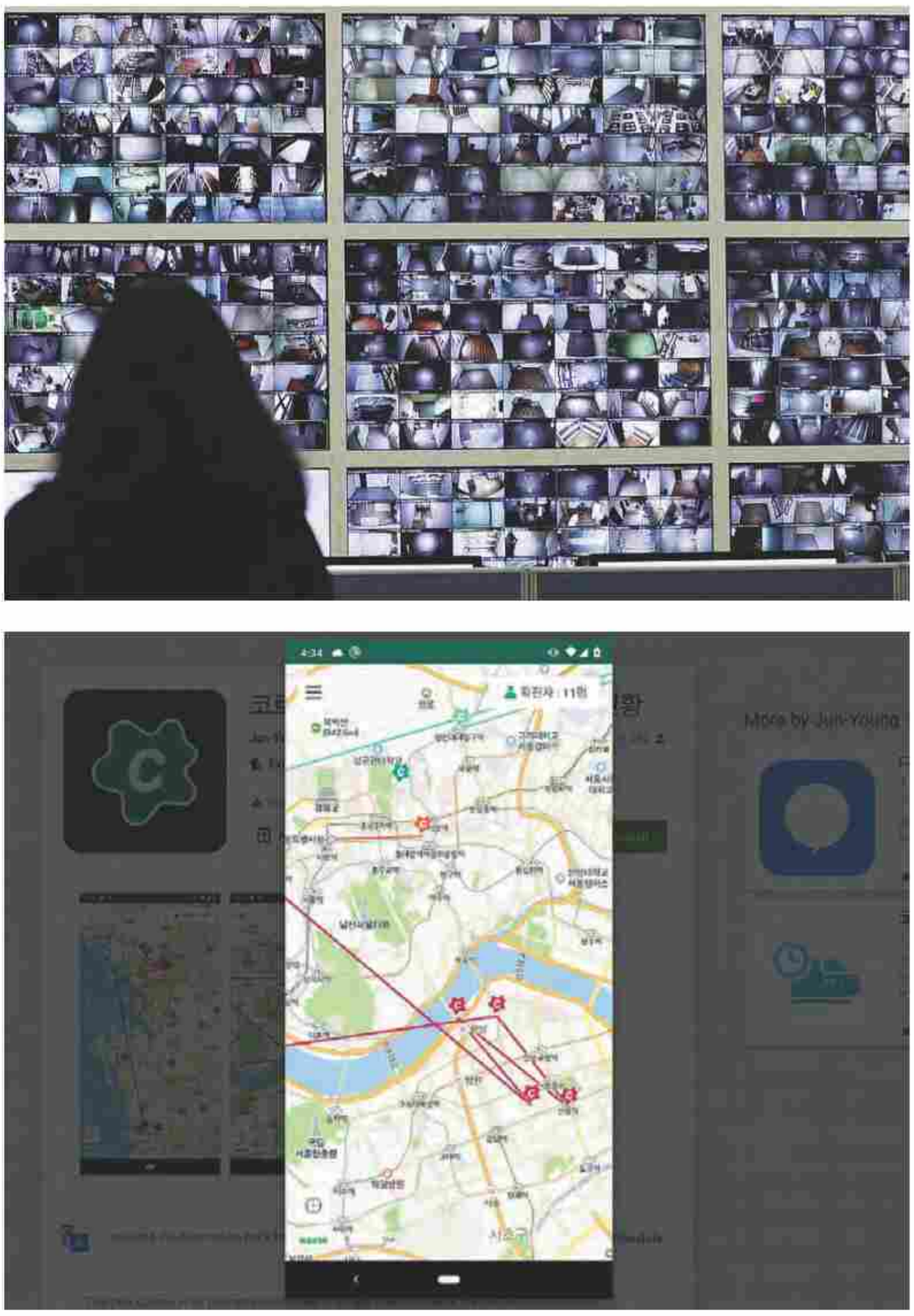
them. Michel Onfray explains well the danger of this isolation: *"But what is this confinement if not an invitation to create as many borders as the French? The national border is not a good border, but the border that separates one person from another is presented as the solution, the only solution, we are told. (...) Maastricht coughs, spits and threatens embolism."* (3)

Democracies faced with the temptation of mass surveillance

Not a few of these measures make us reflect on our future, first and foremost the digital future. Indeed, the number of the governments that are now using our own "tools" to control our location is increasing. Slavoj Žižek has anticipated the risk that such control measures could be adopted also by the democracies: *"The epidemic caused by the coronavirus serves to justify and legitimize measures to control and regulate populations hitherto unthinkable in a Western democratic society - isn't Italy's total confinement a totalitarian fantasy? Not surprisingly, China (which already made massive use of new technologies for social control purposes) is proving to be the best equipped to deal with a catastrophic epidemic - at least judging by what appears to be the current situation. Does this mean that China embodies our future, at least in some respects?"*(4).

Yuval Noah Harari, in his last essay, goes much further, arguing that the possibility that surveillance linked to the Coronavirus, established in some democracies, could then become a daily instrument. Thus he states: *"To stop the epidemic, entire populations must respect certain guidelines. There are two main ways to achieve this. (...) Today, for the first time in human history, technology makes it possible to monitor everyone continuously. Fifty years ago the KGB could not follow 240 million Soviet citizens 24 hours a day, nor could it hope to effectively process all the information collected. The KGB relied on human agents and analysts and just could not place a human agent to follow every citizen. But now governments can rely on ubiquitous sensors and powerful algorithms instead of flesh-and-blood spectres. (...)*

Many short-term emergency measures will become a regular occurrence. This is the nature of emergencies. They cause historical processes to advance rapidly. Decisions that in normal times may require years of deliberation are made within a few hours. Immature and even dangerous technologies are put into service, because the risks of doing nothing are greater. Large-scale social experiments demonstrate their usefulness for entire countries. What happens when everyone works from home and only communicates from a distance? What happens when entire schools and universities operate online? In normal times, governments, companies and school boards would never agree to conduct such experiments. But these are not normal times. In this time of crisis, we have two particularly important choices ahead of us. The first is between totalitarian surveillance and citizen accountability. The second is between nationalist isolation and global solidarity." (5)



Real-time monitoring, South Korea © The Conversation
South Korean government apps showing routes and places where infected people are located © Businessinsider

Cybersecurity: a global field with actors in permanent dialogue

And this is where we begin to shift towards cybersecurity and its coordination, exemplary when compared to many governmental choices.

The reason is simple: in addition to the economic damage purely related to the virus - which various sources already point out as the symptoms of a recession worse than the crisis of 2007, we must understand the additional damage brought by cybercrime.

To give a metaphorical dimension to what is happening in the digital world, if, at the time of writing, COVID#19 was a single multimedia virus, the

number of its victims (asymptomatic, symptomatic, curable or not) would have at least four zeros more than that of the people who contracted the disease. Worse, the spread of multimedia viruses, not attacking a single system (like the human respiratory system in the case of the real virus), is as if every single internal and external part of our body was at risk.

This global mobilization of all sectors, in true public-private partnership, which was the - very optimistic - goal set for 2020 by Microsoft in a 2012 report, is taking shape right before our very eyes.

The birth of this mobilization is not purely economic: even if the virus had been contained in the megalopolis of Wuhan, any major event that would have happened in China, as in the United States, would have had a global economic, political and... cyber impact. The mobilization of the digital security experts started already in early February, at the beginning of the epidemic.

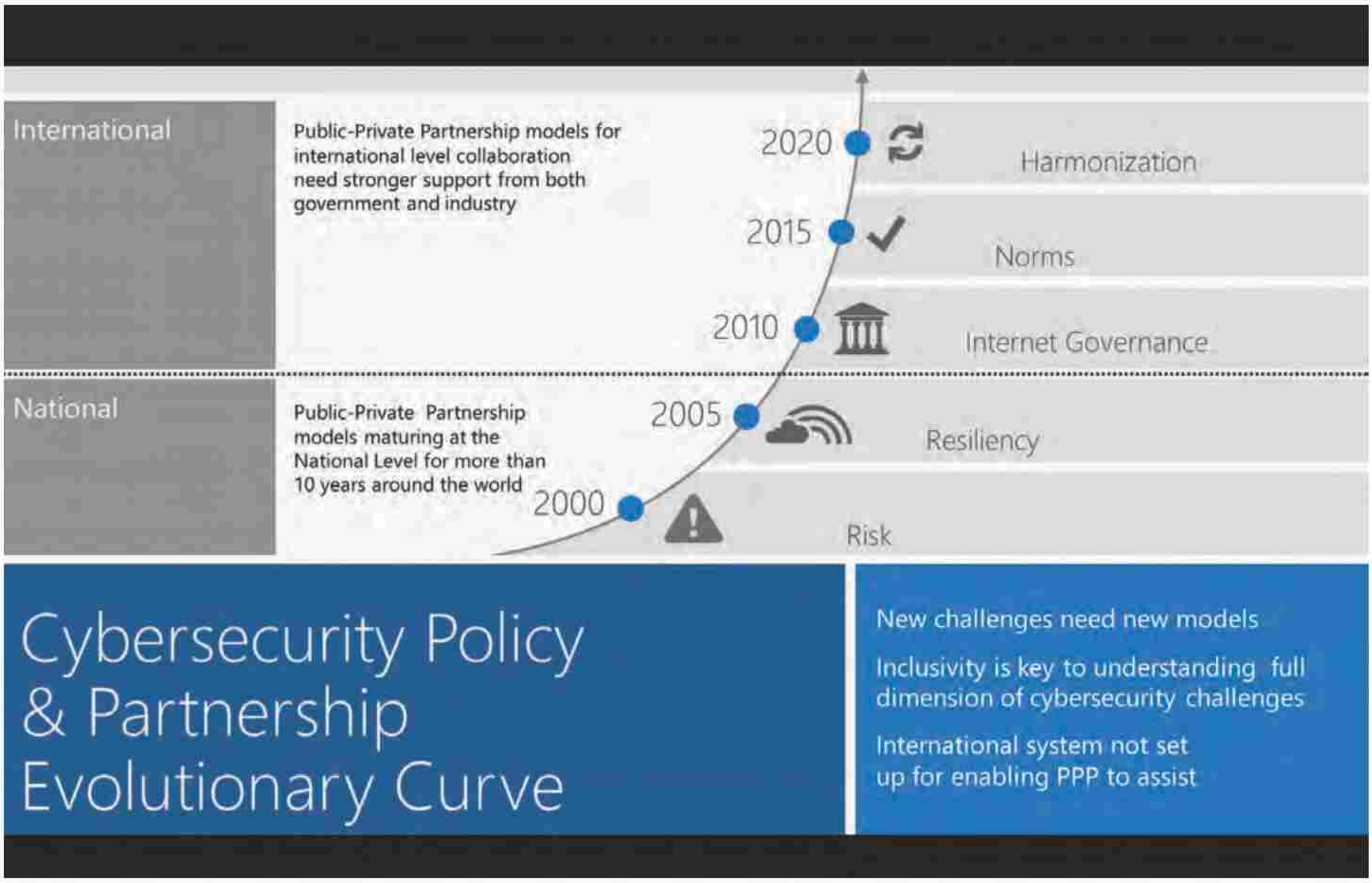
Sure enough, beside the spread of pandemic, the worst of the scenarios is taking shape, the exploitation of a catastrophe by cyber-criminal groups. The cybercrime is promptly adapting: full-scale attacks, multiple strategies, by all means, in all languages, to try to hit all possible types of users and tools (hard, soft, cloud). [For technical data, see the very detailed report of the Insikt Group, *"Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide"* (6)].

Such operations had already been carried out, but with less success, precisely because there had been no governmental reactions so incoherent at a global level, during the first peak of the Ebola epidemic (2002-2003), as perfectly explained by François Mouton and Arno de Coning in the introduction of their very recent study on what is happening in the virtual world (7).

The difference from epidemic management: true international or even global PPPs

When it comes to coping with a series of attacks, trying to creep into all private and professional activities, the big difference between the management of the *human viral pandemic* and the cyber viral pandemic is that in the latter, the political factor is absent. It is the specialised agencies of the various states that are responsible for limiting the damage to citizens, businesses and, *last but not least,* to the digital tools of their own state. The coherence, the accuracy, the very high qualification and the constant trans-professional interaction of those who deal, all over the world, with the current digital urgency are, in comparison, the antipodes of what we see on the physical-human front.

As always, countries that are at the forefront in the timely publication not only of new vulnerabilities of hard- and softwares (as well as patches released by the respective manufacturers), but also in the description,



The evolution forecasted by Matt Thomlinson in Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace
© Microsoft, 05.10.2012

The situation - Cybersecurity Trends

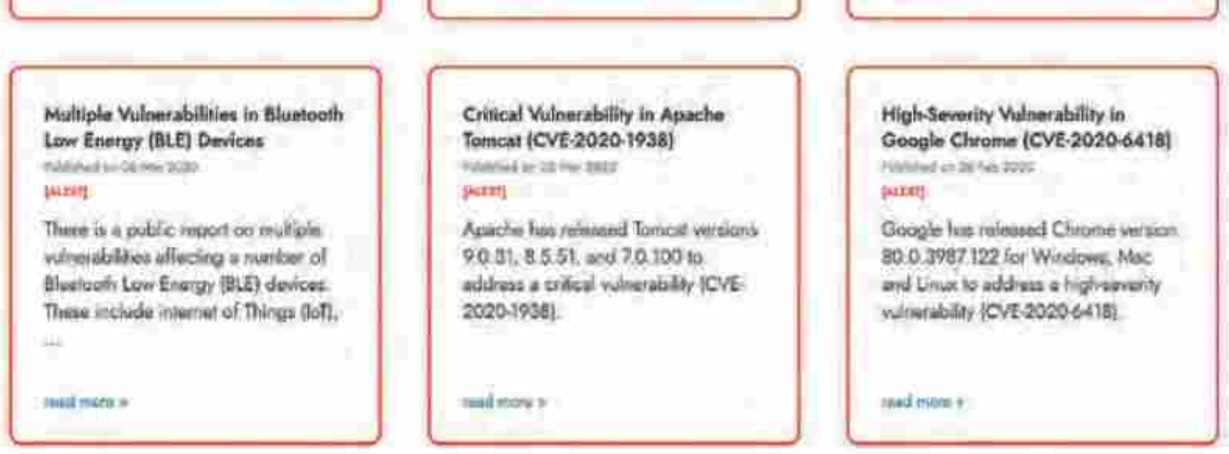
first generalist and sooner technical of the various ransomware, viruses and zero-days, are the ones that stand out. In our opinion **Singapore** has the most dynamic CERT in the world in terms of concentration, sorting and circulation of information (8).

It should be noted that SingCert is not only part of the cyber service of the State Intelligence, but it has a record number of collaborations with third countries and private companies, from majors to medium-sized ones.

Moreover, the effectiveness of the small Asian state amazes the world on the health front. Based on the experience of the management of SARS, we remember that Singapore is, before Taïwan and Hong Kong, the country which has managed the crisis in the best way possible and has also managed to contain the human virus, without any confinement of the population and with open schools and businesses (9).

On the other side of the globe, the United States of America has multiplied its efforts and managed to make a quantum leap that scarce European countries have reached: avoiding countless searches and consultations of public and private websites, the NGO **Staysafeonline** has been offering for a few days a very useful and constantly updated "COVID-19 Security Resource Library" (10), with three sections: state reports, company reports and field articles. The short press releases, instead, are in the special *newsfeed* dedicated to each of the four main targets: children, adults, professionals, companies.

The explanation is simple: Staysafeonline is an emanation of the **National Cybersecurity Alliance**, a very powerful working group that includes the Department of Homeland Security and almost all the majors companies, white hats and universities. It is to be considered as the most effective PPP ecosystem in the world at the moment, with the exception of cyber



The "news" page of the Singcert and a kindergarten in Singapore, 24 March © Axios

SingCERT
Singapore Computer Emergency Response Team

The COVID-19 Security Resource Library page © Staysafeonline

partnerships dedicated to specific sectors (critical infrastructures, industries or particular fields such as banking and healthcare).

Just one example to illustrate the front erected to counter the mass of attacks

To cope with the total siege of all connected objects and their users, all over the world, the most impressive response arrived on Wednesday, March 25th. The founder of the famous Def Con congress, created the **COVID-19 Cyber Threat Intelligence (CTI) League**, already reached by 400 top experts from more than 40 countries, chosen on a co-optation and totally voluntary basis.

The CTI League has already signed protocols of mutual collaboration with numerous states, primarily Canada, or directly with their Cyber Intelligence agencies. Leaving aside malware and sophisticated zero days, which are now monitored and isolated by the group in a timely manner, Rogers motivated the founding of this elite group by noting that *"I've never seen this volume of phishing. I am literally seeing phishing messages in every language known to man."* Thanks to his idea of co-opting the best, from white hats to senior cybersecurity officers of large multinationals as well as specialists of security companies, after only a few days, we assisted at an unprecedented openness from state agencies. Roger, satisfied with the collaboration reached between agencies and companies, wraps it up by saying: *"I have never seen this level of cooperation, I hope it continues afterwards, because it's a beautiful thing to see."* (11). The results of the League, which does not want advertising, will undoubtedly have quick and fruitful effects, without the user realizing it.

The private sector at work 24/7

In addition to the collective efforts mentioned, there are also the specialized companies, which offer new detailed reports every day, drawn up by their teams, which are active on all continents. It is not necessary to make a list here, it could not be exhaustive, because the best way to know them is to access the informative materials available to everyone. Also, to stay updated, one can read the daily articles in papers and specialized online magazines, such as the excellent texts by Montalbano (12), Pilkey (13), Lakshmaman (14) or, in Italian, the excellent text by Salvatore Lombardo (15) with useful tips and links. ■

Notes :

(1) Giorgio Agamben, Riflessioni sulla peste, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste) (quote : author's translation)

(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

(3) Michel Onfray, Berezina, in Les Observateurs, 17.03.2020 (https://lesobservateurs.ch/2020/03/17/michel-onfray-berezina/) (quote : author's translation)

(4) Slavoj Žižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plaît ! in Le Nouvel Observateur, 18.03.2020 (quote : author's translation) (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)

(5) Yuval Noah Harari, Il mondo, dopo il Coronavirus, in Ottimisti e Razionali, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/) (quote : author's translation)

(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

(8) https://www.csa.gov.sg/singcert

(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html

(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/

(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049

(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

(14) Ravie Lakshmanan: Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

(15) Salvatore Lombardo: L'allarme: Coronavirus, in aumento attacchi cyber, phishing e malspam: consigli per difendersi, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

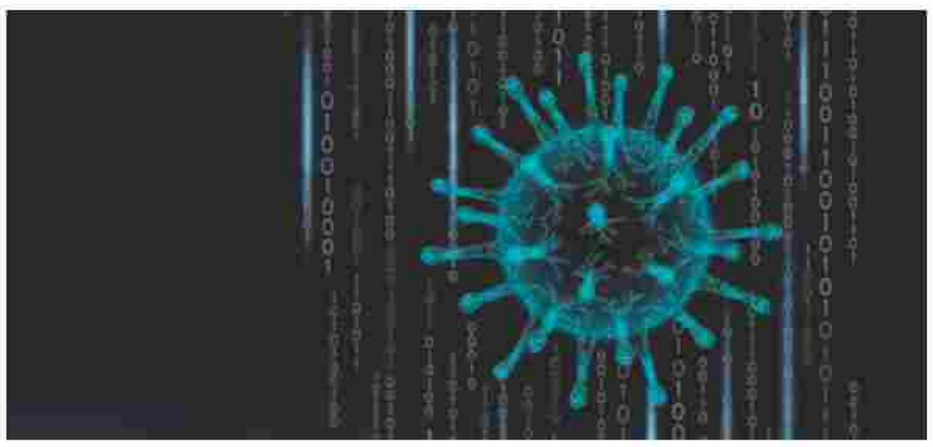
III. The digital impact of the COVID#19: a tsunami of attacks. Explanations.

COVID-19 and Cybersecurity

Author: Marc-André Ryter

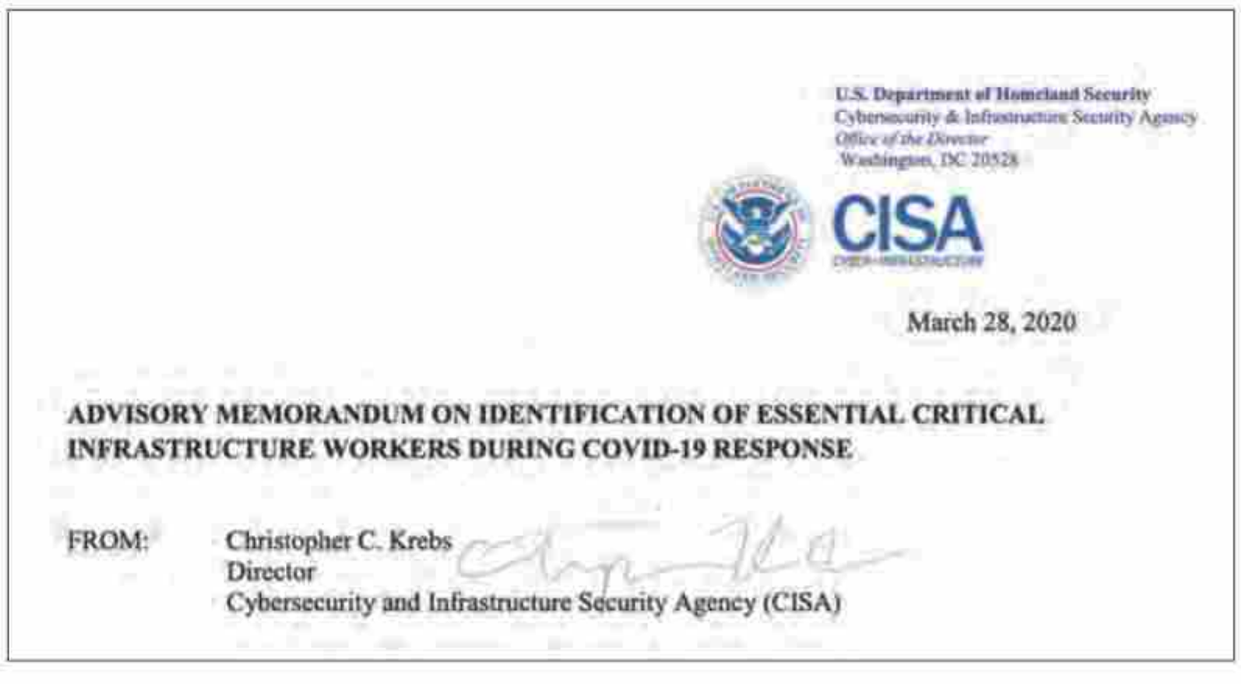
The situation created by COVID-19 will provide lessons in a wide range of areas, from hospital treatment to crisis management to the minimum autonomous production capacities required in each country. One can hope that these lessons will lead to the implementation of concrete measures.

Indeed, it is legitimate to ask how governments could have been so surprised when, for almost two decades, pandemics have been occurring regularly, with a significant impact on populations. We refer here in particular to the SARS epidemic in 2002-2003, followed by the H1N1 swine flu epidemic in 2009-2011 and then by Ebola in 2014. And these are not the only ones.



What interests us here are the similarities and links between this crisis and cybersecurity. First, there is the unstable and risk-generating environment. In such an environment, complexity, increased need for security, control of information, control of products and behaviours, and security of data processing are parameters that must be managed. Both in cyberspace and in the ongoing crisis, flexible, fast, coordinated and effective solutions must be found. The current health crisis is facing the same challenges as in cyberspace: global competition, the need for rapid innovation and the need to integrate the public and private sectors.

The links between the two areas are reflected in the risks that threaten them. First of all, the fragility of the networks and their reliability. These are strained by dependence on numerous external partners. The risk of conduct being disrupted by failing systems is as high in the health sector as in other areas of public life. Malicious actors in cyberspace can take advantage of new and temporary vulnerabilities very quickly.



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

CISA

March 28, 2020

ADVISORY MEMORANDUM ON IDENTIFICATION OF ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS DURING COVID-19 RESPONSE

FROM: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

In this period, new advises and recommendations on cyber-prevention are almost daily posted on the website of the Department of Homeland Security (USA), in particular on its specific website of the Cybersecurity and Infrastructure Security Agency (CISA - www.cisa.gov). Here, the header of the last memorandum, dated March 28th and signed vy the Agency's Director.

Attacks redouble and are specifically developed based on the fears of the population. Manipulations and fake news are multiplying, as are frauds of all kinds. This misinformation can have a significant impact on society and people's behaviour, and thus on critical infrastructures.

The slow reaction only makes the situation worse. Interpretation of weak and strong signals often remains incomplete, slowing the transition from analysis of information to action. This response is made difficult by the

BIO

Expert in security policy, Colonel Marc-André works for the Swiss Army General Staff. He holds a BA in Political Sciences and an MA earned at the NATO Defence College in Rome. He follows and studies the technological evolutions potentially relevant for the Armed Forces, in order to deduce the necessary consequences on the miltary doctrine

The impact - Cybersecurity Trends

economy's just-in-time production system. Firms and public institutions are left with only what they need immediately, both quantitatively and qualitatively. There are no longer any stocks or reserves. The resilience of economic and health systems must, therefore, be improved. The current situation shows the extent of our dependencies, particularly concerning information sources and data exchange channels. There is a significant gap between reality and public perception.

Telework is an important measure taken by governments to deal with the spread of COVID-19. It shows us how dependent we are on networks, their data transmission capabilities and thus their proper functioning. As a result of telework, data exchanges have increased exponentially, and with it the vulnerabilities associated with them.

Crises such as the one we are experiencing open many new loopholes for cybercriminals. The amount of goods bought over the internet is exploding. Many players are looking for digital solutions to their new problems of selling goods or movements. Cybercriminals are taking advantage of this state of weakness and the fears of the population. On the one hand, they multiply known attacks, often in the form of seemingly official e-mails that are supposed to reassure. On the other hand, cybercriminals organise massive frauds of all kinds, mainly concerning the sale of, particularly sought-after goods.

Data protection is essential. During crises, data collection increases, both by individuals and by authorities. Control and protection must be ensured, as well as use and possibly also deletion when the data are no longer useful. Already existing threats, such as classic ransom-type attacks, can have dramatic consequences when they block, for example, the functioning of a hospital.

Following the example of the COVID-19 crisis, it is imperative to understand why security in cyberspace

Country or State	Traffic Change	DL Speed Change
France	↑ 38.4%	↓ 13.9%
Italy	↑ 109.3%	↓ 35.4%
Japan	↑ 31.5%	↑ 9.7%
Spain	↑ 39.4%	↓ 8%
United Kingdom	↑ 78.6%	↓ 30.3%
USA - California	↑ 46.5%	↑ 1.2%
USA - Michigan	↑ 37.9%	↓ 16.1%
USA - New York & New Jersey	↑ 44.6%	↓ 5.5%

Increase of the internet traffic in March 2020 and network speed reduction © Fastly https://www.fastly.com/blog/how-covid-19-is-affecting-internet-performance

is an absolute necessity. It is the only way to protect oneself against the actions of cybercriminals and, above all, to ensure the proper functioning of networks and the availability of essential information. Crisis management and control must be based on a secure cyberspace. The aim is to avoid negative long-term consequences by developing cooperation between all the players to ensure the coherence and similarity of the measures taken.

This need for security, for a better cooperation between actors as well as the duty to share and promote a defensive knowledge base to the largest public possible, this is exactly the aim of the present volume, vital during this particular moment.

Thanks to the quality and diversity of the contributions collected, we are convinced that this special issue of Cybersecurity Trends will remain a valuable basis for thoughts even when the crisis will be over. ■

Stanchion Payment Solutions

Global Payment Specialists

Our experience in complex payments environments and our international perspective of client engagements enable us to offer a range of solutions, services and products to integrate, improve, optimise and secure your payments systems.

Please contact us at *engage@stanchionpayments.com* for further details on our security and payment health-check services.

Visit our website: *stanchionpayments.com/insights/brochures/* to download free brochures on security and securing your payments systems.

STANCHION

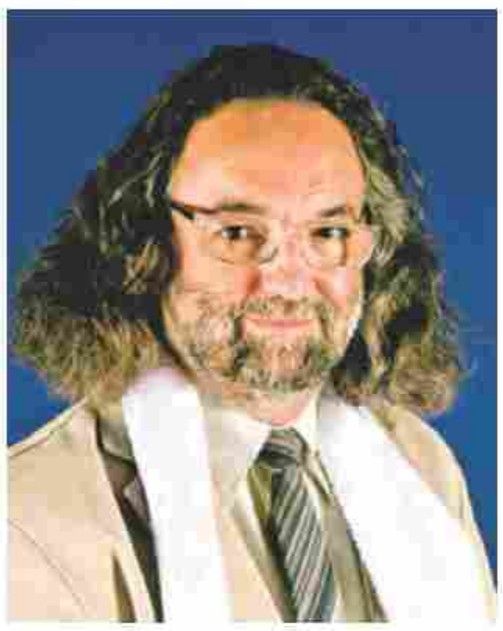
Engage | Innovate | Solve | Secure

www.stanchionpayments.com

Cybersecurity Trends

Contents

The limits of the actual cyber defence plans and the need to rethink the digital world



Author: **Didier Spella**

Issue

The current crisis is plunging us into a unique state which, is not the first time and will certainly not be the last.

Indeed, this is not the first crisis. But as it has a direct impact on our health, for once it has been taken into account by all the world's leaders. Climate change may have been the first, but everyone felt safe, or less concerned... This type of crisis is also seen in cyber attacks.

If such crises are unavoidable, the objective of management must be to minimize their impact so that the structure can continue to operate even in degraded mode and can resume normal activity after a certain period. This is known as Resilience (a value characterizing the resistance of a metal to impact).

The concept of BCP (Business Continuity Plan) has been created. The DRP Disaster Recovery Plan) and the BIA (Business Impact Analysis) have been associated with it to understand the «weaknesses» of the structure.

(

BIO

A former senior officer of the French Air Force, President of Mirat Di Neride, co-Founder of the PPP congress *Charente-Maritime Cyber Security*, Didier Spella is an expert in corporate strategy and cybercrime, head of the CLUSIR - Nouvelle Aquitaine Ouest Office - He has studied the evolution of the different concepts governing today. His knowledge of both analogic and digital security, his experience in risk analysis and his expertise with USA companies have enabled him to position himself as an expert in defining security strategies. Observing and monitoring the cyberattacks that became more and more dangerous and intrusive in our lifestyles, he focuses specifically on the risks incurred by the general population and in particular the threats faced by VSEs and SMEs.

Definitions

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Business Impact Analysis (BIA)

Standard 22301

A standard helps us to take into account these issues of disaster recovery. This standard is ISO 22301. It specifies the requirements for planning, deploying, implementing, operating, monitoring, reviewing, maintaining and continuously improving a documented management system. It will help to reduce the probability of, prepare for, respond to and recover from disruptive incidents of any kind.

The requirements specified in ISO 22301 are generic and intended to apply to all organisations (or parts thereof), regardless of the type, size and nature of the organisation. The scope of application of these requirements depends on the operational environment of the organisation and its complexity.

Emerging Issues

To understand what is happening, we believe it is necessary to model these crises to better understand what is at stake.

These crises share several common features:

- Lack of geographical boundaries;
- Rapid spread;
- Random Propagation;
- Global impact;
- Multi-activities;
- Multi-sector;
- …

These different characteristics lead us to identify limitations to the PCO and DRP. Indeed, BIAs do not cover such characteristics. The prerequisites are generally the following:

- The risks covered are generally fairly co-localized (landslide, fire, flood, etc...);
- Providers are not included in the crisis (not in the same place, not the same activity, not the same resources, etc.);
- The staff or a party may move;
- State organisations are in nominal operation;
- …

So, are our tests still good? Will our Plans be effective in getting back on track?

Structures that already had these analyses and plans were able to use them to go into containment mode. Those that did not have them, the vast majority, "tinkered" with organisations and technical solutions in the field to be able to continue their activity. As security measures took a back seat, they "deliberately" weakened the protection of their information systems.

The impact - Cybersecurity Trends

In both cases, as their claimants were in the same state, they were not able to benefit from their support, contrary to what is generally the case in cases of crisis localized to a company, or at worst a region.

So we see the limitations of the analyses and plans we have developed so far.

Although it is neither the first nor the last, this crisis has proven once again that we need to rethink our activities more globally.

Our analyses must take into account the following concepts:

- Extended Enterprise ;
- Widespread crisis ;
- Degrees of autonomy.

Our plans must:

- Have a comprehensive approach strategically, tactically and operationally;
- Take into account the complete specificities of the structure ;
- Develop a collective awareness among employees.

First conclusions on the impact of the "cyber-COVID" attacks

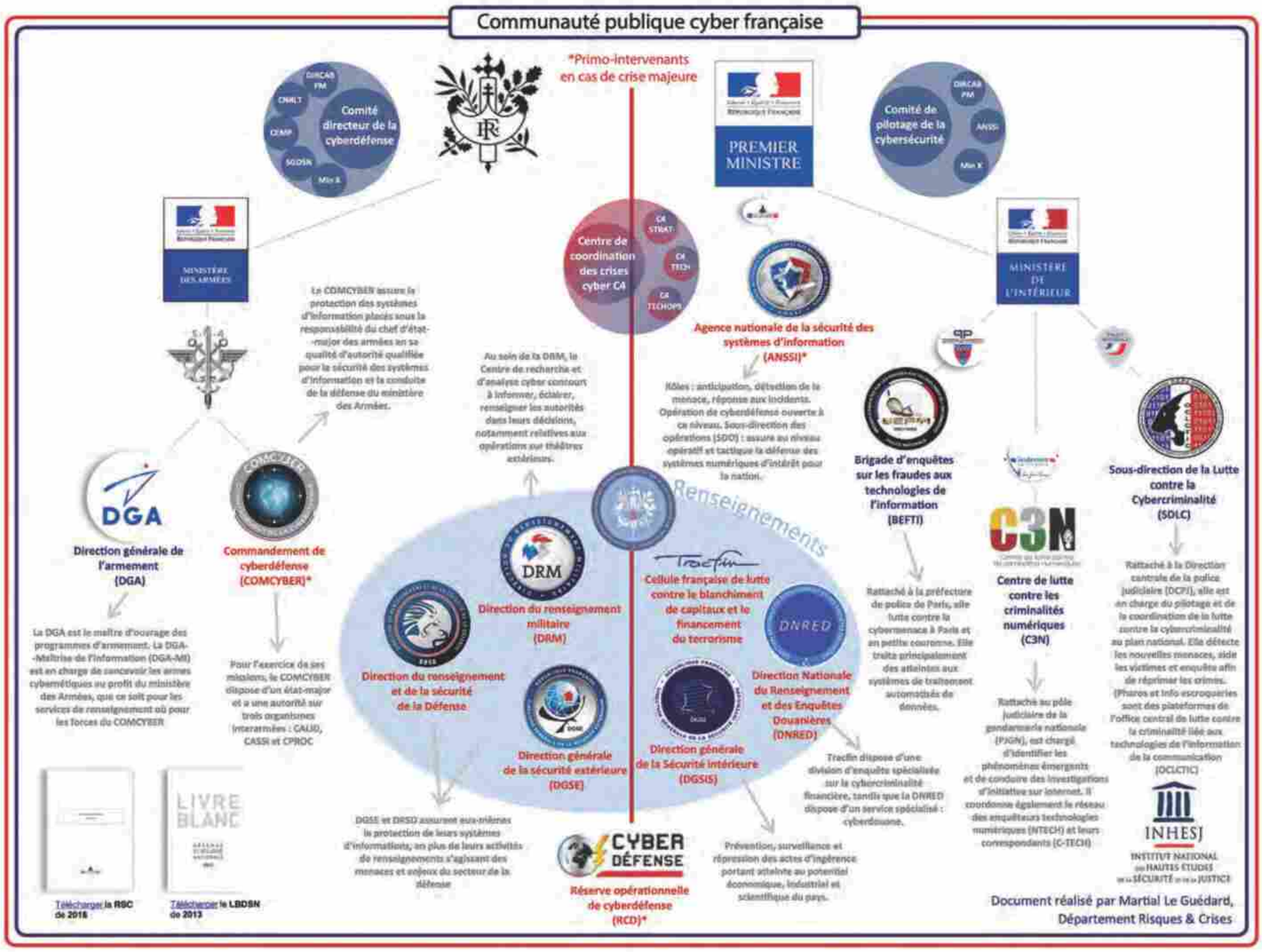
This health crisis shows us the limits of the safety models we have implemented and which, as we can see today, had only one aim: to reassure citizens and employees. They have shown their limits.

We need to rethink our security approaches in a more comprehensive way. As always, let's remain in a continuous improvement approach; whenever we think we have covered a risk, let's be able to think about the new risk we have just developed.

Thinking already to the after-crisis: for a digital maturity

Digitisation affects all sectors of activity and all the professions working in them. This leads us to ask ourselves several questions. Among these, we could choose the following.

1) What will be the evolution of professional skills?
2) With the rise of AI, are we moving towards the end of human thinking in favour of that of the machine?
3) How can the training system evolve?



A general overview of today's French cybersecurity community
(https://inhesj.fr/index.php/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure)

These three questions, and many others relating to the impact of digitization on our daily lives, were only the declination of a more general problem concerning "digitisation".

For me "digitisation" cannot be reduced to a term that vaguely defines the action or actions of transferring or transforming an analogue economy and behaviours into a digital economy.

I think that, first of all, it is necessary to model the digitization and to add a maturity criterion to it.

So I propose that we analyze all of the questions posed using the model that we're going to do.

The Digitisation Maturity Model

To better understand what we are currently experiencing, I think we could describe a digitization process in 4 steps:

Step 1: Scanning the media

This is the very first step in transforming any type of analogue medium into digital, documents, music, in short, all possible types. Humans have a more practical use for these media.

Step 2: Digitising simple tools

It is a question of transforming and adapting analogue tools into digital tools. The typewriter becomes a word processor, the calculator, spreadsheet, etc.. Machine tools are digitised. The human becomes a user.

Step 3: Integration of tools

This third evolution consists in integrating these simple tools into more complex tools by combining different technologies: digital platform - communication - energy. It also combines digital media. We then see the appearance of complex tools, using better the technical characteristics of each of these technological components. The designers of these tools offer comfort through parameterisation, but we cannot speak of real progress. Humans must adapt to the digital tool.

Step 4: Digital integration

By «digital integration», I bring the concept of designing fully integrated digital systems that offer the customisation of all these tools and not just a single parameterisation. The human becomes the central element of this digitization. He can choose the tools that are necessary and useful to him. These tools will evolve with his needs. Personalisation is effective.

As this model has been developed, we can answer the questions asked

What will be the evolution of professional skills?

If we take our model, we can see that the evolution of skills is very real. First of all, we must be able, whatever the activity, to use the basic functions of the tools that make up my business.

However, this level of competence will only allow you to reach the first 3 levels of maturity.

Consideration will need to be given to developing new skills that will enable Level 4 to be achieved. This level involves a «digital redefinition» of my business. This requires, in addition to mastering my activity, knowledge of all the possibilities offered by digital technology, to design a digital integration of my activity.

With the rise of AI, are we moving towards the end of human thinking in favour of that of the machine?

Today's digital world offers us enormous computational possibilities that allow us to consider developing tools

The impact - Cybersecurity Trends

for «decision making». This is at least what the world of artificial intelligence is offering us.

However, even if these calculations seem «infinite», they will never be able to create something from a "zero point", as only the human mind knows how to do, which has allowed us to evolve and thus envisage the impossible. In a very simple way, I will say that today we are capable of dreaming, which a digital machine will never be able to do.

We are therefore moving more in the direction of decision support, should we be at level 4 of the maturity of our systems. The machine would thus offer us all the possible solutions with their constraints, perhaps models of evolution and their "media" representation.

We would then have to choose the best solution.

What about the training system in this evolution?

Given all our reflections, it is obvious that formation must evolve, not to say change.

We cannot be content to reduce the evolution of training to benefit only from the digitisation of media (lighter schoolbags for schoolchildren) or the use of digital tools that allow a little interaction between students and teachers.

Within the framework of "digital inclusion", new forms of teaching must be envisaged where the learner is truly at the centre of the learning process.

The role of the teacher is evolving towards more of a role as a learning prescriber for his or her students. We place the "pupil" or "learner" at the centre of the training system. What is his level, what are his needs, what are his competences, these are the first reflections that the teacher could have in front of his pupil. Complete personalisation of teaching would be implemented so that each pupil acquires the skills necessary for his or her "development".

Conclusion

In conclusion, I think we have before us, through the digital revolution, a major societal transformation.

The digitisation of our society cannot be summed up as simply being users of digital tools that are more or less well developed and integrated into our lifestyles.Progress should not be confused with improved comfort. Today, we are in the business of improving comfort. It is necessary to adapt to the digital world to benefit from it, hence the digital breakthroughs we are observing.

Real progress will require the full integration of digital in our operations. It is up to the digital world to take into account our activities and not the contrary. ■

MANIPULATION THROUGH EMOTION MANAGEMENT

Virtual interactions confer anonymity and can hide the subjective motivation of communication. Users create realities through statements with uncertain validation. The transience and circumstance of the exchange is then confined to emotional communication. Reactions are transformed into carefully formulated outcomes. This staging of emotions sometimes aims to manipulate one or more interlocutors by fascinating or terrorizing them. This can open a door to the discursive strategies of terrorist movements which, when approaching potential sympathisers, implement scenarios that are likely to arouse a certain emotion. Interacting directly with his interlocutor, a manipulator builds a semantic relationship based on an overlap of positive or negative emotions articulated on belonging to a community, a relationship to the event or a fascination with cultural imagery. Laura Ascone's article explores this cognitive field scarcely researched in a scientific way. Her approach, even if centred on the jihadist phenomenon, reveals to be extremely useful to understand our receptivity to the fake COVID#19 messages in this particular period of our lives.

The use of emotions in cyberspace: between discursive strategy and manipulation

Author: **Laura Ascone**

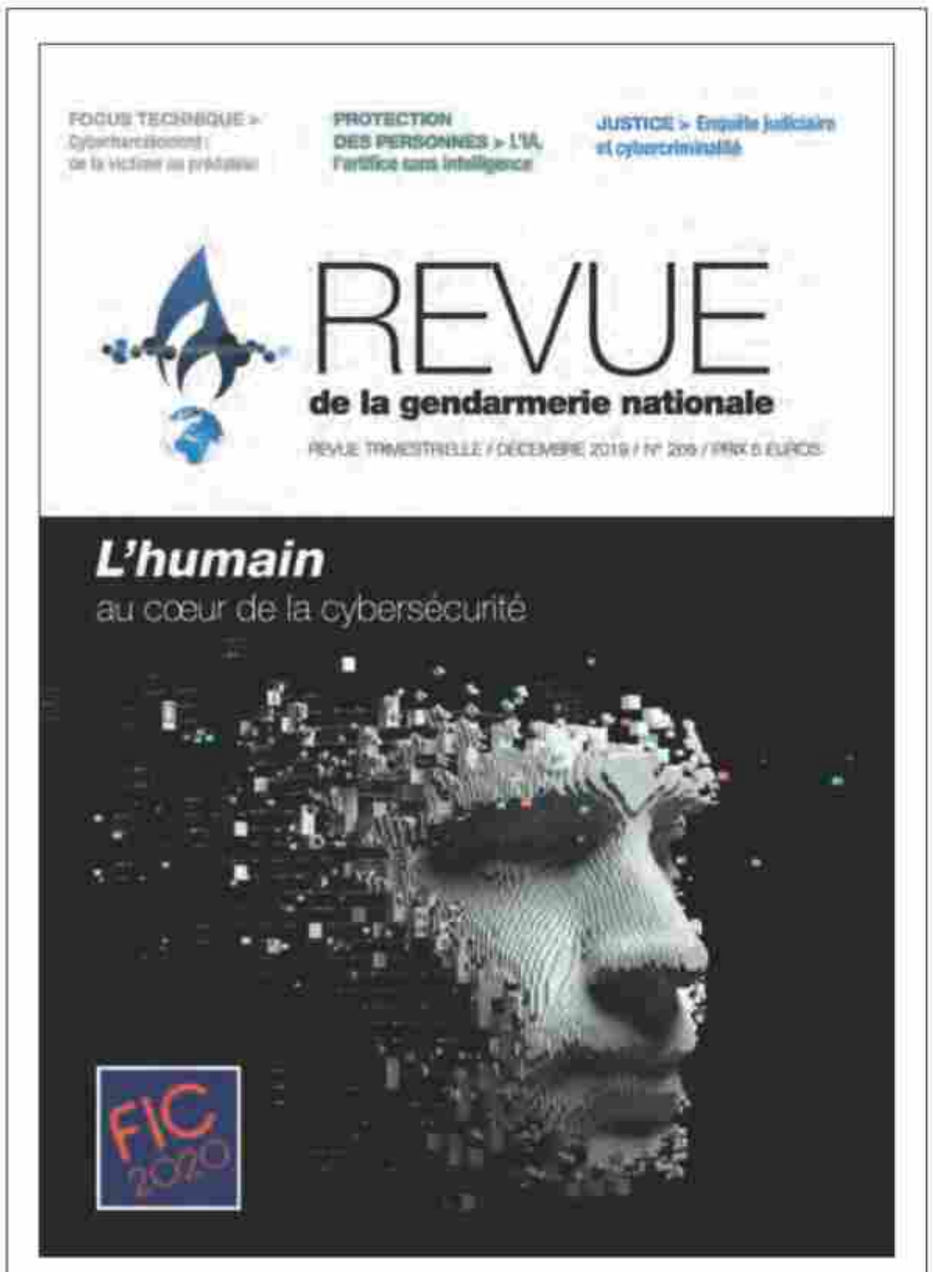
Often accused of dehumanizing interpersonal relationships, cyberspace is, in fact, the theatre of new forms of expression of emotions. Emotional reactions, which are by nature spontaneous, are transformed here into carefully formulated productions. This staging of emotions is sometimes aimed at manipulating one or more Internet users, either by fascinating them or terrorizing them.

BIO

Laura Ascone has a PhD in Language Sciences and wrote her thesis on "Radicalization through the expression of emotions on the Internet" at the University of Paris Seine. She is currently doing a post-doctorate at the University of Lorraine in the framework of an ANR project on hate speech against migrants. Her research focuses on the expression of emotions on social networks, jihadist propaganda and counter-discourse, and hate messages against migrants.

Emotions and Cyberspace

Opening up to cyberspace and the many innovations in communication have inevitably changed how the individual relates to the world and those around him. In particular, notions of time and space have changed dramatically. In cyberspace, network-mediated communication has its own time axis. Despite apparent instantaneity, virtual interactions are not as temporally fluid as real interactions. If one user has to wait for the other to write and send the message, the other has to wait for the message to be read before receiving a reply. However, both users do not seem to perceive this time lag. Similarly, virtual interactions are spatially distinct from real interactions. Although the user is facing the computer in the real world and messages are visible on the screen, the interlocutors do not share the same space (1).



Special thanks: Laura Ascone's original article has been published in French in the *Revue de la Gendarmerie Nationale* n. 266, December 2019, pp. 30-35. We wish to express our deepest gratitude to General Marc Watin-Augouard, the journal's redaction Director and to Colonel Philippe Durand, redactor-in-chief, for allowing us to exclusively reproduce and translate this text. Our most sincere thanks go also to the author, for her kindness and help.

All volumes of the Revue de la Gendarmerie Nationale are available online at:

https://www.gendarmerie.interieur.gouv.fr/Notre-communication2/Publications-Documentations/La-revue

is expressing himself. They will, therefore, tend to modulate the expression of their emotions according to the person they are talking to, the type of conversation they are having and the means of communication they are using.

Types of basic emotions
© ONG Verywell Mind, www.verywellmind.com

Also, the modulation of emotional reactions indirectly influences the reactions of the interlocutor and, therefore, the conversation itself. In other words, deciding how to express an emotion means deciding how to act on the interlocutor, on the communication and on the environment. In particular, the user acts on the interlocutor because the interpretation and the reaction of the interlocutor depend mainly on the way the emotion has been expressed. Kramer et al (2) showed how an emotion expressed on Facebook influences the emotions of other users.

Exposure to a large number of positive messages will lead users to post positive messages. Manipulation and use of emotions The expression of emotions, plays a crucial role in any interaction, whether real or virtual. When the user interacts in cyberspace, the emotions he or she is feeling dissipate instantly, before he or she has time to express them in writing. This is because emotions only last a few milliseconds. Therefore, the user can, more or less voluntarily, decide how to verbalize his emotional reactions. Thus, virtual communication can be considered as emotional communication, rather than the expression of a spontaneous reaction. Emotional communication, where the individual expresses his emotion at the very moment he feels it,

The spontaneity of emotions put to the test

The spatio-temporal shift, which characterises virtual interactions, allows users to hide their identity and the subjective motivation to communicate. In other words, users can create any kind of reality and identity through more or less truthful statements. Moreover, this discrepancy strongly influences the way interlocutors interact and express their emotions. In cyberspace, when the user has an emotional reaction and wants to communicate it to his interlocutor, he will automatically take into account the context in which he is characterised by the description of the emotion once it has dissipated (3). In other words, emotional communication is closer to the notions of performance, rhetoric and persuasion (4). Emotions can, therefore, be staged to influence the speaker's reactions and behaviour.

The terrorist propaganda discourse disseminated in cyberspace is an obvious example of this subtle exploitation of the expression of emotions. The link between terrorist propaganda discourse and emotions can be found in the Latin name terror. This term comes from the Indo-European root ter-, which means „to tremble" and thus marks the link between terrorism and fear (5).

The jihadist discourse testifies to the proximity between terrorist action and fear. On 4 July 2014, the day the Caliphate was reinstated, Abu Bakr Al-Baghdadi said that it was necessary to *„return to the Islam of the early ages to obtain Allah's forgiveness and to regain Arab pride by instilling fear in infidels and bad Muslims".*

In other words, according to Daesh's leader, it is more important to instil fear than to kill infidels and bad Muslims. Concerning propaganda discourse in cyberspace, the jihadist magazine Dar al-Islam is a crucial source of analysis. It allows us to better understand the discursive strategies employed by Daesh.

Widespread on the net since the 23rd of December 2014, Dar al-Islam released ten issues aimed at an audience that has already embraced jihadist ideology. Since it is not an interaction, the magazine cannot modulate its discourse according to the interlocutor. The publisher must, therefore, take into account the different profiles that may have access to this content. Although the expression of emotions plays a central role in propaganda discourse, it is possible to see that emotions are rarely expressed directly. On the contrary, the enunciator will use scenarios that are likely to stimulate a certain emotion. Speeches and images thus contribute to the staging of emotions to reinforce adherence to jihadist ideology. If the exaltation of the jihadist group is intended to nourish love for that community, the condemnation of the enemy is intended to fuel hatred against it.

Emotions and enlistment

Jihadist discourse in cyberspace does not circulate only through official journals. Social networks are also vectors for jihadist propaganda. In contrast to Dar al-Islam, social network interactions are aimed at an audience that is in the process of radicalization. Consequently, the expression of emotions aims at influencing the interlocutor to adhere to the promoted ideology. An example of this manipulation can be seen in the clip They're Telling You, produced by the government to counter jihadist radicalisation in cyberspace. After looking at the Facebook profiles of several jihadists, the protagonist of the video receives a message:

1. Salut
Cool les trucs que tu like,
ça t'intéresse ce ki se passe
au Cham en ce moment ?
si ta des questions hésite pas,
la vérité elle est la bas,
c'est maintenant qu'il faut partir !
si tu me donnes ton num j'ai des amis
la bas ki se battent jte met en contact.

1. Hi
Cool stuff that you like,
You interested in whats going on
at Cham right now?
if you got questions, don't hesitate
the truth is out there,
it is now we have to go!
If you give me your num, I have friends
there fighting I put u in contact.

The messages provokes positive and negative emotional reactions, which can be then fed within the feeling of belonging to a community and rejecting an adversary© Fotofabrika/Revue de la Gendarmerie Nationale

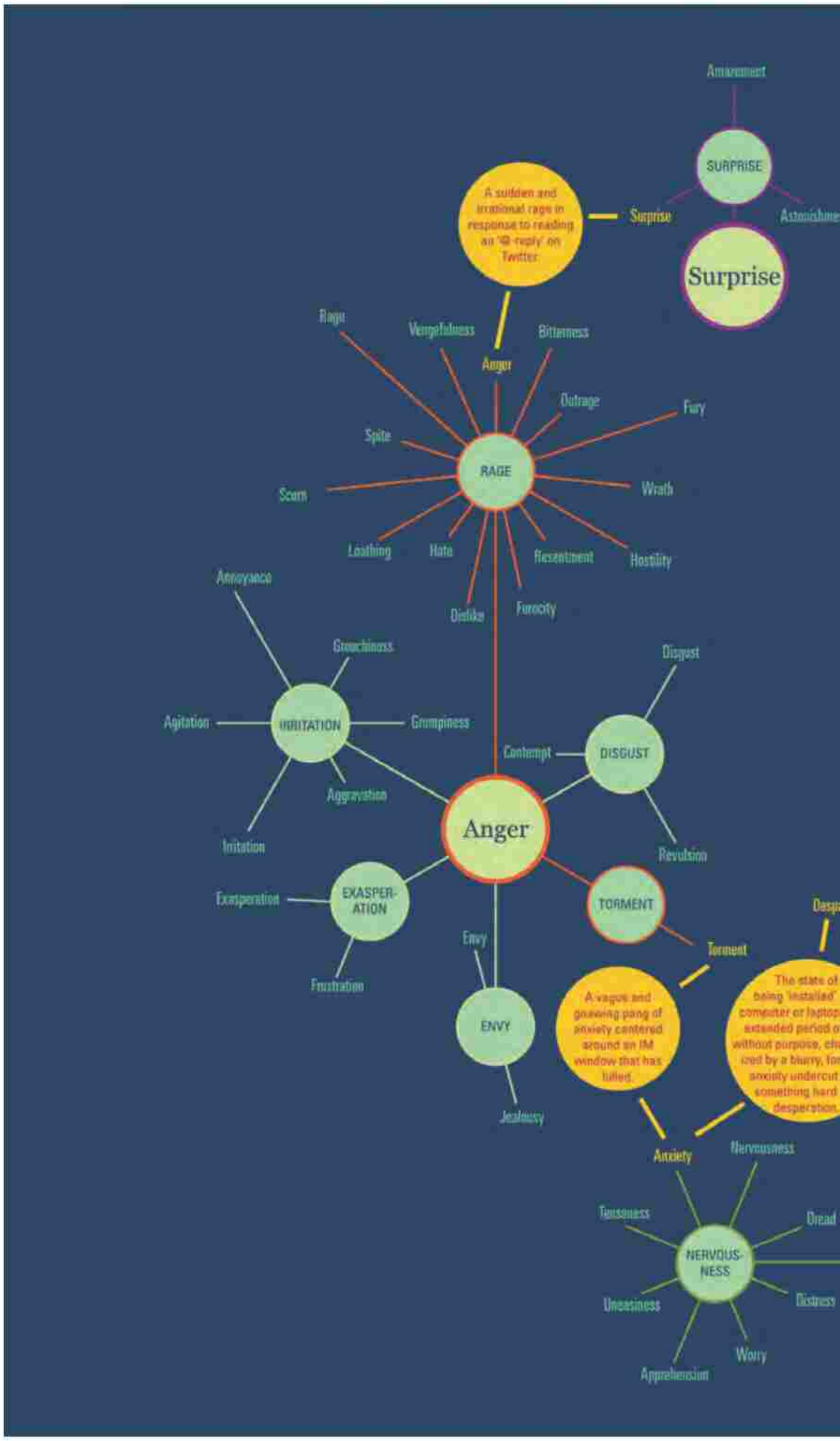
Although it is a reproduction, this message shows the anxiety-provoking nature of messages sent by recruiters. Interacting directly with his interlocutor, the recruiter can easily modulate his speech. He can also create an ad hoc identity thanks to the nature of cyberspace: the perception we have of an individual is mainly built on the information that this individual transmits to us (6). The choice of many jihadists to use a picture of a lion as a profile picture on Facebook aims to show them as strong and courageous people. The internet user, who will tend to forget and detach himself from the real world around him, will end up perceiving everything that happens in cyberspace as true and real. Ben-Ze'ev (7) defines this phenomenon as "detachment". Despite the space-time distance, the user feels a sense of attraction and establishes a kind of relationship with his interlocutor. This manipulation of emotions aims to cut the individual off from his real surroundings so that he no longer feels any emotions towards those close to him. In the same way, through exposure to violent content, the jihadist embezzler aims to accustom his target to violence so that he is no longer afraid to die. In other words, the embezzler uses emotions so that the target no longer feels them.

The paradoxical combination of emotions in jihadist discourse

Although the link between terrorism and fear is obvious, jihadist terrorist discourse does not revolve solely around fear and other negative emotions. Aiming to fascinate its sympathizers as well, jihadist discourse also makes use of positive emotions. Positive and negative emotional reactions are thus articulated within the same discourse. In some cases, two opposite feelings (8) feed on each other. Hate against the unbelieving enemy feeds love towards the jihadist community. And conversely, love for the community feeds hatred against the enemy. This overlap of positive and negative emotions can also emerge with an event. A terrorist attack on Western soil will evoke positive reactions such as joy, pride and adrenaline in the jihadist community. Also, the same attack may also elicit positive reactions from the targeted community. The attacks on French soil, for example, have awakened feelings of solidarity and love.

An approach to analysing emotions in cyberspace

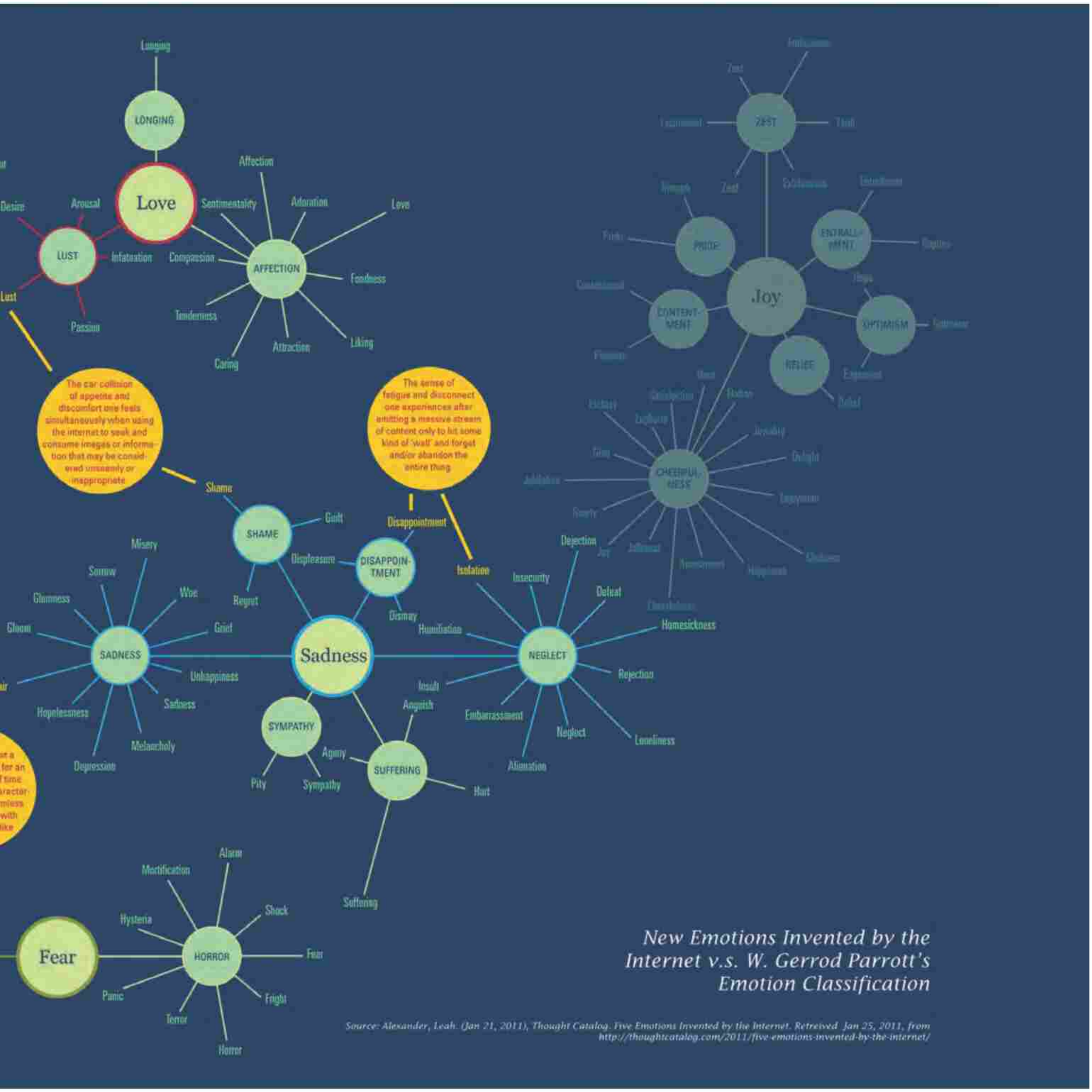
This synthetic panorama of the expression of emotions in cyberspace has revealed elements that need to be taken into account when examining the jihadist discourse disseminated on the Internet. First of all, it is important to analyse a text in its context. This means considering the medium used and the impact it may have on the discourse, the events to which the interlocutors may refer, and the views of the various users participating in the conversation. In particular, this last point makes it possible to determine whether a message expressing a positive emotion is really positive content or whether, on the contrary, the object of such an emotion constitutes a potential danger to the community. Furthermore, it is necessary to consider that our discourse is imbued with our impressions even when we do not express our emotions directly (9). Therefore, to analyze jihadist radicalisation through the expression of emotions in cyberspace, we



cannot limit the study to the analysis of only negative emotions. Similarly, as we have shown, it is important to study not only the expression of emotions but also how the enunciator, through his speech, elicits emotional reactions in his interlocutor. ■

Notes:

(1) Kramsch, C. G. (2009). The Multilingual Subject: what foreign language learners say about their experience and why it matters. Oxford University Press.
(2) Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 8788-8790.
(3) Plantin, C. (2011). Les bonnes raisons des émotions. Peter Lang Publishing Group.
(4) Arndt, H., & Janney, R. W. (1991). Verbal, prosodic, and kinesic emotive contrasts in speech. Journal of pragmatics, 15(6), 521-549.
(5) Di Cesare, D. (2017). Terrore e modernità. Torino: Giulio Einaudi Editore.
(6) Mantovani, G. (2002). Internet haze: why new artefacts can enhance situation ambiguity. Culture and Psychology 8, 307–326.
(7) Ben-Ze'ev, A. (2005). 'Detattachment': the unique nature of online romantic relationships. In Y. Amichai- Hamburger (ed.), The social net: Human behavior in cyberspace, 115–138. New York: Oxford University Press
(8) Contrairement aux émotions, qui ne durent que quelques millisecondes, les sentiments ont une durée plus importante. Ekman (1992) identifie six émotions primaires : joie, peur, colère, surprise, tristesse et dégoût
(9) Shaver, P., Schwartz, J., Kirson, D., & O'connor, C. (1987). Emotion knowledge: Further exploration of a prototype approach. Journal of personality and social psychology, 52(6), 1061



New Emotions Invented by the Internet v.s. W. Gerrod Parrott's Emotion Classification

Source: Alexander, Leah. (Jan 21, 2011). Thought Catalog. Five Emotions Invented by the Internet. Retreived Jan 25, 2011, from http://thoughtcatalog.com/2011/five-emotions-invented-by-the-internet/

THIS SPECIAL ISSUE IS PLACED UNDER THE AEGIS OF:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

IT HAS BEEN REALISED IN PARTNERSHIP WITH:

National Gendarmry (FR)
www.gendarmerie.interieur.gouv.fr/

Research Centre of the Officers' School of the National Gendarmry (FR)
www.gendarmerie.interieur.gouv.fr/crgn/CREOGN

Geneva State Police (CH)
www.ge.ch/organisation/corps-police

CYBERINT Centre of the Romanian Intelligence Service (RO)
www.sri.ro

Directorate of Countering Organised Crime - Romanian Police (RO)
www.politiaromana.ro

National Cyber Security and Incidents Response Team (RO)
www.cert.ro

National Authority for Management and Regulation in Communications (RO)
www.ancom.ro

Global Cybersecurity Center (IT)
www.gcsec.org/

Association of Users of Information Systems in Morocco (MR)
http://www.ausimaroc.com/

Forum international de la cybersécurité (FR)
www.forum-fic.com

Charente-Maritime Cyber Sécurité (FR)
www.cmcs-connect.fr

Cybersecurity Dialogues (RO-IT-CH)
www.cybersecurity-dialogues.org

Swiss Cybersecurity Assciation (CH)
www.swiss-cybersecurity.ch

AND WITH THE SUPPORT OF:

www.blockapt.com

www.stanchionpayments.com

When isolation associated to fake news can lead to hospital

Author: **Octavian Oancea**

Dear Reader,

Today, I would rather tell you a real story, so as I am putting my cybersecurity hat off, I will open one of my personal drawers.

The other day, something unusual and sad happened. As I was going about my life and work in auto imposed isolation, I received a call from a friend concerning one of the people we both know. It turned out that he had a severe episode of depression. We knew that for a couple of years he was consuming different conspiracy theories and although we tried to combat them with science and facts, it was usually to no avail. What we missed was the effect these years of exposure to misinformation can do to someone's mind. We then sat in front of it, visiting our buddy in the hospital. Yes, it was that bad!

It turns out that the poor fellow panicked so severely, watching this content around COVID-19, packed with a plethora of nonsense around 5G

technology and other pseudofacts, and got pushed to the edge in such a way that he could not sleep for several nights. This, in turn, strained his physical limits and then he snapped. With a snipped of sanity in his brain, he realized he needed help and reached out.

Talking with him in the hospital yard, he now realized how bad his decisions were, to trust those theories and how much it harmed him, but he admitted it was impossible at the time to let them go. Somehow, it fed his quest for sensational news, and he had a sense of privilege to have access to such information.

And this brings us to today's topic: misinformation and the effect on our health. We tend to overlook this, mainly because we are educated to filter our newsfeed. Working in the cybersecurity field, we are the lucky ones, because our work makes us better in spotting fake news and disinformation as it is quite connected with our work: phishing campaigns, social engineering and the likes. And I have to admit, the many times, friends that asked me how to better protect themselves in the digital space, I was quick to come up with solutions, well… concerning the devices themselves – securing them and their behaviour around them as well. I hardly taught on giving

BIO

Octavian is currently the CEE Channel Business Manager of Trend Micro. He holds a BSc and an MSc from the Polytechnics University of Bucharest. He has a genuine passion for excellence, driven in both his career and private life. As a professional, he proves highly skilled in evaluating markets and identifying untapped opportunities through forging new business relationships. Previous roles include General Manager and founder of McAfee Romania, Avnet Technology Solutions Romania and ZyXEL Communication Romania. On a personal side, his deep interests go in Music, Photography, Sports and Information Technology with a focus on Information Security.

them advice on how to consume the news on those devices, and yet it looks that nowadays this may the bigger problem.

Think of it: let's say that, with a bit of bad luck, you may get a ransomware variant on one of your devices. Chances are that, if you have good security in place, you would only get a scare. Going a bit more unlucky, you may lose your data on that device. And so you learned the hard way to change your cyber habits, but apart from a bit of frustration, you get to accept that what's done is done and you move forward. I've met people that lost some (considerable) amounts of money as a result of some targeted campaigns. They were annoyed, but managed to put this behind them, learned the lesson, and moved further.

Now, let's get back on the effect of the daily frustration the everyday people get from their news, their social media and TV and put this into a context where most of us are in a lockdown. We don't know so much about this virus and hence we are afraid: for our families, health, jobs - so many unknowns. Plus, we do have more time than ever to spend around our devices. Think about the chemical cocktail in every day's people's brains. No wonder so many people, getting out of their quarantines, went directly to the lawyers.

Where am I going with this? Knowing the above, we should acknowledge our roles in society and educate people on how to consume information. Humanity battled severe crisis before, but there is an unprecedented level of media manipulation that most people don't know how to handle, and, particularly in these times, there are severe consequences on wellbeing and sanity of population.

Reach out to some of your closest friends today. See how they fare, and if you can, bring the discussion where you can help them filter their daily news. Let's start from here ☺.

Stay healthy! ■

Perimeter security and VPN versus "Zero Trust" security within the coronavirus pandemic

Author : Cătălin Pătraşcu

Several mainstream media headlines (1-3) pointed out that, with the coronavirus (SAR-CoV-2) pandemic, cyber attacks have increased dramatically, with attackers focusing now on exploiting this situation, a fact is also confirmed all national and international competent authorities (4,5).

This is due, on the one hand, to the fact that the pandemic has taken virtually all the global attention, and this increased interest greatly enhances attacks based on techniques related to social engineering (phishing, spear-phishing, landing hole, spam, etc.). On the other hand, most people now work from home and access the company's computer resources

(email, documents, databases, files, etc.) remotely, creating vulnerabilities for companies that still rely on the concept of perimeter security - unfortunately most companies.

We are not talking here, however, about new types of attack, or new techniques used by attackers. The difference is that the pandemic provided the best «platform» and favourable context possible to cybercriminals. For example, watering hole attacks are based on malware infecting the websites used by the targeted group, result in infecting all those accessing the infected website.

At the time we write these lines, websites providing real-time information and maps about the pandemic are by far ideal candidates for such type of attack, an opportunity immediately seized by the criminals.

BIO

Cătălin is an experienced cyber security expert with more than eight years of a demonstrated history in the information security field. He started his Cyber Security journey in the Romanian Ministry of Defense (2010-2012), continued as a coordinator of the incident handling team at the Romanian National Computer Security Incident Response Team – CERT-RO (2012-2018), and is currently activating as a Security Delivery Manager for a company that offers cyber security services worldwide. He successfully managed cyber security related projects, planned and moderated cyber exercises, handled different security incidents at national scale, and conducted various studies on cyber security and cyber crime topics.

But let's go back to the concept of perimeter security. Traditionally, businesses secure their infrastructure by creating virtual network areas, most often Internet (public, unsecured area), DMZ (typically server and application area), and LAN (internal network). But since the increased mobility of employees and their need to access company resources wherever they are, the limits of this strategy were already highlighted.

VPN technology came as a momentary "patch", allowing the off-network terminals to be connected via a virtual network to the company's internal network, thus having access to resources as if they were actually inside that network.

Alas, that the pandemic created a significant increase of the number of VPN connections and many companies were not ready to cope the consequences of this "boom", meaning that the equipment that enabled this type of connection was not sized to grant all employees a safe connection from home.

Companies had to upgrade their hardware in a very short time, which in addition to financial costs usually meant temporary service interruptions.

Ideally, we would advise replacing perimeter security and VPN technology by a new framework called "zero trust", based on each user, each terminal, each application, and each process, with the same level of trust for all employees, wherever they are, but with levels of access being tailor-made and designed according to the position and needs of every single collaborator. Fortunately, this framework is useful not only in the context of the coronavirus pandemic but, as it has been strongly encouraged during the recent years when mobility and remote work have grown, its adoption will grant an enhanced level of security to the company opting for it way after the sanitary crisis will be over. ■

Notes:

(1) https://euobserver.com/coronavirus/147869
(2) https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
(3) https://securitytoday.com/articles/2020/03/26/world-health-organization-facing-cyber-attacks-during-coronavirus-response.aspx
(4) https://cert.ro/citeste/alerta-campanii-frauduloase-coronavirus
(5) https://www.us-cert.gov/ncas/alerts/aa20-099a

IV. Short guide of cyber-defense to be used during (and after) the pandemic

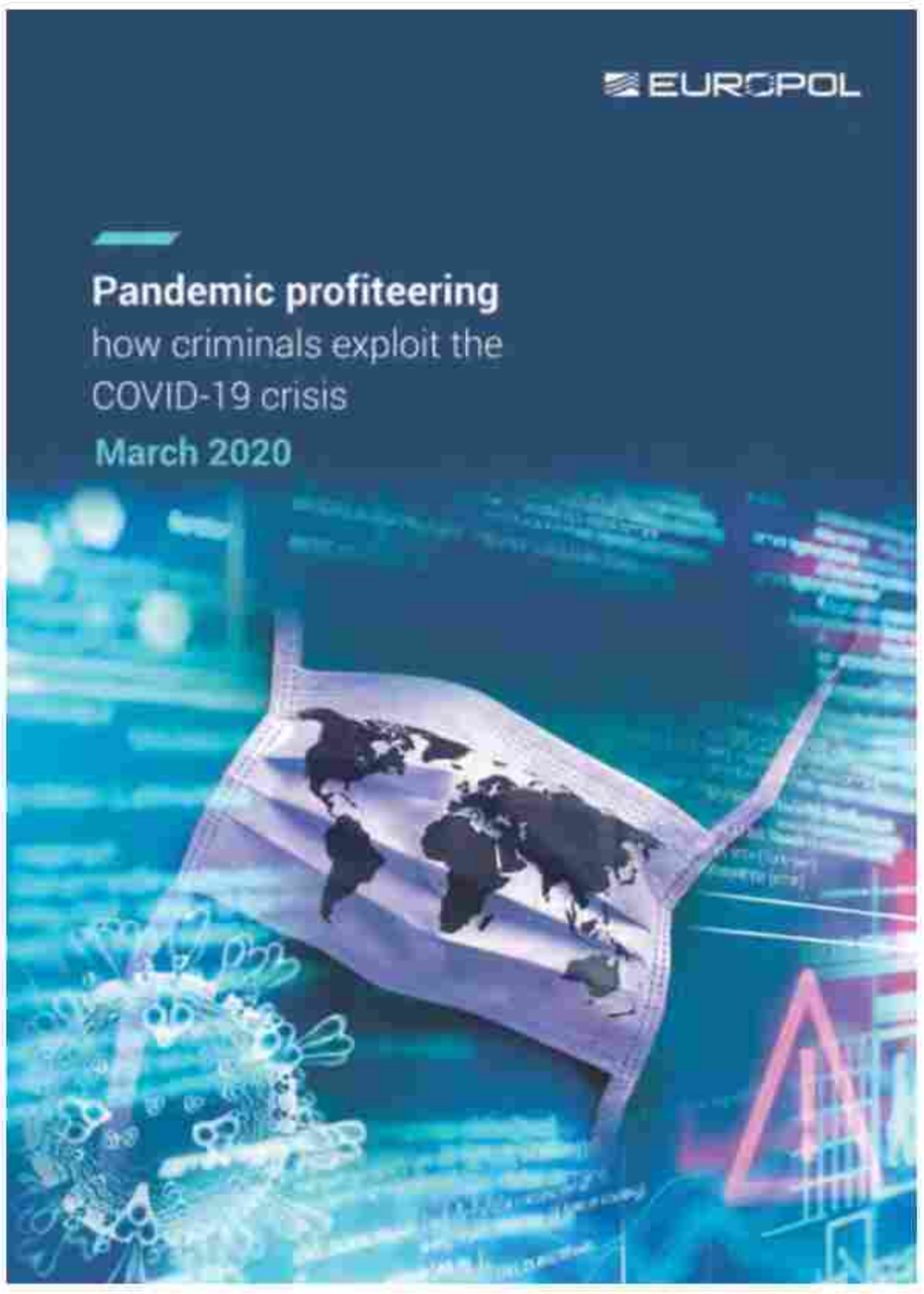
COVID#19: a brief international guide to cyber-defence and self-protection

Author: Laurent Chrzanovski

An Europe with always shy and uncoordinated bodies, in the EU just like in the individual member countries

Despite the total emergency of cyber-attacks, Europe provides, of course, information, but very few centralized agencies have created a special COVID section on their homepage. CERT-EU (www.cert-europa.eu), for example, continues as if nothing had happened while offering all the technical details of the attacks found and examined, as does ENISA (www.enisa.europa.eu). The most proactive agency therefore remains EUROPOL's EC3 cell, which not only developed a basic educational cartoon available to all, but also created a high-quality report *"Pandemic Profiteering: How Criminals Exploit The Covid-19 Crisis"* (16) with useful tips and examples and a special section on its homepage (www.europol.europa.eu).

If we then look at the individual countries, there is a colossal contrast between Spain and the other states. In Madrid, it was decided to centralize all the information on the INCIBE (InstitutoNacionál de Ciberseguridad) website (www.incibe.es), creating a huge banner on the homepage dedicated to the COVID attacks (17). In addition to recurring reports and a timely updated newsfeed, the various vital messages are also widely broadcast by all law enforcement agencies - from Police to Army to Civil



Some of the Spanish «pills» © INCIBE

BIO

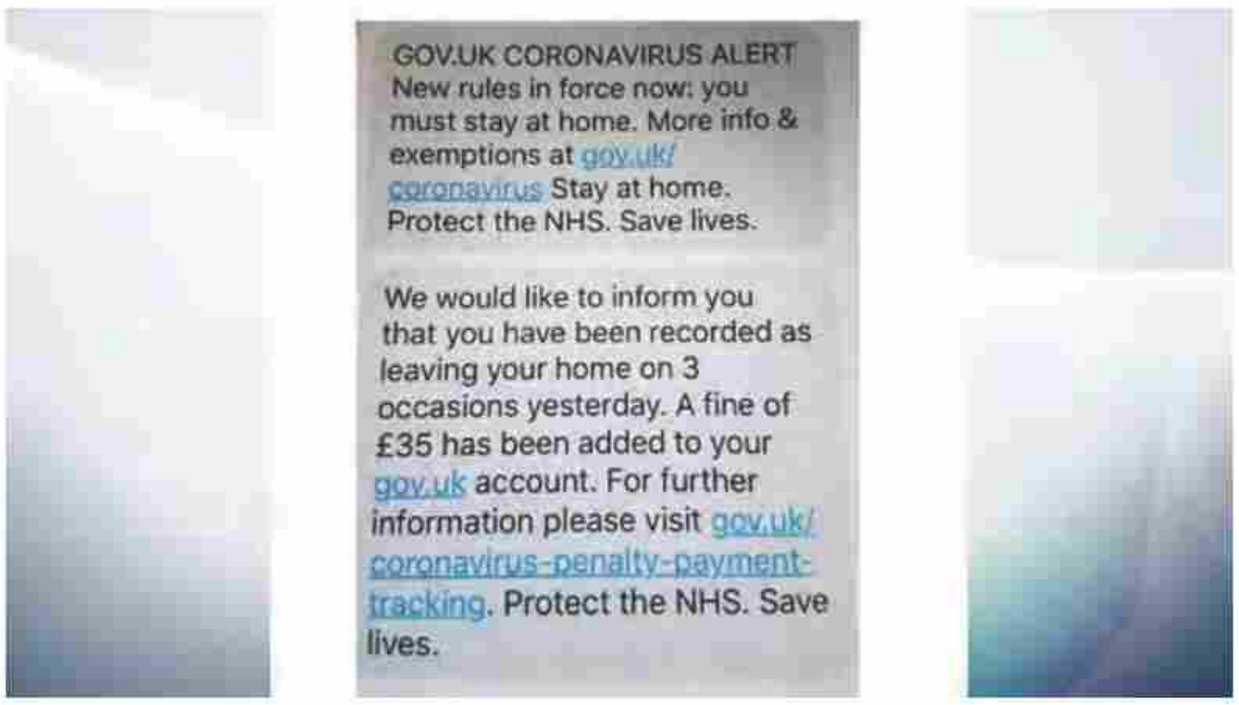
With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/editor of 32 books, of more than 150 scientific articles and of as many general-public articles.
In the frame of cybersecurity, Laurent Chrzanovski 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 cyber security 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: A cyber front with no limits. Attacks never seen before, in diversity and quantity. Guidelines for facing them and defending yourself.

For the use of our readers, we would like to propose here a list of the main means used by cyber criminals to attack almost every kind of people and entities, *"urbi et orbi"*. According to Bitdefender, the global attacks in March saw an increase of 500% compared to those in February... which were already very high.

1. Mass misinformation in times of panic, including e-virus

Many countries have taken extraordinary steps to censor fake news. They almost always come across the problem that all specialists in the field have: social networks and extra-territoriality. The lack of discernment between an official statementand fake news, onthe part of many citizens, continues to forever propose the theme of awareness.



Fake British Government news sent via Whatsapp © Skynews

There is no lack, however, of examples of false official documents, as it happened in Italy. As a matter of fact false ministerial letters to the imageof that of the Ministry of Education, sent on social issues and denounced by Minister Lucia Azzolina (22), made news recently.

Protection and tax authorities - on their websites, in the form of 30 "pills", with graphics that deserves much of a hat.

Italy, like almost all the other countries of the continent, offers the citizen a real maze of sites that do not refer to each other, thus reducing the visibility of their advice and documents, although very useful and drafted with great care. The **Communications Police** updates daily on the most serious facts (www.commissariatodips.it) while there are no less the sites, with pages dedicated to COVID-Cybercrime, of the **Cert of the Public Administration** (18), the **Agency for Digital Italy** (19), **CertFIN** (20) and the **Italian Association of Clinical Engineers** (21). The other organizations, in the image of the CERT-EU, prefer, until today, to treat the attacks as they appear, whether or not they are tied to the COVID# 19 and to the specificities of the ways of life and work now imposed on all Italians.

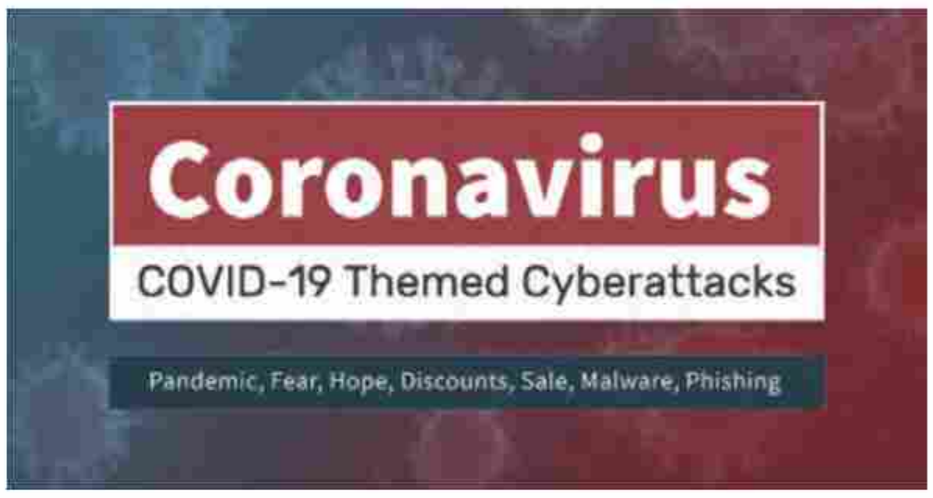
▸▸Learn how to inform yourself correctly !

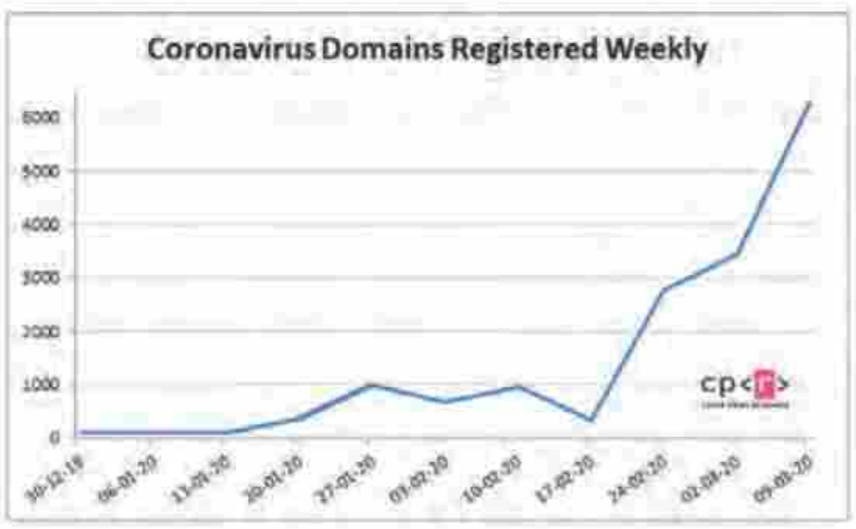
With the urgency of COVID, the proactive *News Litteracy Project* has launched, for the English-speaking public, one of the best possible initiatives: a direct teaching app, almost ironically entitled *Are you informable?* (https://newslit.org/coronavirus/).

The app to calm the panic and get back to reliable sources © News Litteracy Project

A booming element is precisely the use of the same fake news to hide powerful malware, as was revealed by a recent report by Adam Pilkey for F-Secure (see biblio 13), masterfully illustrated and partially reproduced here. As can be seen in the article, these are considered as examples related to *malwares* in as many as 12 countries, from Asia to Europe and the United States. Another major concern is the number of domains that refer to the official or popular name of the virus, all potentially in the hands of criminals, as highlighted in Lakshmanan's report *(biblio n. 14)*.

Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks





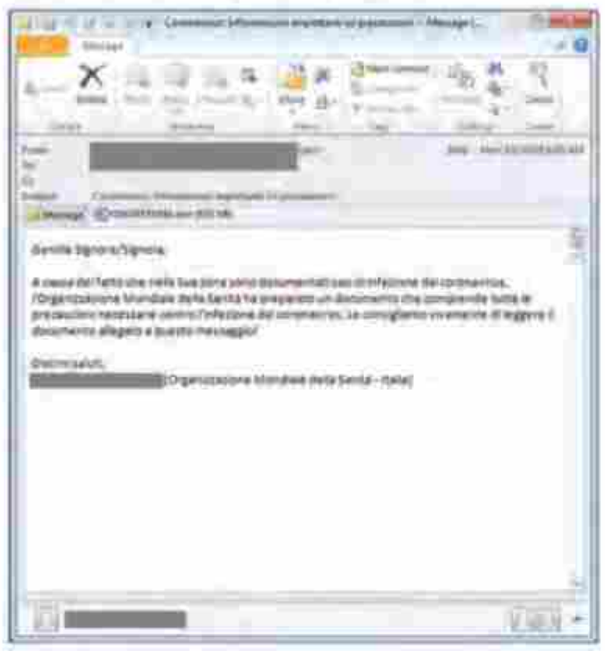
MAR 2020

Legitimate News

CORRIERE DELLA SERA · MALATTIE INFETTIVE

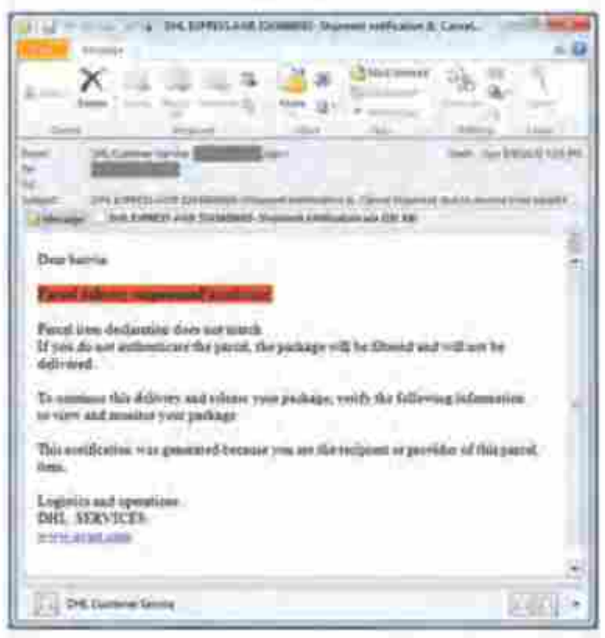
Coronavirus, in Italia i casi sono 1.694. I dati regione per regione al 1 marzo

TRICKBOT Spam



Legitimate Advisory

FORMBOOK Spam



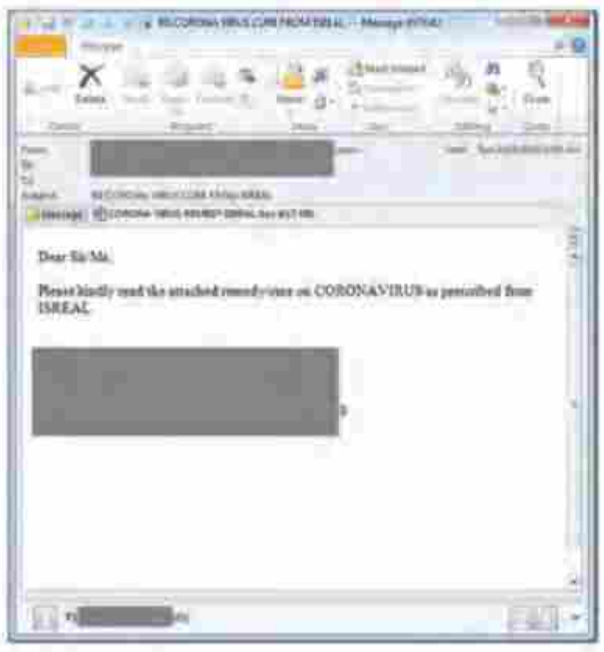
Right: part of Pilkey's illustration. Left: headlines of specialized newspapers © Cyberhub and Montalbano, Threatpost (biblio n. 12); number of sites related to the name „Coronavirus" purchased by criminals in recent weeks © Checkpoint, see Lakshmanan (biblio n. 14).

Legitimate News

NEW YORK POST

Israeli scientists claim to be weeks away from coronavirus vaccine

AGENTTESLA Spam



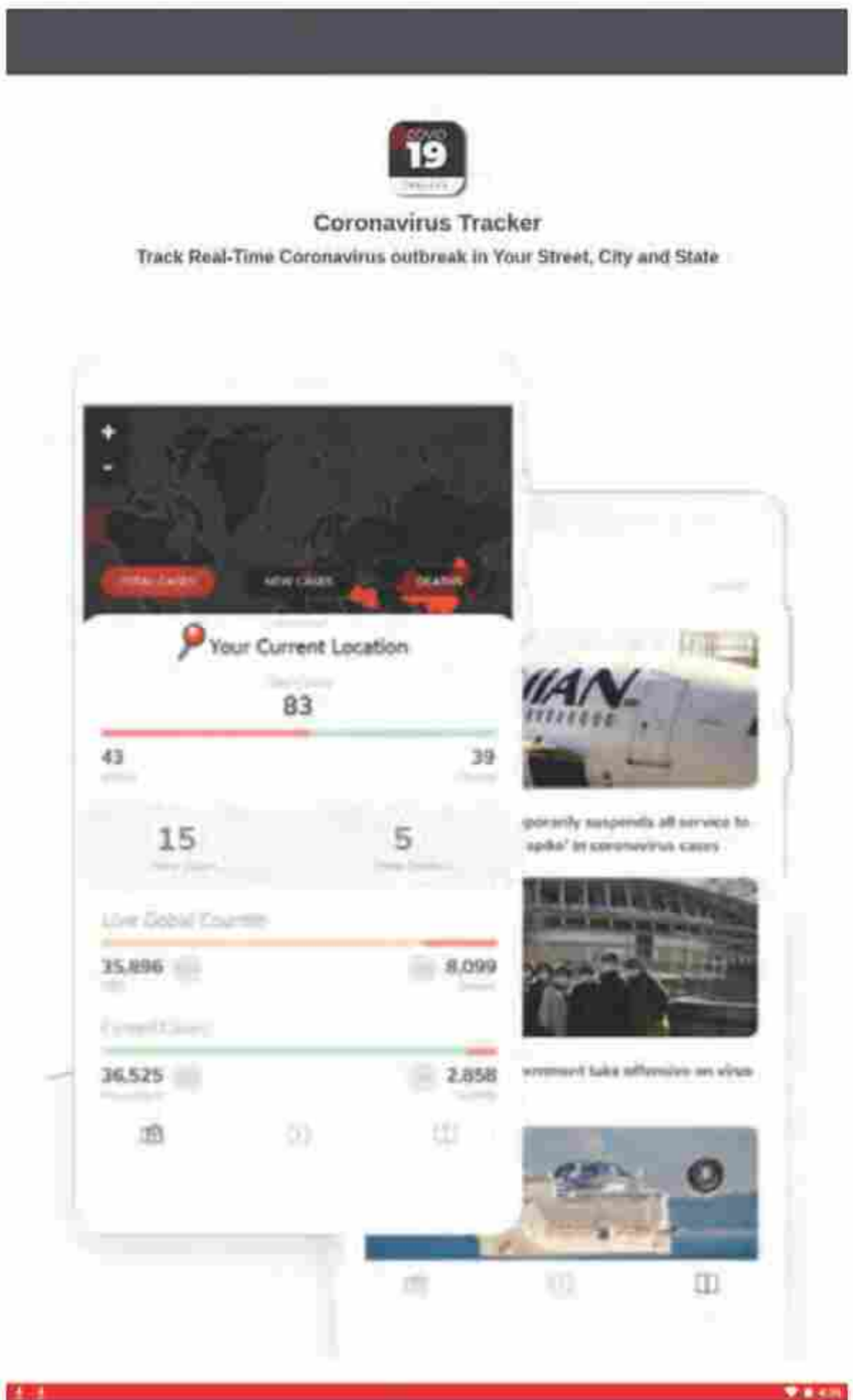
2. Desperately looking for mobile tools info: the criminal apps dedicated to COVID#19

Beside the number of fake news sent through mails, such as scam or malicious links on social networks, dozens of fake apps are being created weekly to "inform" the user about the global and national situation and provide "useful information".

Almost all of them intended for smartphones equipped with the Android system, are giving all security specialists a hard time. Although rejected by the various native "stores" of smartphone manufacturers, they are downloaded directly from the Internet by users. While

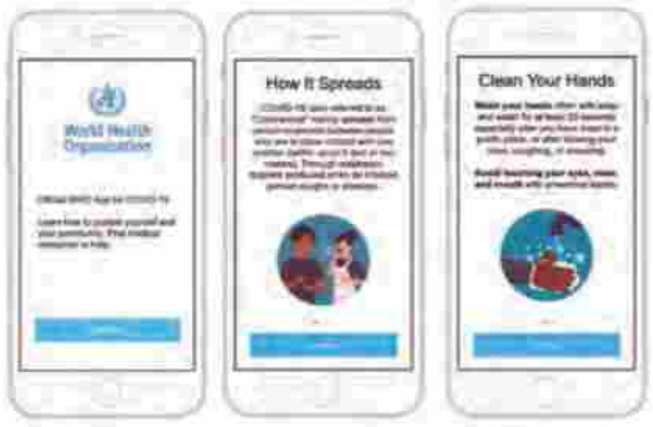
many of these apps simply copy more or less substantial parts of the contents of the victim's smartphone, some of them spy the users through the use of the microphone and camera.

At the moment, the most evil of these Apps is undoubtedly **"Covid 19 Tracker"**, discovered on March 10, because it's not only a very powerful spyware but also a ransomware. A few hours after its activation, it blocks the smartphone with a powerful crypto-ransomware and requires $100 in bitcoin to unlock it, as well explained by Tarik Saleh (23).



"Covid 19 tracker»: advertising, visual and... blackmail © Saleh, Domaintools

"Covid 19 tracker»: advertising, visual and... blackmail © Saleh, Domaintools



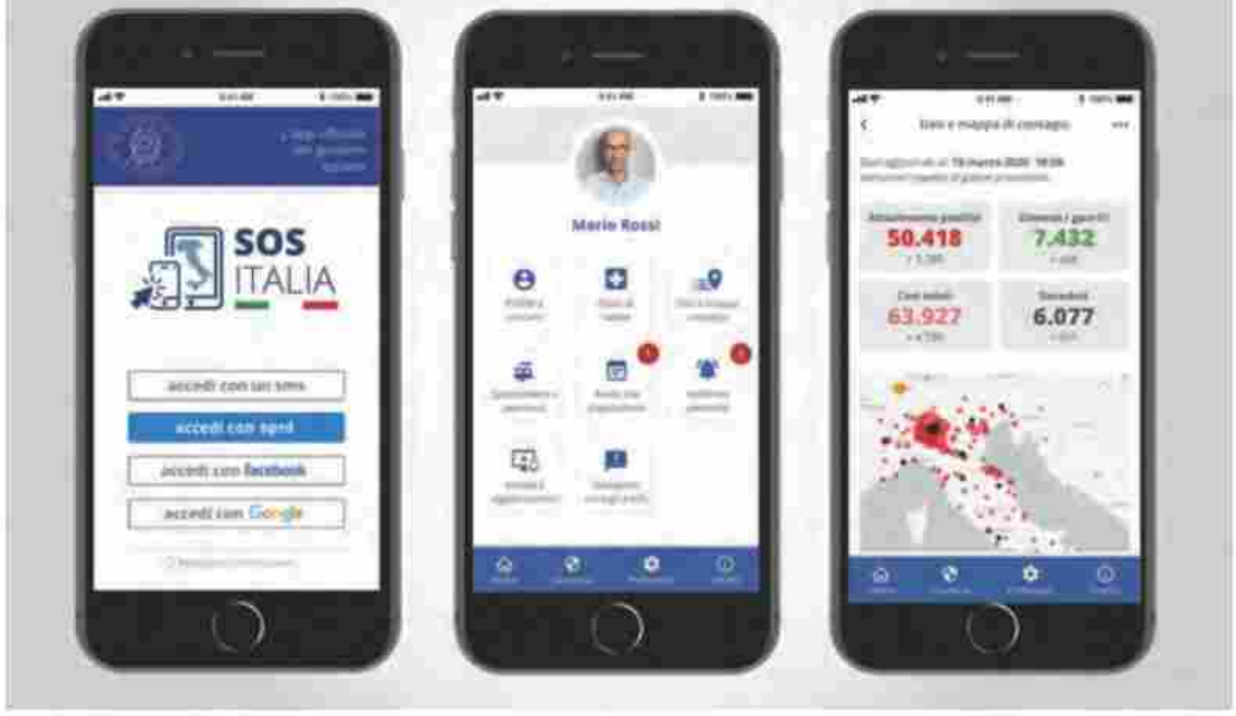
The interface of the WHO MyHealth app according to the prototype given to the media ©New York Post

DOWNLOAD apps guaranteed by States, WARNING in the use of GAFAM apps

In the face of the huge number of apps about the virus, the World Health Organization will launch, at the latest in early April, an App of its own, free and available in all the languages of the world, called *"WHO MyHealth" (24)*.

Meanwhile, in Italy, there are two initiatives ready. The first is the planning of an app for health and scientific disclosure purposes, intended to reassure, give advice, make the self-diagnosis of the first symptoms of the virus easier and track contagions. It is the result of the work of a scientific group of excellence, and is now awaiting final validation by the Ministry of Health (25).

The second app aims at the collaboration of citizens, at the management of the crisis and facilitates the completion of the exceptional forms. It was developed by the Italian Digital Revolution Association with SOS Italia in the framework of the governmental project "Innova per l'Italia" (26). The app has as its first aim the simplification of pandemic management, thanks to a system that integrates a self-diagnosis tool, an account of the latest news and official communications, a contagion map and a self-certification management system based on QR Codes, that simplifies the work of law enforcement (27).



The interface prototype of the "Sos Italia" app © La Stampa

The GAFAM apps, always the same non-European management, always the same practices: your data becomes theirs, *forever.* It is right, in this field, to encourage prudence and reflection before making the decision to download and use one of the official apps of GAFAM and the companies they own.

This also applies to most of the paying apps that have emerged in the wake of this new market. Please check which parameters and information on your smartphone will necessarily be accessed *"for optimal operation"* before downloading them!

As for social networks, we'll have to wonder if we'll be ready to accept in one click a very long contract that explains that all your data **can/will be recorded (without time limit) "to improve our products",** as we read, to give an example, in the privacypolicy of Apple's "COVID-19 Screening Tool" app (https://www.apple.com/legal/privacy/en-ww/).

3. Heart of gold? Don't let criminals take advantage of your generosity!

On the web and social pages of all the police forces of Europe, not a day goes by without an emergency announcement being posted about false fundraising, like the one issued by the Communications Police in Italy. (28).

The most serious of the attacks was aimed precisely at the world crisis management agency, the World Health Organization (WHO). Millions of phishing emails were sent, in almost every language of the world, calling for donations.The email include the OMS logo as well as parts of the descriptions of the "COVID-19 Solidarity Response Fund"(https://covid19responsefund.org) and false bank account numbers. Furthermore the emails often collect personal data, and sometimes they include, the icing on the cake, attachments carrying a malware. The official reaction of the UN body explains well the gravity of the incident (29):

World Health Organization

Beware of criminals pretending to be WHO

Criminals are disguising themselves as WHO to steal money or sensitive information. If you are contacted by a person or organization that appears to be from WHO, verify their authenticity before responding.

The World Health Organization will:

- never ask for your username or password to access safety information
- never email attachments you didn't ask for
- never ask you to visit a link outside of www.who.int
- never charge money to apply for a job, register for a conference, or reserve a hotel
- never conduct lotteries or offer prizes, grants, certificates or funding through email.

The only call for donations WHO has issued is the COVID-19 Solidarity Response Fund, which is linked to below. Any other appeal for funding or donations that appears to be from WHO is a scam.

▸▸Use only the information provided by the official websites.

The only advice, in this period more than ever, is to never listen to charity requests received by email. Once you have chosen the Organisation or the Non-profit to which you wish to contribute with a cash gesture, you must check on the original website of the organisation of your choice which are the payment methods, the exact titles and the correct bank references.

4. Scared? Beware of medications, masks and other sanitary utensils for sale online

On all sites with "ads" now prevail the advertisements inciting the purchase of miraculous "antivirals", protective masks, and whole panoplies of means intended to "prevent contagion". A large part of the scams - some with powerful viruses attached (30) - received by email have in fact sniffed out human fear and the need to seek protection as the weakest link of a rationality that we all tend to lose when our lives or those of our loved ones are at stake.

IT MUST BE REMEMBERED THAT THERE IS NO SUCH THING AT THE MOMENT, NEITHER VACCINE NOR CURE APPROVED TO COPE WITH COVID#19.

The treatments - **in hospital and only there** - that have allowed the recovery of many patients who did not suffer from serious medical history are in fact different from country to country and often from hospital to hospital. It should be stressed that certain products praised by the press, such as *Chloroquine* - are only partial components of the "pharmaceutical cocktails" developed by hospitals. As such, they must never be used in self-medication - they are illegal to purchase, and their use without medical supervision has already caused many deaths in the United States.

Buying online on sites that hide well their real geographical location is very dangerous. An example of this are the websites selling false insurance policies for coverage by COVID-19 reported by the Communications Police (31), the risk of which is that you never receive anything after your payment, the least of the evils I'd say.

The worst case scenario is that the order you have bought arrives at your home, complete with boxes containing counterfeit medicines, which at best are flour dough, at worst they include dangerous substances that could prove to be a real harm to your health, as is well illustrated here, below by a page, from the comic book of the *Swiss Crime Prevention Group* (32).

On the spread of the COVID-19 and of related cyberattacks: a double threat for our societies

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

Author: **Arthur Mattli, Ambassador of Switzerland to Romania**

The spread of the COVID-19 and the current spread of Cyberattacks have many things in common: both spread invisibly at high speed, they disrupt the lives of millions in a dreaded way, they have an ominous economic impact worldwide, and both are unwantedly interlinked. Most of the lockdown measures imposed by Governments led to extensive disruption of human behaviour. While the food supply chains and logistic businesses seem to hold on, we witness a profound shift in the service industries towards remote workstations, schools switching temporarily to on-line courses and on-line services facing exploding demands.

Luckily, the digital world we are living in offers us in this unparalleled difficult time tremendous opportunities to continue to do business, to maintain social contacts and even to improve human lives. But its unintended effects of our brave new digital world on the security of people and countries around the world are decidedly real: ironically, the constraints imposed to protect millions of people on from the COVID-19 are exposing a record number of digital users to cyberattacks. And while the world has learnt ubiquitously how to clean and sanitize hands, faces and door latches, little education and promulgation has been carried out to keep computer and networks safe and secure from cyberattacks. One concomitant of cyberattacks is fake news. On 28th March, the infestation of false information about the virus motivated an intervention of the UN Secretary General in person, issuing a stern warning on this topic.

In the slipstream of COVID-19, organized cybercrime has increased in an unprecedented magnitude and speed. Large-scale fraud campaigns are in circulation, including fake advertisements for medical goods urgently in need. Cyber criminals exploit recklessly the facts that millions of cyber users share their information and their digital behaviour during this time of distress. Predators alike, they lure the ignorant, the novices, dig for loopholes and place traps.

The present edition of Cybersecurity Trends is meant to fill an important information gap in the current discussion of cybersecurity and helps to better understand the current risks and immediate threats in the digital world in the context of COVID-19 and beyond.

My thanks go to Laurent Chrzanovski, his editorial team and to all the authors of the texts published here, for the thematic farsightedness of the current publication and for contributing to a much-needed discussion and international coordination. ■

Disclaimer: The views and opinions expressed by the author are solely his and do not necessarily reflect those of the Swiss Confederation.

NO RISK NO FUN

TIP:

NOBODY KNOWS EXACTLY WHAT IS IN MEDICINES SOLD ON THE INTERNET. THE PRICE AND EASY ACCESSIBILITY GET IN THE WAY OF COMMON SENSE. THERE IS LITTLE THOUGHT OF THE (POSSIBLY FATAL) WORST CASE SCENARIO WHEN CLICKING THE "BUY NOW" BUTTON. SO KEEP YOUR HANDS AND MOUTH AWAY FROM ANY MEDICINES FROM UNLICENSED SOURCES! AND THIS GOES FOR EVERYONE – NOT JUST GRANDPA.

Stories from the Internet, p. 19 © Swiss Confederation

▸▸Use only the original websites of well-known pharmacies or online shops in your country.

To be in compliance with the authorities, do not buy medicines from other countries, including the European Union. The prescription requirements for each individual medicine are very different from country to country, as are the dosages.

The same applies to the purchase of facial masks, medical disinfectants and other health products. The best solution is to physically go to your local pharmacy and order what you need there.

Maximum attention to "antivirus care" messages referring to the antivirus-covid site.(various logs) : once you open the web page, it triggers a very powerful malware called BlackNet on your PC (33). If you have your PC infected, contact the postal police immediately.

5. Confined home? Watch out for your children!

Special attention should be paid to minors. While the schools are closed, cyber criminals are multiplying the invention of new games with malware attached. Furthermore a wave of solicitation attempts towards minors has been reported by the Communications Police (34).

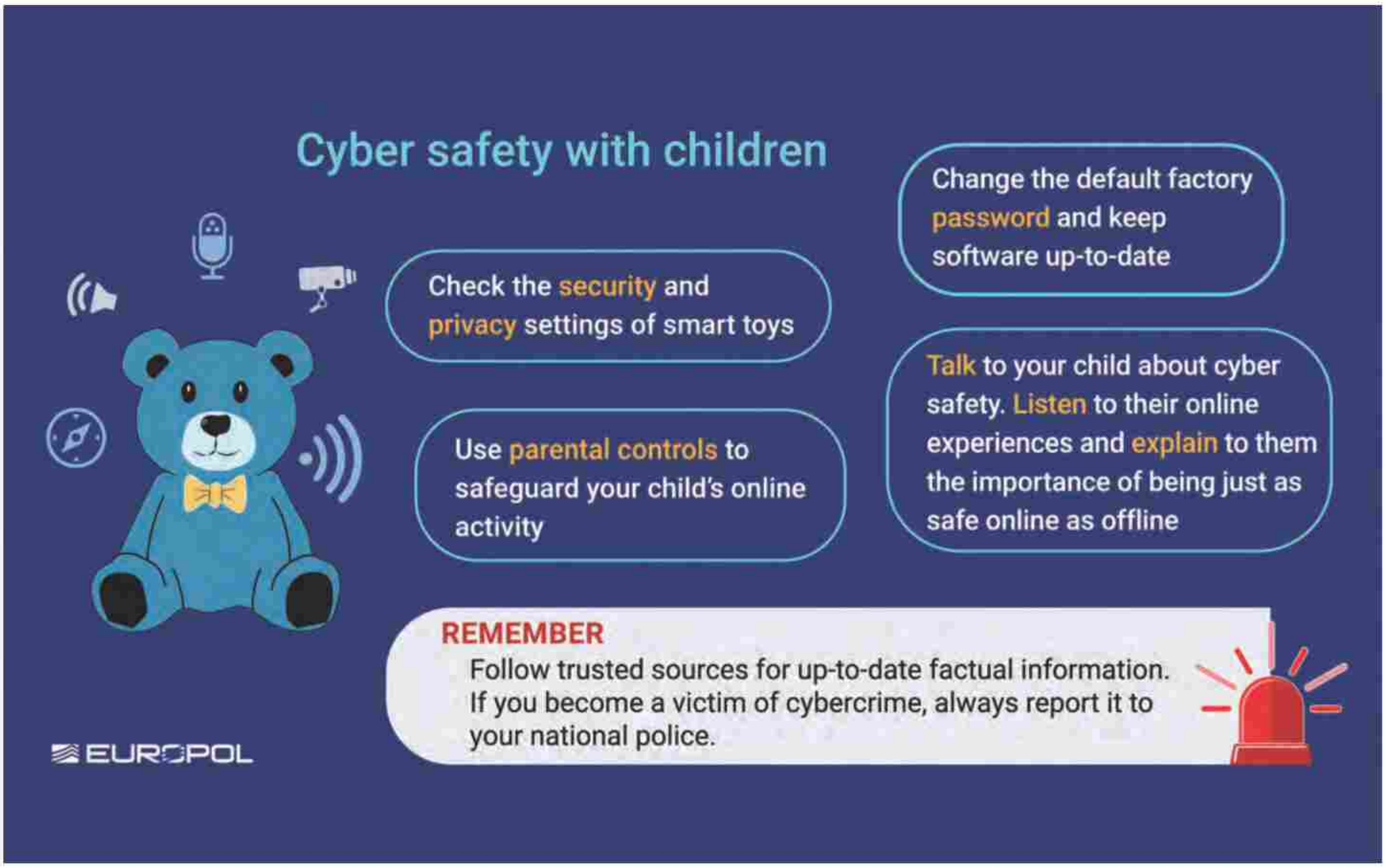
▸▸Use only the original games offered by the various app stores of Smarphone companies and stores licensed to sell Online Games licenses.

A panoply of measures to be taken into account, depending on the age of minors, has been masterfully written by the English PPP GetsafeOnline, with tutorials made in the form of short videos and clips, easy to understand and tailored to the current situation, *"Keepingchildrensafe online during the Coronavirus outbreak"* (35).

6. Confined home? Watch out for your moments of fun and shopping!

We are witnessing a generalized assault on video streaming platforms - a powerful zero-day even interrupted *Google Play* for an hour before it was defeated - and pop-up/invasive advertisements and scams, that refer to criminal sites that offer whole months of free movie and game packages, complete with... credit card to sign up, are multiplying.

The exponentialincrease of phishing emails, with false commercial offers of all kinds,isnoteworthy, although they remain easier to find because they are generally full of grammatical errors - in "minor" languages - or generic phrases. However, the user's mistrust is sometimes put to the test. Just like it happened in Romania, national case reported by CERT-RO (see figure below) (36). The ergonomics of the email, the positioning of the logos of the large German supermarket chain and, above all, the name of the trap-site have been particularly well studied: the address is that of the multinational company (Kaufland.com) to which, however, "-bon" (voucher) has been added and, above all, the final register of the site (.club).



The fake website imitating the original Kaufland website © CERT-RO

▸▸Do not buy anything that is offered to you by e-mail by clicking on the integrated link

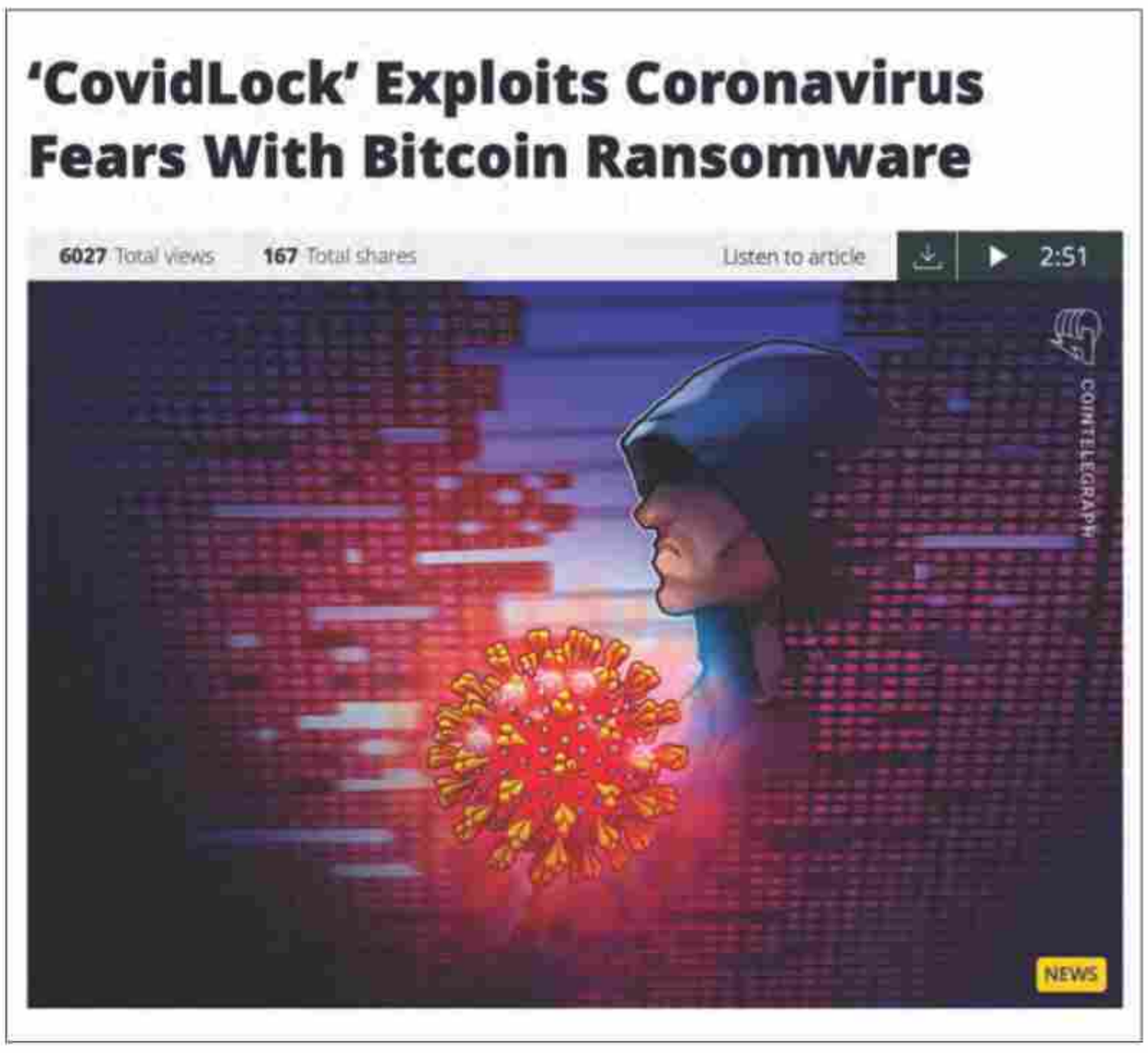
Even if you are perfectly familiar with the sites of the shops that you are a customer of and where you have an account, as a precautionary measure, do not click on the offers received, even legitimate offers, of the same shops: you will find them once you have logged in to the official website.

7. Confined home? Beware of any bank / financial offer!

In Italy, as in almost all European countries, there is a massive proportion of phishing which is linked to the financial world. The e-mails include incredible offers such as high credits at zero interest rates, moratorium on mortgage instalments, repayment of percentages of money if you use this "new instrument" etc., as has been very well summarized by the Communications Police (37).

▸▸Do not buy anything that is offered to you by e-mail by clicking on the integrated link

Also, watch your bank accounts. Check your account balance often via e-banking. For Bitcoin owners,



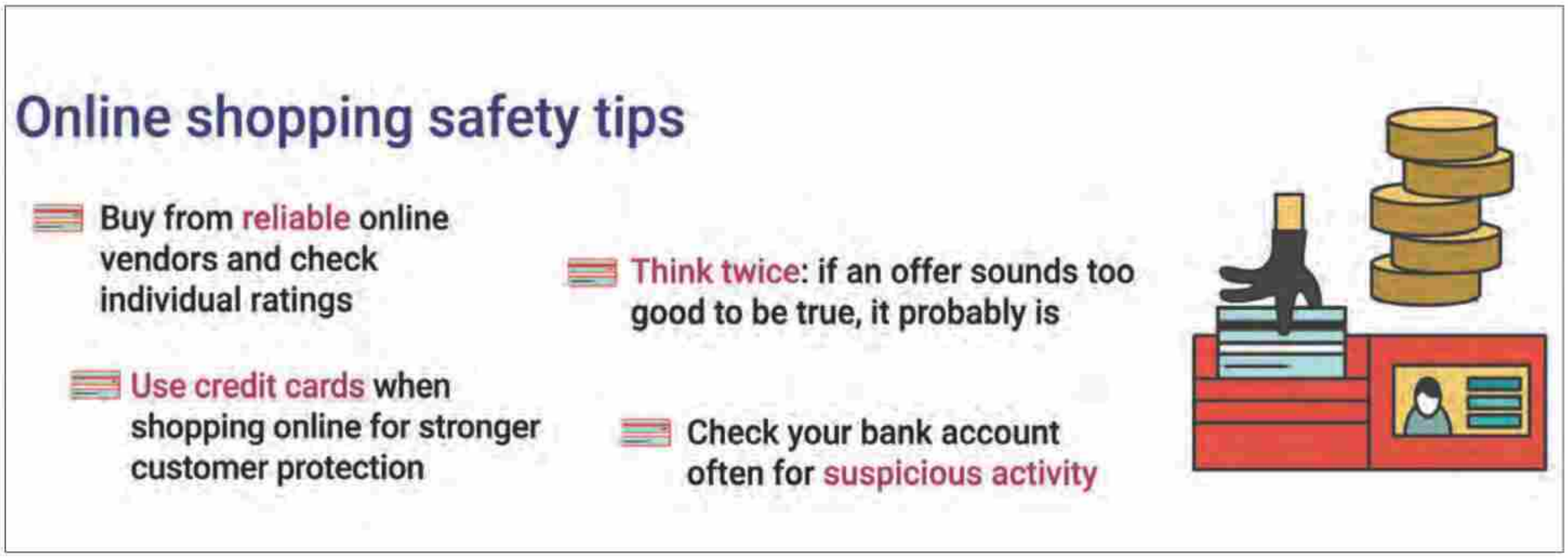
The graph of Haig's article © Cointelegraph

only carry out the necessary transactions: a very powerful ransomware specifically designed for Bitcoin movements is in action (38).

8. Working at home? Watch out for all connected objects!

A lot of companies weren't ready to have all their employees work from home. The protocols for videoconferencing, data access, interaction between the employee's mobile phone and private laptop and the company's central IT infrastructure (and the cloud) are under siege. Suffice it to say that hackers have managed to find a loophole in the iPhones' robust VPNs, now filled by Apple.

Moreover, in "old Europe", fixed networks - excluding optical fiber areas - are almost collapsing in many regions, while the really available speed of mobile networks varies from position to position even in the same neighborhood.



Obviously, this represents the paradise that cybercriminals have been waiting for for a long time not only to saturate the networks even more, but to put in malware and zero days of all kinds, as well as scams. They can even make use of fake phone calls claiming them to be orders from the company they belong to or other companies/clients/suppliers.

▸▸Make sure you have the best of the best when it comes to protection

a) Install and update all antivirus/protections and regularly update the operating systems of all your devices.

b) Cover the video camera / video cameras and microphones of laptops and mobile phones once the professional teleconferencing was over (many teleconferencing systems and protocols were pirated: companies responded with patches - often not installed by SMEs - which in turn were pirated again).

c) Tips for smartphones, tablets and PCs: at the moment the best tips to make your "home office" safe are to be found, in Italian, at the CertFin website (cf. 20) and, for mobile phones and tablets, on the German Intelligence Services page (39). Tip : download the materials and enter the texts on www.deepl.com , the best online translator at the moment for the most important languages.

The guidelines (pdf) of the Canadian Centre for Cyber Security (40) and those of the IVCAEW (Institute of CharteredAccountants in England and Wales) (41) areproving to bevery useful for a complete digital hygiene, especially for freelancers, but also for simple employees.

For companies and the verification of the effectiveness of the VPN system, it is recommendable to consult the excellent report of Homeland Security which details both threats and solutions (42), as well as all the recommendations of Staysafeonline, category "Business" (n.10).

9. Doctor, medical specialist, hospital manager? You are the most sought-after target!

There is no need here to go into the details of the countless attacks that are targeting healthcare facilities and doctors, and in particular medical equipment. As we have already explained many times, the patient's health data is worth a hundred times more on the black market than the data of a credit card.

Attention, there are not only super-sophisticated attacks: from doctors to nurses to all employees,

anyone working in a hospital's ecosystem is prey to an exponentially greater amount of scams, phishing and other grooming attempts than professionals in other sectors (43).

▸▸Find out from the best

As the medical system in Canada and the United States of America is mostly private, guidelines, alerts and advice

can be found on both government and private sites in these two countries.

We therefore recommend all those working in the digital field in the medical world to go daily to (selected examples): https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations; https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19?utm_source=hp_slideshowtm_medium=webtm_campaign=dhsgov; www.healthcareitnews.com; https://healthitsecurity.com/

Where will we go?

On an optimistic note, we hope that citizens and governments will learn the right lessons from what is happening. As Yuval Noah Harari (no. 5) wrote, *"Humanity needs to make a choice. Will we walk the path of disunity or will we adopt the path of global solidarity? If we choose disunity, this will not only prolong the crisis, but will probably lead to even worse catastrophes in the future. If we choose global solidarity, it will be a victory not only against the coronavirus, but against all future epidemics and crises that could assault humanity in the 21st century."*It is now up to each of us to make the right choices and set an example. ■

NOTES :

(1) Giorgio Agamben, Reflections on the plague, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste)

(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/ ; ed: we propose here an excerpt in Italian from the CNN interview during which Harari took up most of the topics of his article https://it.gariwo.net/educazione/yuval-noah-harari-sull-emergenza-covid19-21870.html).

(3) Translation (author) of two final paragraphs by Michel Onfray, Berezina, in Les Observateurs, 17.03.2020)

(4) Translation (author) of a paragraph by SlavojŽižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plaît ! in Le Nouvel Observateur, 18.03.2020 (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)

(5) Yuval Noah Harari, The World, after the Coronavirus, in Optimists and Rational, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/)

(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

(7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

(8) https://www.csa.gov.sg/singcert

(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html

(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/

(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049

(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

(14) Ravie Lakshmanan: Hackers Created Thousandsof Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

(15) Salvatore Lombardo: The alarm: Coronavirus, increasing cyber attacks, phishing and malspam: advice to defend oneself, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

(16) Europol REPORT: PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS (pdf) https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

(17) Subdomenio COVID of INCIBE (Instituto nacional de Ciberseguridad) https://www.incibe.es/cibercovid19

(18) Cert Public Administration, COVID page: https://www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/

(19) Agency for Digital Italy, COVID page: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/27/coronavirus-difendersi-malware-truffe-online

(20) CertFin, COVID page: https://www.certfin.it/newsroom/rendi-la-tua-casa-una-cyber-fortezza/

(21) Italian Association of Clinical Engineers, COVID page: http://www.aiic.it/covid19/

(22) Communications Police: Coronavirus: Minister Lucia Azzolina reports false document of the Ministry of Education, 21.03.2020 https://www.commissariatodips.it/notizie/articolo/coronavirus-il-ministro-lucia-azzolina-denuncia-falso-documento-del-ministero-dellistruzione/index.html

(23) Tarik Saleh, CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware, in Domaintools, 13.03.2020 - with additional link containing full technical description of the malware https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#

(24) Kyle Bradshaw, World Health Organization to launch COVID-19 tips app for Android, iOS, in 9to5Google, 26.03.2020 https://ww.9to5google.com/2020/03/26/world-health-organization-covid-19-app/#

(25) Elena Tebano, Coronavirus, ready the Italian app to trace the contagions: „So we can stop the epidemic", in Corrieredella Sera, 20.03.2019 https://www.corriere.it/tecnologia/20_marzo_18/coronavirus-pronta-app-italiana-tracciare-contagi-cosi-possiamo-fermare-l-epidemia-c6c31218-6919-11ea-913c-55c2df06d574.shtml?refresh_ce-cp

(26) https://innovaperlitalia.agid.gov.it/home/

(27) Andrea Nepori, SOS Italy, here is how the app for the monitoring of the epidemic could be, in La Stampa, 26.03.2020 https://www.lastampa.it/tecnologia/news/2020/03/25/news/sos-italia-ecco-come-potrebbe-essere-l-app-per-il-monitoraggio-dell-epidemia-1.38636482

(28) Communication Police : Coronavirus: Beware of false fundraisingcampaigns ! https://www.commissariatodips.it/notizie/articolo/coronavirus-attenzione-alle-false-campagne-di-raccolta-fondi/index.html

(29) https://www.who.int/about/communications/cyber-security

(30) Communications Police : Coronavirus: BlackNET: RAT distributed via fake „Corona Antivirus". https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(31) Communications Police : Coronavirus : false insuranceproposals for coverage by COVID-19 https://www.commissariatodips.it/notizie/articolo/coronavirus-false-proposte-assicurative-per-la-copertura-da-covid-19/index.html

(32) Internet Stories. Federal Office of Communications OFCOMFederal Office of Consumer AffairsOFCOMFederal Data Protection and TransparencyCommissionerFDPIC Coordination Unit for Combating Internet Crime CYCOReporting and Analysis Centre for Information Assurance MELANIAvailable and downloadable online at: https://www.websters.swiss/it/

(33) Communications Police : BlackNET: RAT distributed via fake „Corona Antivirus". https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(34) Communications Police : Coronavirus : risk of solicitation of minors online https://www.commissariatodips.it/notizie/articolo/coronavirus-rischio-adescamento-minori-online/index.html

(35) Keepingchildrensafe online during the Coronavirus outbreak https://www.getsafeonline.org/news/keeping-children-safe-online-during-the-coronavirus-outbreak/

(36) Continuă valul de campanii de tip scam. Atacatorii se folosescacum de imagineaMega Image https://cert.ro/citeste/alerta-scam-kaufland-ikea

(37) Communications Police : Coronavirus : smishingwith false messages fromcredit institutions https://www.commissariatodips.it/notizie/articolo/coronavirus-smishing-con-falsi-messaggi-di-istituti-di-credito/index.html

(38) Samuel Haig, 'CovidLock' Exploits Coronavirus FearsWith Bitcoin Ransomware, in Cointelegraph, 14.03.2020 https://cointelegraph.com/news/covidlock-exploits-coronavirus-fears-with-bitcoin-ransomware

(39) EffectivelyprotectBSI-BUND, smartphone and tablet https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

(40) Canadian Centre for Cyber Security, Cyber Hygiene for COVID-19 https://cyber.gc.ca/sites/default/files/publications/Publication-COVID-19-e.pdf

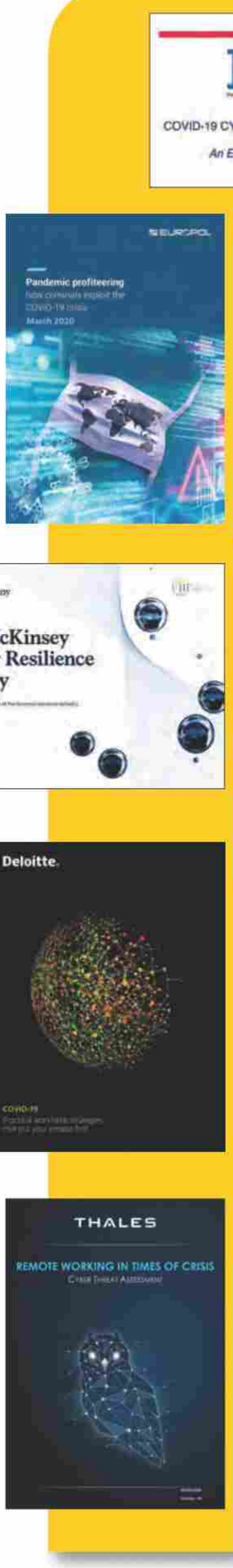
(41) IVCAEW (Institute of CharteredAccountants in England and Wales), Coronavirus guide: cyber hygiene and data https://www.icaew.com/-/media/corporate/files/technical/information-technology/tech-faculty/coronavirus-guide-cyber-hygiene-and-data.ashx

(42) CISA (U.S. Department of Homeland Security) : Alert (AA20-073A) Enterprise VPN Security https://www.us-cert.gov/ncas/alerts/aa20-073a

(43) Gareth Corfield, Health workers are top of phishers' target lists thanks to data value, in The Register, 16.03.2020 https://www.theregister.co.uk/2020/03/16/proofpoint_interview/

V. Resources, useful links, State recommendations

Resources



Selected most recent reports in English:

Europol (EC3): Pandemic Profiteering: how Criminals exploit the COVID-19 Crisis (27.03.2020)

Document is available at: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

(Fully reproduced at the end of the volume) Joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Advisory: COVID-19 exploited by Malicious Cyber Actors (April 2020)

Document is available at: https://www.ncsc.gov.uk/files/Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20V1.pdf

European Cyber Security Organization, *COVID-19 CYBERSECURITY RESPONSE PACKAGE. An ECSO Cyber Solidarity* Campaign (April 2020) (gathering an impressive list of links and useful resources by companies and State Agencies Europe-wide)

Document is available at: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

McKinsey &Co, *The cybersecurity posture of financial-services companies: IIF/McKinsey Cyber Resilience Survey* (April 2020)

Document is available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-cybersecurity-posture-of-financial-services-companies-iif-mckinsey-cyber-resilience-survey?cid=eml-app

PWC, Managing the Impact of COVID-19 on Cyber Security (20.03.2020)

Document is available at: https://www.pwc.co.uk/cyber-security/pdf/impact-of-covid-19-on-cyber-security.pdf

Deloitte, *COVID-19 Practical workforce strategies that put your people first* (April 2020)

Document is available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-workforce-strategies-that-put-your-people-first.pdf

Insikt Group, *Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide* (13.03.2020)

Document is available at: https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

Thales Group, *Remote Working in Times of Crisis - Cyber Threat Assessment* (03.04.2020)

Thales Group, *COVID-19 - Cyber Threat Assessment* (24.03.2020)

Both documents are available at: https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/covid-19-new-weapon-cyber

Resources - Cybersecurity Trends

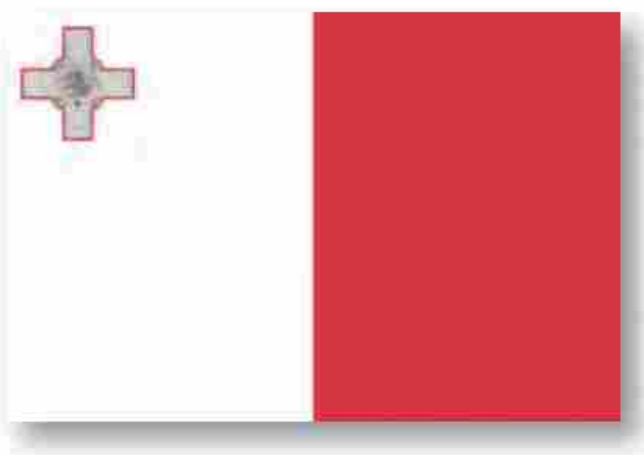
Helpful State resources for each country:

UNITED KINGDOM

Report phishing: phishing@hmrc.gov.uk
Report fraud/attack: https://www.actionfraud.police.uk/
https://www.gchq.gov.uk/ (Government Communications Headquarters)
https://www.ncsc.gov.uk/ (National Cyber Security Centre)
www.getsafeonline.org (Kids + Adults + Businesses special website : advices, tips, and much more)
https://www.getsafeonline.org/news/uk-most-targeted-nation-for-covid-19-spam-email/ (on coronavirus spams)
https://www.getsafeonline.org/coronavirus/ (on coronavirus with tips and more materials)

REPUBLIC OF IRELAND

Report an incident: https://www.ncsc.gov.ie/incidentreporting/
https://www.ncsc.gov.ie/ (National Cyber Security Centre)
https://www.ncsc.gov.ie/pdfs/COVID19Advice.pdf (cybersecurity basics)
https://www.ncsc.gov.ie/pdfs/WFH-Advisory.pdf (working home)
https://cybersafeireland.org (Kids + Adults + Businesses special website : advices, tips, and much more)



REPUBLIC OF MALTA

Report an incident: https://www.mfsa.mt/firms/enforcement/report-a-breach/
https://cybersecurity.gov.mt (Malta's National Cybersecurity Center)

AUSTRALIA

Report spam: https://www.acma.gov.au/stop-getting-spam
Report scam: https://www.scamwatch.gov.au/report-a-scam
Report incident, fraud, attack : https://www.cyber.gov.au/report
https://www.cyber.gov.au/ (Australian Cyber Security Centre)
https://www.cyber.gov.au/COVID-19 (on coronavirus with tips and more materials)
www.staysmartonline.gov.au (Kids + Adults + Businesses special website : advices, tips, and much more)

NEW ZEALAND

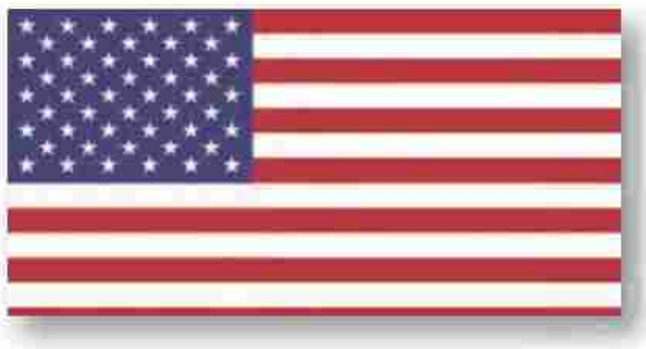
Report spam: https://www.reportspam.co.nz/
Report scams, fraud, incidents: https://www.cert.govt.nz/individuals/report-an-issue/
www.ncsc.govt.nz (New Zealand›s National Cyber Security Centre)
www.cert.govt.nz (Govermental CERT) (Kids + Adults + Businesses special website: advices, tips, and much more)
https://www.ncsc.govt.nz/newsroom/covid-19-useful-cybersecurity-resources/ (coronavirus resources guide)
https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/?gclid=EAIaIQobChMIs963_4__6AIVjg8YCh3jEAKrEAAYASAAEgK8ofD_BwE (coronavirus special guide)

REPUBLIC OF INDIA

Report any type of incident: National Cyber Crime Reporting Portal : https://cybercrime.gov.in/
Report phising: https://www.incometaxindia.gov.in/Pages/report-phishing.aspx
ww.cert-in.org.in (Indian National CERT) (Kids + Adults + Businesses special website: advices, tips, and much more)
https://www.cyberswachhtakendra.gov.in/ (Botnet Cleaning and Malware Analysis Centre)

CANADA

Report spam: https://www.fightspam.gc.ca/eic/site/030.nsf/frm-eng/MMCN-9EZV6S
Report phishing/fraud/incident :https://www.antifraudcentre-centreantifraude.ca/report-signalez-eng.htm
www.cyber.gc.ca (Canadian Centre for Cyber Security)
https://cyber.gc.ca/en/news/staying-cyber-healthy-during-covid-19-isolation (on coronavirus with tips and more materials)
www.getcybersafe.gc.ca (Kids + Adults + Businesses special website : advices, webinars, and much more)
www.getcybersafe.gc.ca/cnt/blg/pst-20200415-en.aspx (advices, tips, and much more)



UNITED STATES OF AMERICA

Report any type of incident/fraud etc. (reproduced hereafter): https://www.us-cert.gov/report
https://www.us-cert.gov/ncas/alerts/aa20-099a (on coronavirus)
https://www.dhs.gov/topic/cybersecurity (Department of Homeland Security)
https://www.cisa.gov/ (Cybersecurity and Infrastructure Security Agency)
www.staysafeonline.org (Kids + Adults + Businesses special website: advices, tips, and much more)
https://staysafeonline.org/covid-19-security-resource-library/ (coronavirus special resource page)

I. Prefaces of our partners

Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to

systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

Threat Response

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces:
http://www.fbi.gov/contact-us/field

Internet Crime Complaint Center (IC3):
http://www.ic3.gov

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):
http://www.secretservice.gov/contact/field-offices

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

---

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or
https://www.ice.gov/webform/hsi-tip-form

HSI Field Offices: https://www.ice.gov/contact/hsi

HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes

Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

Asset Response

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov

United States Computer Emergency Readiness Team:
http://www.us-cert.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

If there is an immediate threat to public health or safety, the public should always call 911.

National Cyber Security Centre
a part of GCHQ

CISA
CYBER+INFRASTRUCTURE

Advisory: COVID-19 exploited by malicious cyber actors

Version 1.0

8th April 2020

This is a joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Introduction

This advisory provides information on exploitation by cyber criminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

COVID-19 exploitation

An increasing number of malicious cyber actors are exploiting the current COVID-19 pandemic for their own objectives. In the UK, the NCSC has detected more UK government branded scams relating to COVID-19 than any other subject. Although, from the data seen to date, the overall levels of cyber crime have not increased both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

APT groups and cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails. This advisory provides you with an overview of COVID-19 related malicious cyber activity. It offers practical advice that individuals and organisations can follow to reduce the risk of being affected. The IOCs provided within the accompanying .csv and .stix files of this advisory are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation.

Summary of attacks

APT groups and cyber criminals are exploiting the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and information operations.

Cyber criminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cyber criminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution using coronavirus or COVID-19 themed lures
- Registration of new domain names containing coronavirus or COVID-19 related wording
- Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.

Social engineering techniques

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
    - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device.[1]
- Open a file (such as an email attachment) which contains malware.
    - For example, email subject lines contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).'

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other examples purport to be from an organisation's human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus or COVID-19 related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."

Note: A non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files linked to this advisory.

[1] https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/

Phishing

The NCSC and CISA have both observed a large volume of phishing campaigns which use the social engineering techniques described above.

Examples of phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails will contain a call to action encouraging the victim to visit a URL that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information and other personal information.

SMS Phishing

Most phishing attempts come by email but the NCSC and CISA have observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives, including government payments and rebates (such as a tax rebate) as part of the lure. Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages.

For example, a series of SMS messages uses a UK government themed lure to harvest email, address, name, and banking information. These SMS messages, purporting to be from 'COVID' and 'UKGOV,' (see figure 1) includes a link directly to the phishing site (see figure 2).

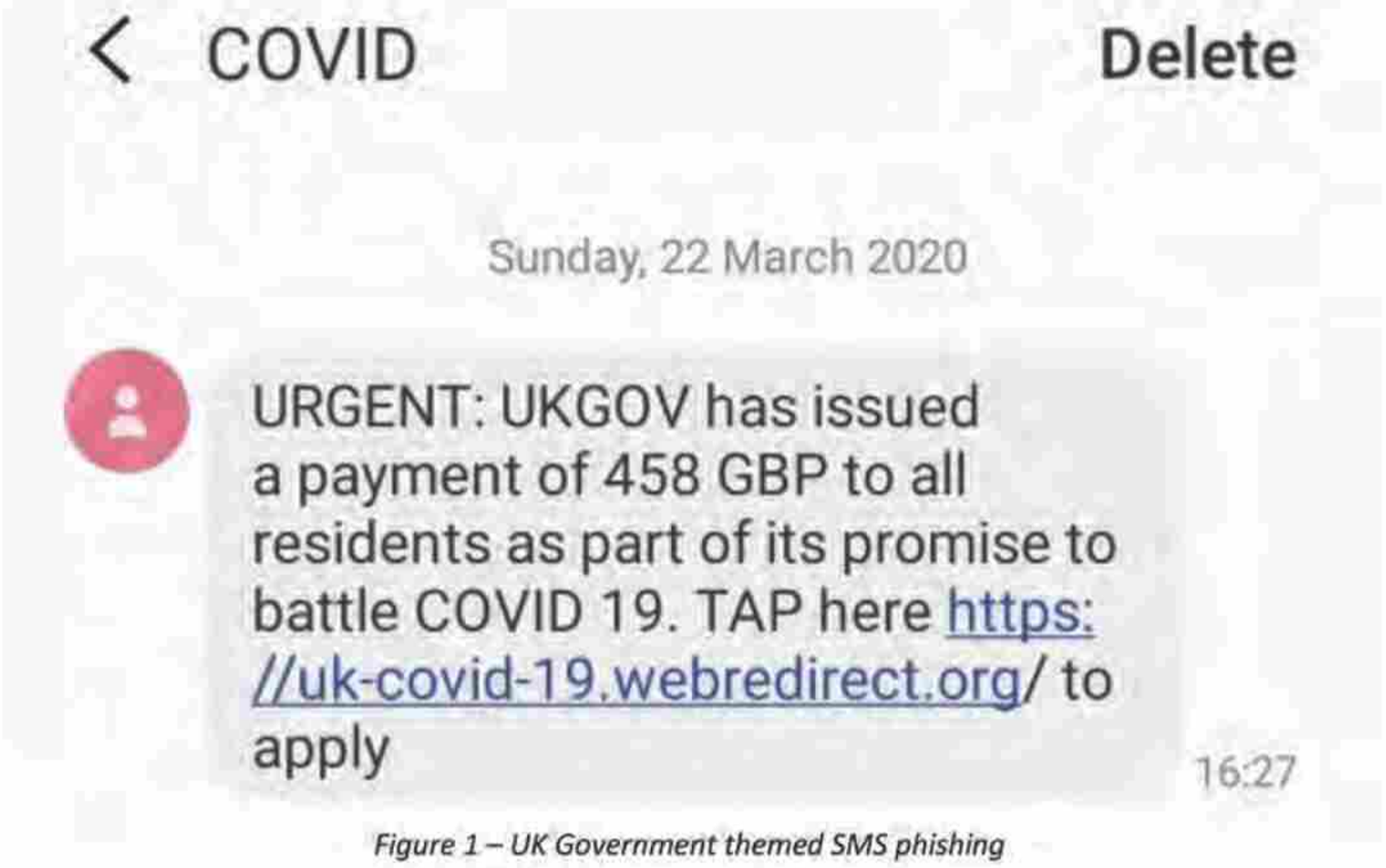


Figure 1 – UK Government themed SMS phishing

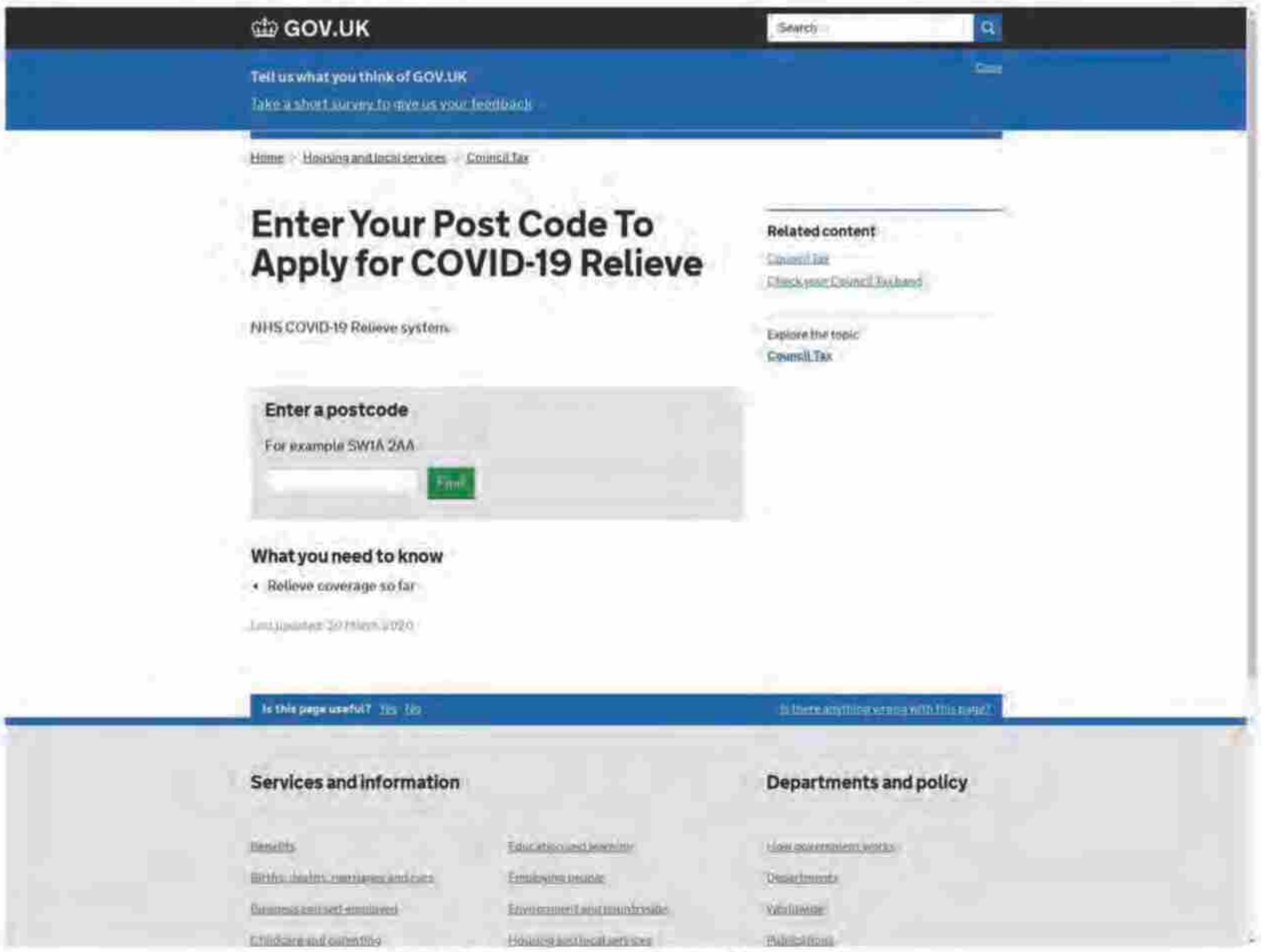


Figure 2 - UK Government themed phishing page

As this example demonstrates, malicious messages can arrive by methods other than email. In addition to SMS, possible channels include WhatsApp and other messaging services. Malicious cyber actors are likely to continue using financial themes in their phishing campaigns. Specifically, it is likely that they will use new government compensation schemes responding to COVID-19 as themes in phishing campaigns.

Phishing for credential theft

A number of actors have used COVID-19 related phishing to steal user credentials. These emails will include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.

If the user clicks on the hyperlink, a spoofed login webpage appears which includes a password entry form. These spoofed login pages may relate to a wide array of online services including - but not limited to - email services provided by Google or Microsoft, or services accessed via government websites.

To further entice the recipient, the websites will often contain COVID-19 related wording within the URL (for example, 'corona-virus-business-update,' 'covid19-advisory' or 'cov19esupport'). These spoofed pages are designed to look legitimate or

accurately impersonate well-known websites. Often the only way to notice malicious intent is through observing the website URL. In some circumstances, malicious cyber actor specifically customise these spoofed login pages for the intended victim.

If the victim enters their password on the spoofed page, the attackers will be able to access the victim's online accounts such as their email inbox. This access can then be used to acquire personal or sensitive information, or to further disseminate phishing emails, using the victim's address book.

Phishing for malware deployment

A number of threat actors have used COVID-19 related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked web page. When they open the attachment the malware is executed, compromising the victim's device.

For example, the NCSC has observed various email distributed malware which deploys the Agent Tesla keylogger malware. The email appears to be sent from Dr Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO). This email campaign began on Thursday, March 19, 2020. Another similar campaign offers thermometers and face masks to fight the epidemic. The email purports to attach images of these medical products but instead contains a loader for Agent Tesla.

In other campaigns, emails included an Excel attachment (e.g. '8651 8-14-18.xls') or contained URLs linking to a landing page that – if clicked - redirects to download an Excel document such as 'EMR Letter.xls.' In both cases, the Excel file contains macros that, if enabled, execute an embedded dynamic-link library (DLL) to install the Get2 loader malware. Get2 loader has been observed loading the GraceWire Trojan.

The TrickBot malware has been used in a variety of COVID-19 related campaigns. In one example, emails target Italian users with a document purporting to be information related to COVID-19 (see figure 3). The document contains a malicious Macro which downloads a batch file (BAT) which launches JavaScript, which - in turn - pulls down the TrickBot binary, executing it on the system.

Figure 3 – Email containing malicious macro targeting Italian users[2]

In many cases, Trojans - such as Trickbot or GraceWire2 - will download further malicious files such as Remote Access Trojans (RATs), desktop-sharing clients and ransomware. In order to maximise the likelihood of payment, cyber criminals will often deploy ransomware at a time when organisations are under increased pressure. Hospitals and health organisations in the United States,[3] Spain[4] and across Europe[5] have all been recently affected by ransomware incidents.

As always, you should be on the lookout for new and evolving lures. Both the NCSC[6] and CISA[7,8] provide guidance on mitigating malware and ransomware attacks.

Exploitation of new home working infrastructure

Many organisations have rapidly deployed new networks, including VPNs and related IT infrastructure, to cater for the large shift towards home working.

Malicious cyber actors are taking advantage of this on this mass move to home working by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, the NCSC and CISA have

---

[2] https://www.bleepingcomputer.com/news/security/trickbot-malware-targets-italy-in-fake-who-coronavirus-emails/

[3] https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/

[4] https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware

[5] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/

[6] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[7] https://www.us-cert.gov/ncas/tips/ST18-271

[8] https://www.us-cert.gov/Ransomware

observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability (CVE-2019-19781) and its exploitation has been widely reported online, since early January 2020. Both the NCSC[9] and CISA[10] provide guidance on CVE-2019-19781 and continue to investigate multiple instances of this vulnerability's exploitation.

Similarly known vulnerabilities affecting VPN products from vendors Pulse Secure, Fortinet and Palo Alto continue to be exploited. CISA provides guidance on the Pulse Secure vulnerability[11] and the NCSC provides guidance on the vulnerabilities in Pulse Secure, Fortinet, and Palo Alto.[12]

Malicious cyber actors are also seeking to exploit the increased use of popular communications platforms (such as Zoom or Microsoft Teams) by sending phishing emails that include malicious files with names such as 'zoom-us-zoom_##########.exe' and 'microsoft-teams_V#mu#D_##########.exe' (# representing various digits that have been reported online).[13] The NCSC and CISA have also observed phishing websites for a number of popular communication platforms. In addition, attackers have been able to hijack teleconference and online classrooms that have been set up without security controls (e.g. passwords) or with unpatched versions of the communications platform software.[14]

The surge in home working has also led to an increase in the use of Microsoft's Remote Desk Protocol (RDP). Attacks on unsecured RDP endpoints (i.e. exposed to the internet) are widely reported online,[15] and recent analysis[16] has identified a 127% increase in exposed RDP endpoints. The increase in RDP use could potentially make IT systems, without the right security measures in place, more vulnerable to attack.[17]

Indicators of compromise

The NCSC and CISA are working with law enforcement and industry partners to disrupt or prevent these malicious COVID-19 themed cyber activities. We have published a non-exhaustive list of COVID-19 related IOCs via the following links:

- CSV file: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.csv
- Stix File: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.stix.xml

---

[9] https://www.ncsc.gov.uk/news/citrix-alert
[10] https://www.us-cert.gov/ncas/alerts/aa20-031a
[11] https://www.us-cert.gov/ncas/alerts/aa20-010a
[12] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities
[13] https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/
[14] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
[15] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ and
[16] https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work
[17] https://www.us-cert.gov/ncas/tips/ST18-001

The importance of repositioning - positively - the human as an actor of cybersecurity.

Centre de recherche de l'EOGN

FIC — FORUM-FIC.COM —

Author: **General Marc Watin-Augouard**

The crisis triggered by COVID-19 will undoubtedly accelerate the digital transformation for the better rather than the worse. Predators have realized that the context offered them an opportunity to migrate with all their skills into the digital space, which has no containment measures. They will stay there! Honest Internet users have never used, daily, so many applications and so long, in particular, because of the massive recourse to teleworking, but also for their need to maintain human contacts despite "social distancing".

Tomorrow, we will probably see the territories reshaping themselves, with a great return to the "countryside", more resilient than the cities, provided that very high-speed broadband will be available. Tomorrow, the contributions of 5G, Big Data and AI will encourage new uses, particularly for telemedicine, epidemic prediction and deployment. Tomorrow, remotely controlled robots will enable teleworking for those who are today "on the front line", to deliver products to protect vulnerable people. But nothing can be done without a quest for meaning! "Putting the human back in the very heart of cybersecurity" is not an option among others; it is a requirement! Cybersecurity, more than ever, must be at the service of freedom. We know how dear it is to us and how it must be defended against those who have other conceptions of mankind.

Cybersecurity has been built up in successive layers. The control of data "processing" (1978) was followed by the protection of automated data processing "systems" (1988) and finally by the protection of "data", which was placed at the centre of the digital ecosystem (2018). Personal data has always been the object of particular vigilance, but never has their sensitivity been so highlighted, due to the exponential growth of platforms, applications and connected systems that "reformat" our society at such an incredible pace that it is often imperceptible to our senses. More than ever, our data can characterize us, reveal our intimacy, penetrate the sphere and the secrets of our private life, without which there is no freedom. More than ever, profiled by algorithms, the human being is no longer the master and tends to become a subject, at the risk of ending up being a slave. However, nothing is lost, because mastering the digital transformation requires above all a mobilization of skills, a shared acculturation to the challenges of the new world. Build around all those topics, too often left to specialists and experts, cybersecurity must, in fact, be the fruit of an individual and collective stance resulting from a widely disseminated education starting from the earliest age. Too often identified as a field reserved for men, cybersecurity must also be carried by women, who today account for only 10% of the jobs in

In addition, there are a number of useful resources online, which provide details of COVID-19 related malicious cyber activity:

- Recorded Futures' report, Capitalizing on Corona Panic, Threat Actors Target Victime worldwide
- DomainTools' Free COVID-19 Threat List – Domain Risk Assessments for Coronavirus Threats
- GitHub list of IOCs used in COVID-19 related cyberattack campaigns, gathered by GitHub user, Parth D. Maniar
- GitHub list of Malware, spam, and phishing IOCs that involve the use of COVID-19 or coronavirus gathered by SophosLabs
- Reddit master thread to collect intelligence relevant to COVID-19 malicious cyber threat actor campaigns
- Tweet regarding the MISP project's dedicated #COVID2019 MISP instance to share COVID-related cyber threat information

Conclusion

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19 related information as an opportunity to deliver malware and ransomware and to steal user credentials. Individuals and organisations should remain vigilant. For genuine information about the virus, please use trusted resources such as the UK government website[18], Public Health England[19] or NHS websites[20].

Mitigating the risk

Following the NCSC and CISA advice set out below should help mitigate the risk to individuals and organisations from malicious cyber activity related to both COVID-19 and other themes:

- NCSC guidance for the public to help them spot, understand and deal with suspicious messages and emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- NCSC phishing guidance for organisations and cyber security professionals: https://www.ncsc.gov.uk/guidance/phishing
- NCSC guidance on mitigating malware and ransomware attacks: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- NCSC guidance on home working: https://www.ncsc.gov.uk/guidance/home-working

[18] https://www.gov.uk/coronavirus
[19] https://www.gov.uk/government/organisations/public-health-england
[20] https://www.nhs.uk/conditions/coronavirus-covid-19/

- NCSC guidance on End User Device security: https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns
- CISA guidance for defending against COVID-19 cyber scams: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
- CISA Alert (AA20-073A) on enterprise VPN security: https://www.us-cert.gov/ncas/alerts/aa20-073a
- CISA website providing a repository of the agency's publicly available COVID-19 guidance: https://www.cisa.gov/coronavirus

Phishing guidance for individuals

The NCSC's suspicious email guidance explains what to do if you've already clicked on a potentially malicious email, attachment or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take (such as changing your passwords). It also offers NCSC's top tips for spotting a phishing email:

- **Authority** - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing guidance for organisations and cyber security professionals

Organisational defences against phishing often rely exclusively on users being able to spot phishing emails. However, you should widen your defences to include more technical measures. This will improve your resilience against phishing attacks.

In addition to educating users on defending against these attacks, you should consider NCSC's guidance for organisations that splits the mitigations into four layers, on which you can build your defences:

1. Make it difficult for attackers to reach your users

2. Help users identify and report suspected phishing emails (see CISA Tips, Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams)
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

NCSC and CISA also recommend organisations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimise the damage caused.

Communications platforms guidance for individuals and organisations

Due to COVID-19, an increasing number of organisations and individuals are turning to communications platforms (such as Zoom and Microsoft Teams) for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI March 30, 2020 press release, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Disclaimers

This report draws on information derived from NCSC, CISA and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favouring by CISA.

Is **Cyber Essentials** for you?

Businesses of all shapes and sizes use Cyber Essentials to help protect their IT from attack. You could too.

No matter what your organisation does, Cyber Essentials can help to keep the devices and data you rely on safe.

We understand that not everyone has a dedicated IT department, or an in-depth knowledge of cyber security.

Cyber Essentials has been designed to be flexible, taking into account all types and sizes of organisation.

Certification will reassure current and potential customers that you take cyber security seriously. You'll also be listed in our directory of certified organisations.

CYBER ESSENTIALS

Further information

Information online that will help you secure your IT against cyber attack.

www.cyberessentials.ncsc.gov.uk

www.ncsc.gov.uk/smallbusiness

www.ncsc.gov.uk/charity

www.ncsc.gov.uk/guidance/10-steps-cyber-security

www.iasme.co.uk/cyberessentials

National Cyber Security Centre
a part of GCHQ

IASME CONSORTIUM

CYBER ESSENTIALS

Protect your organisation against the most common cyber attacks

To find out more please visit
www.cyberessentials.ncsc.gov.uk

National Cyber Security Centre
a part of GCHQ

IASME CONSORTIUM

What is **Cyber Essentials?**

Cyber Essentials is a simple and effective Government backed scheme that will help you protect your organisation against a range of the most common cyber attacks.

From the small scale startup to the established and growing business, Cyber Essentials will help you avoid the consequences of such things as:

- **Phishing attacks**
- **Malware**
- **Ransomware**
- **Password guessing**
- **Network attacks**

Our advice, in the shape of five technical controls, is easy to implement and designed to guard against these attacks.

Two levels of confidence

The NCSC works in partnership with The IASME Consortium to deliver Cyber Essentials, ensuring that the scheme continues to evolve to meet the cyber security challenges of the future.

- Cyber Essentials self-assessment is a first step towards helping you protect your business from the most common cyber attacks. The process is simple and certification costs around £300.
- Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

For more information about how to get certified visit www.cyberessentials.ncsc.gov.uk

How does **Cyber Essentials** work?

Cyber Essentials sets out five controls which you can implement immediately to strengthen your cyber defences:

1. Use a firewall to secure your internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date

National Cyber Security Centre

Home working:
Managing the cyber risks

Working from home is not new to many of us, but the coronavirus (COVID 19) means organisations are using home working on a greater scale, and for longer periods. This page will help organisations introducing (or scaling up) home working. It also provides advice on spotting COVID-19 scam emails.

Cyber criminals are preying on fears of COVID-19 and sending scam emails. These may claim to have a cure for the virus, offer a financial reward, or might encourage you to donate. If clicked, you're sent to a dodgy website which could download viruses onto your device, or steal your passwords.

Don't click on any such links. For genuine information about the virus, please use trusted resources such as the **Public Health England** or **NHS** websites.

If you've already clicked, don't panic:

- open your antivirus software and run a full scan, following any instructions
- if you've been tricked into providing your password, you should change your passwords on all your other accounts
- if you're using a work device, contact your IT department and let them know
- if you have lost money, you need to report it as a crime to Action Fraud (you can do this by visiting **www.actionfraud.police.uk**)

1. Setting up user accounts & accesses

Set strong passwords for user accounts; use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.

2. Preparing for home working

Think about whether you need new services, or to just extend existing services so teams can still collaborate. NCSC guidance on implementing Software as a Service (SaaS) can help you choose and roll out a range of popular services. In addition:

- **Consider producing 'How do I?' guides for new services so that your help desk staff aren't overwhelmed with requests for help.**
- **Devices are more likely to be stolen (or lost) when home working. Ensure devices encrypt data whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.**
- **Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.**
- **Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.**
- **Staff feeling more exposed to cyber threats when home working should work through the NCSC's Top Tips for Staff e-learning package.**

3. Controlling access to corporate systems

Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the NCSC's VPN Guidance, which covers everything from choosing a VPN to the advice you give to staff.

If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.

4. Helping staff to look after devices

Whether using their own device or the organisation's, ensure staff understand the risks of using them outside the office. When not in use, staff should keep devices somewhere safe.

Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.

Ensure staff understand how to keep software and devices up-to-date, and that they apply updates promptly.

5. Using removable media safely

USB drives may contain sensitive data, are easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:

- **disable removable media using MDM settings**
- **use antivirus tools where appropriate**
- **only permit the use of sanctioned products**
- **protect data at rest (encrypt) on removable media**
- **encourage alternative means of file transfer (such as online tools).**

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Wash your hands of coronavirus scams!

Friends Against Scams aims to protect and prevent people from becoming victims of scams.

Be aware of people offering or selling:

- Virus testing kits - these are only offered by NHS.
- Vaccines or miracle cures – there is currently no vaccine or cure.
- Overpriced or fake goods to protect yourself from coronavirus such as anti-bacterial products.
- Shopping or medication collection services.
- Home cleaning services.

Protect yourself and others:

- Don't be rushed into making a decision. If it sounds too good to be true it probably is.
- Only purchase goods from legitimate retailers and take a moment to think before parting with money or personal information.
- Don't assume everyone is genuine. It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- If someone claims to represent a charity, ask them for ID. Be suspicious of requests for money up front. If someone attempts to pressurise you into accepting a service they are unlikely to be genuine. Check with family and friends before accepting offers of help if you are unsure.

Be a good friend, help to protect your family, friends and neighbours from scams.

Read it.
Share it.
Prevent it.

#Coronavirus
#ScamAware

Friends Against SCAMS

Contact

For advice on scams call the Citizens Advice Consumer Helpline on **0808 223 11 33**

To report a scam call Action Fraud on **0300 123 2040**

Contact your bank if you think you have been scammed.

NATIONAL TRADING STANDARDS
Scams Team

To learn more about the different types of scams visit **www.FriendsAgainstScams.org.uk**

STAYING CYBER-HEALTHY DURING COVID-19

Cyber attackers take advantage of high-profile events, particularly those that cause worry and concern.

The Canadian Centre for Cyber Security offers the following tips to help Canadians stay cyber-healthy during the COVID-19 pandemic.

BEWARE OF UNSOLICITED EMAILS AND TEXTS

COVID-19-related phishing attempts are on the rise.

Cyber attackers try to trick you into clicking on links or attachments so they can infect your device or steal your data.

- **Be cautious if the tone of the message is urgent or threatening**
- **Look for typos** as they are often a sign of a phishing attempt
- **Don't click on links or attachments from senders you don't know**
- **Use trusted anti-malware software**

BEWARE OF FAKES

Fake websites related to COVID-19 are popping up.

Cyber attackers are using fake websites, imitating health agencies or government departments, to spread disinformation or to scam people.

- **Check web addresses for spelling mistakes**
- **Navigate to the page using a search engine** instead of clicking on a provided link
- **Don't submit login credentials or credit card details** unless you are sure the web page is legitimate

WORKING FROM HOME

Cyber attackers are looking to exploit teleworking connections, because so many people are now working outside their organizations' IT security perimeters.

- **Secure your home wireless router** with strong passphrases
- **Do not let family members or others use your telework account**
- **Turn off Wi-Fi, Bluetooth and GPS** when not in use
- **Use trusted anti-malware software**
- **Report suspicious activity** to your IT security team immediately

ATTENTION: HEALTH WORKERS

Good cyber hygiene is extra important for health workers right now.

- Cyber criminals are likely to exploit the extra pressure on health organizations
- Hackers are likely to try to steal sensitive data and research related to COVID-19

GENERAL TIPS

Now is the perfect time to up your overall cyber hygiene game.

- **Create passphrases:** strings of words are stronger than passwords and easier to remember
- **Install software updates right away** as they often contain security patches
- **Use multi-factor authentication to unlock your device** like a PIN **and** a fingerprint
- **Store your data securely:** back up your crucial data and know how to retrieve it
- **Secure your social media and email accounts:** apply all the security and privacy settings

LEARN MORE

These tips are a great place to start. For more information visit: cyber.gc.ca

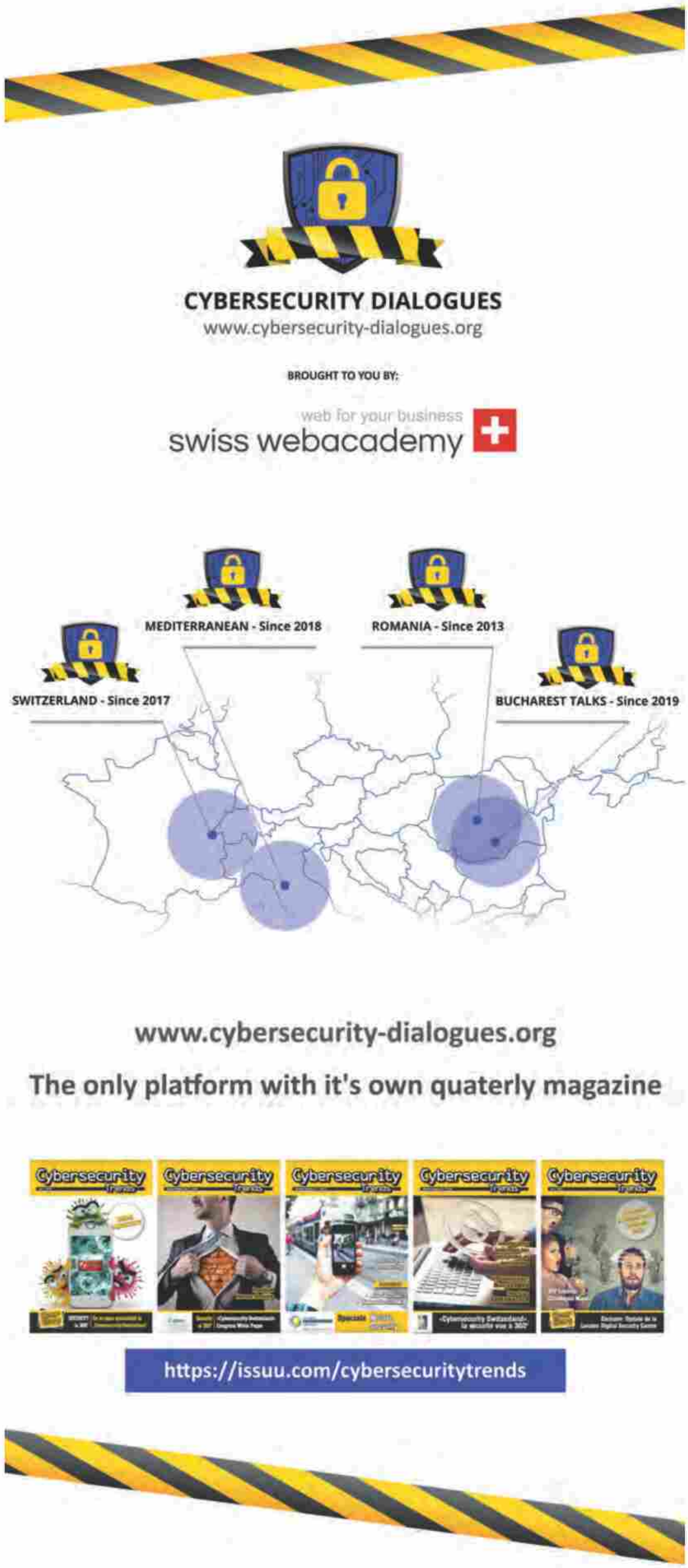
- Spotting Malicious Emails
- Best Practices for Passphrases and Passwords
- Staying cyber safe while teleworking
- Telework Security Issues
- Social Media in the Workplace
- Instant Messaging
- Five practical ways to make yourself cybersafe

FOR MORE INFORMATION ON COVID-19 VISIT

canada.ca/coronavirus or call **1-833-784-4397**

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada



A publication

web for business
swiss webacademy

Redaction:

Laurent Chrzanovski and
Romulus Maier †

Translation and proofreading:

Gabriela Marinescu, Laurent Chrzanovski,
Norman Frankel, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Address:

Swiss Webacademy
Str. Şcoala de Înot nr.18,
550005 Sibiu
Romania
www.swissacademy.eu
www.cybersecurity-dialogues.org

Special webpage to download this issue in French, English and Romanian:

https://swissacademy.eu/cybercovid/

BLOCKAPT

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.

Partner Congresses

CHARENTE-MARITIME CYBER SÉCURITÉ
— CMCS-CONNECT.FR —

CYBERSECURITY PUBLIC - PRIVATE DIALOGUES
— CYBERSECURITY-DIALOGUES.ORG —

FIC
— FORUM-FIC.COM —

Charente Maritime Cyber Sécurité
CMCS2020 - 13, 14 & 15 octobre 2020

OBJECTIFS : L'évolution grandissante des attaques numériques et informatiques nécessitent prévention et sécurisation. Ces cybers attaques sont massives, multiples et incessantes. La gravité de leurs impacts ne fait que s'accroître au fil du temps. C'est une criminalité organisée à l'échelle mondiale tournée vers l'extorsion de fonds. CMCS 2020 traitera des risques économiques et sociaux, notamment sur les populations les plus fragiles. Le tourisme sera l'axe économique qui permettra de pragmatiser le discours. C'est une véritable approche sociétale du cyber monde que nous voulons explorer.

Quels Risques ? : Aujourd'hui, il est facile d'identifier les risques qui nous menacent :

- L'Hyper numérisation des outils, qu'ils soient du quotidien ou professionnels
- L'Hyper connexion des différents éléments de notre vie quotidienne
- L'Hyper information que nous créons dans tous les domaines
- L'Hyper utilisation de l'énergie électrique

INFORMER
SENSIBILISER
FAIRE AGIR

Quelles Parades ?
Les parades sont nombreuses et devront s'appliquer aux 4 types de risques que nous avons identifiés. Mais en aucun cas ces parades ne sauraient nous protéger de façon globale. Nous sommes donc contraints d'adopter un comportement qui visera à renforcer la résilience des systèmes plutôt que leur résistance.

AUSIM
beyond digital

Les #ASSISES de l'AUSIM sont de retour :

Venez vivre avec nous cette édition exceptionnelle!

21-23 OCT 2020
à Marrakech
#AssisesAUSIM2020
Les Assises de l'AUSIM
#SAVE THE DATE#

Réseaux sociaux :
0522 92 83 02/03
contact@ausimaroc.com

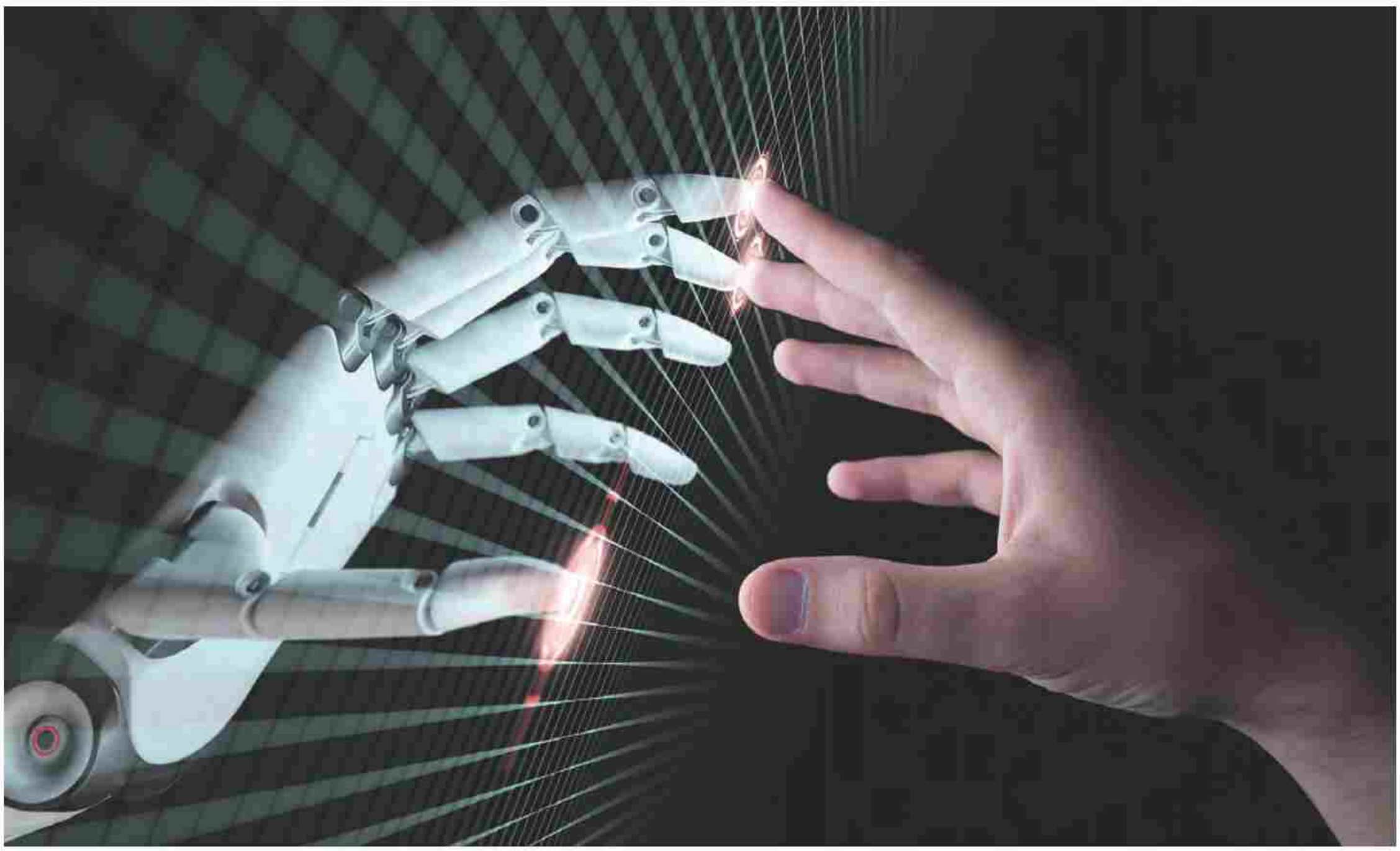
BIO

- Founder and Co-Director, International Cybersecurity Forum - FIC
- Director, Research Centre of the National Gendarmerie Officers School (CREOGN)
- Former Inspector General of the Armed Forces-Gendarmerie
- Army General (2008)
- Lieutenant General (2007)
- Major General (2006)
- Commander, Gendarmerie for the Northern Defence Zone (2005 - 2008)
- Commander, Nord-Pas-de-Calais Gendarmerie Region
- Advisor for the Gendarmerie, Cabinet of Dominique de Villepin (2004 - 2005)
- Brigadier General (2003)
- Security Advisor, Cabinet of Nicolas Sarkozy (2002 - 2004)
- Commander of the Champagne-Ardenne Departmental Gendarmerie Legion (2000 - 2002)
- TEACHING: Lecturer in law, Universities Panthéon-Assas (Paris II), René Descartes (Paris V) and Aix-Marseille III-Méditerranée.

this field, even though they make up more than half of the population. We must, without doubt, consider the use of the newest technologies, such as artificial intelligence, to secure our networks, our exchanges and our data. Above all, however, it is important to reposition - positively - the human as an actor of cybersecurity, when he or she is essentially regarded today as a victim or as a perpetrator, whether voluntary or involuntary, of cyber incidents or cybercrimes.

In our quest for cybersecurity, we are too often waiting for the answer to the question "how?", letting technologies into the role to answer this vital question; we have also neglected the question "why", by demanding achievements set in line with our conception of humanity. *"Science without conscience is the ruin of the soul"*, wrote Rabelais in Pantagruel. This invitation to combine the "hard" sciences and the humanities is needed more than ever. Cybersecurity needs jurists, sociologists, philosophers, historians, etc. to guarantee security for everyone and in the service of the freedom of everyone.

It is time to put the human back into the heart of discourse and action. We know that, without a shared European vision, we will tomorrow have the choice between "supervised freedom" and "supervised security", depending on whether we will be "colonised" by the West or by the East. It is up to Europe to finally have a real political project that aims to ensure "secure freedom", which guarantees the values shared by the 27 Member States. This is an opportunity to bring back life into a digital transformation, overwhelmingly built on materialistic aims. It is the minimal basis for offering to the rest of the world an alternative to the growing imperium of the two digital giants. We have lost the battle of hardware, software and platforms. We can win the human battle. Many Internet users in Europe, "from the Atlantic to the Urals" and in Africa are only waiting for that. ■



Increased cyber attacks in the context of the COVID-19 pandemic

Author: **General Anton Rog**

In the context of the spread of SAR-CoV-2 virus, during March this year, we observed a clear intensification of illegitimate cyber activities directed against some Romanian State Institutions.

Cyber actors, exploiting the pandemic, are interested in launching numerous cyber-attack campaigns to damage and/or block the correct functioning of the targeted systems. The most common types of criminal campaigns led during this period are *ransomware attacks* and *web defacement attacks*.

These campaigns predominantly concerned not only the IT&C infrastructures used and managed by governmental ministries, institutions or bodies responsible for enforcing the measures to mitigate the effects generated by the COVID-19, but also those belonging to private companies active in the domains of health, education and research.

To ensure a high rate of success for their activities, cyber attackers have updated and adapted their operations to the international/national context, diversifying their tactics and techniques. They track the distribution of malware through phishing and/or spear-phishing campaigns, which exploit the general need for information about the state of the spread of COVID-19 and the lack of medical resources.

In addition, to gain their victims' trust, attackers integrate into the email/messages transmitted through phishing and spear-phishing campaigns specific impersonation elements (email addresses, titles, logos, text content) of international and national institutions empowered to deal with the pandemic situation.

The cyber threat is also enhanced by the circulation of a large number of files spread via unofficial channels.

It is expected that the number of cyber-attack campaigns will increase, within the context of the COVID-19 pandemic. Hence, we strongly recommend the adoption of a preventive and precautious behaviour in the digital environment, by not opening emails and attachments from unreliable sources, by using strictly legally-purchased and updated applications and by accessing information only from official sources. ■

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.