2018 no. 31

USTO

d+i developing ideas

LLORENTE & CUENCA

HYPERCONNECTED
and hyper-vulnerable

DEVELOPING IDEAS

Developing Ideas by LLORENTE & CUENCA is a hub for ideas, analysis and trends. It is a product of the changing macroeconomic and social environment we live in, in which communication keeps moving forward at a fast pace.

Developing Ideas is a combination of global partnerships and knowledge exchange that identifies, defines and communicates new information paradigms from an independent perspective. Developing Ideas is a constant flow of ideas, foreseeing new times for information and management.

It is because reality is neither black nor white, Developing Ideas exists.

UNO

UNO is a magazine of Developing Ideas by LLORENTE & CUENCA addressed to clients, professionals, journalists and key opinion leaders, in which firms from Spain, Portugal and Latin America, along with Partners and Directors of LLORENTE & CUENCA, analyze issues related to the field of communication.

UNO

DIRECTION AND COORDINATION:
Developing Ideas by LLORENTE & CUENCA

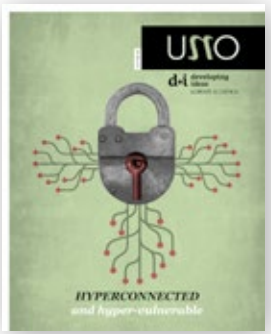
CONCEPT AND GRAPHIC DESIGN:
AR Difusión

ILLUSTRATIONS:
Marisa Maestre

PRINTING:
naturprint.com

Printed in Spain
Madrid, September 2018

WWW.DEVELOPING-IDEAS.COM
WWW.UNO-MAGAZINE.COM



SUMMARY

2018 **no. 31**

4
WHO ***ARE*** OUR ***contributors?***

8
HYPERCONNECTED and hyper-vulnerable

11
THE ***TECHNOLOGICAL intrusion***

14
INSTITUTIONAL ***COMMUNICATIONS*** ON SUBMARINE ***San Juan***

17
FROM ***HYPER-CONNECTIVITY*** TO ***hyper-vulnerability***

20
GOVERNMENT CYBERSECURITY, A ***priority***

23
DEALING WITH ***COMPLEXITY***: IT'S ***normal chaos***

25
ARTIFICIAL INTELLIGENCE TAKES US INTO A ***new era***: *ZERO CLICK*

27
CHALLENGES TO ***SECURITY*** IN DIGITAL ***transformation***

30
SOCIAL MEDIA ACTS LIKE A SELF-CLEANING OVEN FOR ***fake news***

33
"STRATEGIZING" corporate DISPUTES

37
USTO**01**
INTERVIEW WITH CARLOS PADRÓN ESTARRIOL

40
HYPERCONNECTED AND ***HYPER-VULNERABLE***? THE RISKS OF DIGITAL ***MISINFORMATION***

43
COMMUNICATIONS REFLECT ***conscious*** MANAGEMENT

45
HYPER-DISPERSED

47
CYBER-RISK AND CYBERCRIME: THE ***GREAT CHALLENGES*** IN THE CONTEMPORARY ***business*** WORLD

51
IOT: ***INNOVATION***, ***opportunity*** AND ***risk***

54
LITTLE ***TRUTHS*** AND BIG ***lies***

57
THE NEW ***PARADIGM*** FOR ***crisis and risk*** COMMUNICATIONS

61
UNO´S AWARDS

62
LLORENTE & CUENCA

José Antonio Zarzalejos

A permanent **external adviser** at LLORENTE & CUENCA and former general manager of the firm in Spain, Zarzalejos holds a law degree from Deusto University and is a journalist. The former editor-in-chief of *El Correo de Bilbao*, secretary of Vocento and editor-in-chief of *ABC* in Spain, he has been distinguished with several professional awards, including the Mariano de Cavia Award, Federation of Spanish Press Associations award, Javier Godo Award for Journalism and Luca de Tena Award. [Spain]

Enrique Antonio Balbi

Born in Bahia Blanca Aug. 18, 1965, Balbi completed his primary and secondary education in Mar del Plata (Argentina) before graduating from the Military Navy School as Midshipman with a degree in Naval Systems. He went on to study at the Submarine School in 1991. He is now an Operations Analyst who completed a postgraduate course in Disaster Risk Management and holds master's degrees in University Management (pending his thesis) and Organizational Communications Management. He currently holds the rank of Ship Captain and is **head of the Institutional Communications Department, as well as a spokesman for the Argentine Navy**. [Argentina]

Guillermo Vidalón

Vidalon holds a degree in Social Communications from Universidad Nacional Mayor de San Marcos, in Peru, where he graduated from the Centro de Altos Estudios Nacionales. He has written multiple books, including *Minería, Desafío de la Persuasión* (2010), *Minería, una Oportunidad de Desarrollo del Perú* (2012) and *Minería en la Estrategia de Desarrollo del Perú* (2014). He also coauthored *Empresa, Economía y Libertad* (2005) and *Visiones de Desarrollo: Perspectivas Indígenas, Estatales y Empresariales* and *Manual entre las Buenas y Malas Prácticas de la Consulta Previa* (2015). Vidalon writes international business columns for COMEX Peru and El Montonero online. He is currently the **superintendent of Public Relations at Southern Peru Copper Corporation**. [Peru]

Dionys Sánchez

With over 15 years in Telecommunications, Sanchez has extensive experience with data transmission systems and MPLS networks, with a particular focus on the preparation, planning and execution of systems integration projects. He has worked for important technology companies such as NCR Corporation, Tricom Latinoamérica and Cable & Wireless Panama. During his time as **national director of the Technology and Transformation unit of the National Authority for Government Innovation (AIG)**, he headed major national projects. He holds a degree in Electronic Engineering and Telecommunications, a postgraduate degree in Senior Management and a master's degree in Marketing. [Panama]

Hugo Marynissen

Marynissen is a professor and academic director for the Executive Ph.D. program at the Antwerp Management School and a visiting professor at various universities. He is also a senior partner at PM Risk–Crisis–Change, an agency specializing in risk and crisis management. Since 2008, he has provided regular coaching and consultancy services in the field of risk and crisis management. Marynissen is also the **president of the CIP Institute**, a nonprofit organization that brings scientists and practitioners from various disciplines together in an inspiring and innovative platform to exchange ideas and develop knowledge of the Complex and Interactive Processes (CIP) in the crisis management field. The focus of his current research is the crisis team dynamics, safety leadership, normalized chaos and the role of crisis communications during extreme events. [Belgium]

WHO *ARE* OUR *contributors?*

Mike Lauder

Lauder started his working life as a military engineer and served in the British Army for over 20 years. During this time, he experienced the practical issues involved in risk management and crisis planning firsthand. While his work included project management (both in engineering and procurement), corporate planning and process design, the majority of his career focused on explosive ordnance disposal work, in which good risk management became a very personal issue. Lauder holds a Business Doctorate from the Cranfield University School of Management. He has published multiple books and research papers on risk governance and crisis management practices and is also as a visiting professor at Antwerp Management School and Cranfield University School of Management. He is currently the **managing director of Alto42 Ltd**. [United Kingdom]

Javier Sirvent

Communications media and experts have dubbed him a **Technology Evangelist**. Sirvent is considered one of the most brilliant minds in the Spanish technology industry, as he is a visionary who connects the worlds of science and technology. He is the author of several industrial patents and the founder of companies that consult on innovation and IoT for entities in various sectors, including insurance, banking, industry 4.0, transport, retail and more. A professor at EOI, INESDI, IE Business School, CH.Garrigues, ICADE, ESIC, ICEMD, The Valley Digital School, FOM Industria4.0, Telefónica Schools of Excellence and various other educational programs for businesses and people on digital transformation, disruptive innovation and exponential technologies, Sirvent has also been a speaker at several conferences. He has shared a stage with experts such as the founder of Twitter, global genetics and molecular engineering authority George Church, Apple co-Founder Steve Wozniak and executives from companies such as Facebook, Google and Amazon. These are just some of the people with whom he shares friendship, passions and a few unmentionable secrets. [Spain]

Marc Asturias

The Senior Manager of Marketing & Public Relations at Fortinet for Latin America and the Caribbean, Asturias has over two decades of experience in business security marketing. He has directed programs and efficient teams for companies such as Apple, Veritas/Symantec, General Dynamics Advanced Information Systems and Cisco, where he led marketing initiatives for technical training and cybersecurity throughout all verticals and segments in the Americas. He has also led key programs with Mexico First, Canieti, the World Bank and the Office of the President of Mexico; with the SENAC in Brazil; the Government of Costa Rica; and military veterans initiatives with the White House and U.S. Department of Defense. [United States]

María Luisa Moreo

The Communications Manager at VOST Spain and digital magazine iRescate, Moreo was formerly a senior consultant in LLORENTE & CUENCA's Corporate Communications Area. She assesses security projects for the European Commission regarding social networks and emergencies and lectures in several courses for the National Civil Protection School of Madrid. She previously worked for Onda Cero Radio and Cadena COPE and was head of communications at SUMMA 112. [Spain]

Javier Robalino

Robalino is a **managing partner of FERRERE Abogados in Ecuador** and member of the firm's global executive committee (2015). He also co-chairs the arbitration practice and acts as managing partner for Ecuador. He represents many multinationals in various local and international commercial and investment disputes. He has participated in numerous cases under the laws of ICSID, UNCITRAL, CIAC, ICC and CAM-Santiago, among others. Robalino also participates in international public law cases under the WTO, the Andean Community of Nations (CAN) and the American Convention on Human Rights frameworks, among others. He obtained a master's from the Duke University Faculty of Law (2006, cum laude) and a Ph.D. (SJD) from the Catholic University of Quito (1990-1995). [Ecuador]

Alex Romero

Currently **CEO and Founder of Alto Data Analytics**, Romero was vice-chairman of Viacom for Southern Europe, Turkey, the Middle East and before founding his analytics company in 2012. Before Viacom, he was in charge of Yahoo!'s business development in Southern Europe, an extension of his role in the Vodafone Group, where he forged strategic alliances with global enterprises such as Microsoft and Google. Before working for Vodafone, Romero was a manager at Alcatel-Lucent. Throughout his career, he has successfully helped numerous firms create digital strategies in multiple world markets. He holds a master's in Engineering with a specialty in Electronics and Automation from the University of Malaga (UMA) (Spain) and an MBA from Henley Business School (UK). [Spain]

Vanessa Silveyra

Silveyra holds a degree in Political Science from the Autonomous Institute of Mexico (ITAM) and a master's degree in Public Administration and Public Policies from the Monterrey Institute of Technology and Higher Education (ITESM) and the John F. Kennedy School of Government, Harvard. She coordinated the Integrity and Transparency in the Mexican Private Sector Program, in which she worked to help control corruption from a systemic and human rights perspective. She was also an officer in the Mexican Supreme Court of Justice and Federal Electoral Institute, focusing on freedom of information and a shift toward civic and democratic values. She is currently the **manager of User Care and Services of ALEATICA**. [Mexico]

Werner Zitzmann

Zitzmann is a consultant and executive with a lengthy track record in the media industry. He was vice-chairman and secretary of Casa Editorial El Tiempo de Colombia for 11 years; an independent consultant for family businesses and enterprises, particularly in the digital arena; and member of the Managing Boards of several organizations, including Asomedios and Old Mutual. Since May 2017, he has been heading the transformation of the **Colombian Information Media Association** (AMI) which brings together the most important national news media in the country. [Colombia]

Olga Botero

Botero is an IT executive with over 25 years of experience. She is a **founding partner of C&S Customers and Strategy**, a boutique consultancy focused on technology, operations and cybersecurity for numerous industries in Latin America, and a senior advisor for the Boston Consulting Group regarding technology and cybersecurity. She is an independent director and chair of the Technology and Cybersecurity Commission of Evertec (NYSE EVTC), co-chair of Women Corporate Directors (WCD) in Colombia and has sat on the boards of ACH Colombia, Todo1 Services, Multienlace and Tania. She has also participated in several international advisory groups. [Colombia]

Emanuel Abadía

With over 30 years of experience in the Panama insurance sector, Abadia is the **Country Head & Managing Director at Marsh Semusa**. Together with the multifaceted, dynamic human talent at Marsh Panama, his main goal is to boost growth in the insurance industry, thus contributing to the country's sustainable growth. He has participated in numerous seminars and conferences, promoting a culture of risk identification, prevention and mitigation. [Panama]

Roberto Dias

Dias is the **managing editor for newspaper Folha de S.Paulo**. A journalist, he graduated from the University of Sao Paulo School of Communications and Arts (ECA-USP) and holds a postgraduate degree from the University of Barcelona and Columbia. He has worked at Folha de S.Paulo since 1998, where he reports on and edits the sports, politics and economy sections. For a time, Dias was the New York correspondent, and was also responsible for coordinating the newspaper's digital strategy. [Brasil]

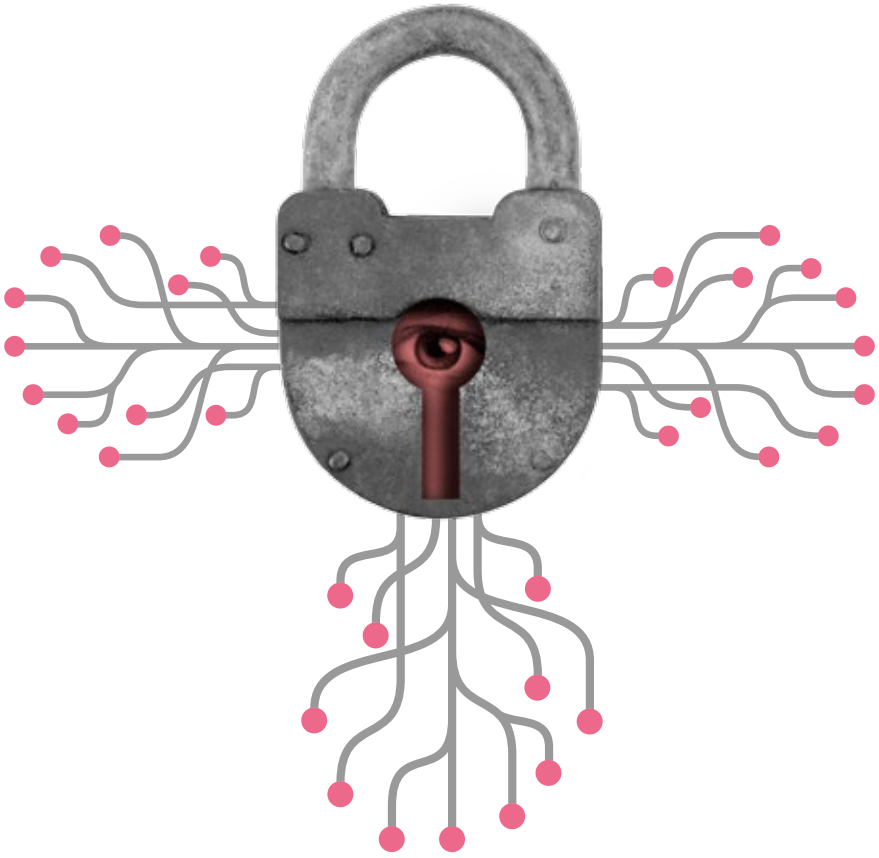
Iván Pino

A **Partner and Senior Director of LLORENTE & CUENCA's Digital Area**, Pino is a journalist with a degree in Information Science from Malaga University (UCM) and a master's degree in Sustainability and Corporate Responsibility from UNED-UJI. He has 20 years of experience in corporate reputation and communications, with a specialization in Digital Communications. He coauthored the book *Claves del nuevo Marketing. Cómo sacarle partido a la Web 2.0* (2009, Gestión 2000) and edited the first Spanish-language e-book on social media communications, *Tu Plan de Comunicación en Internet. Paso a Paso* (2008). He is also a lecturer for the Corporate and Institutional Communications master's program at Carlos III University and Unidad Editorial, as well as for the Corporate and Publicity Communications master's program at the Complutense University of Madrid. [Spain]

Luis Serrano

The **global leader of the Crisis and Risk Area at LLORENTE & CUENCA**, Serrano is one of Spain's top experts on communications management, crisis situations and the development of crisis action protocols for social networks. With a degree in journalism, he was the press manager for the Emergencies Centre 112 for the Community of Madrid for 17 years, where he actively participated in handling extreme situations such as the 11-M terrorist attack in Madrid. He has been part of over 100 incidents, accidents with multiple victims, health crises, etc., writing his experiences in his book, *11M y otras catástrofes. La gestión de la comunicación en emergencias*. He also has extensive teaching experience in crisis management and emergencies. As a journalist, he worked in Onda Cero's news services for seven years. [Spain]

HYPERCONNECTED
and hyper-vulnerable



"The lack of protection for our personal data and communications threatens to put pressure on the current system of international global relations

José Antonio Llorente

Founding partner and chairman of LLORENTE & CUENCA / United States - Spain

THE HIGH COST OF REPUTATION CRISES. ARE WE READY FOR THEM?

The crisis Facebook experienced this year is just one example of the complex world in which we live. The paradigm shift we witnessed is a reflection of the shifting virtual scenario in which risks evolve and crises brew.

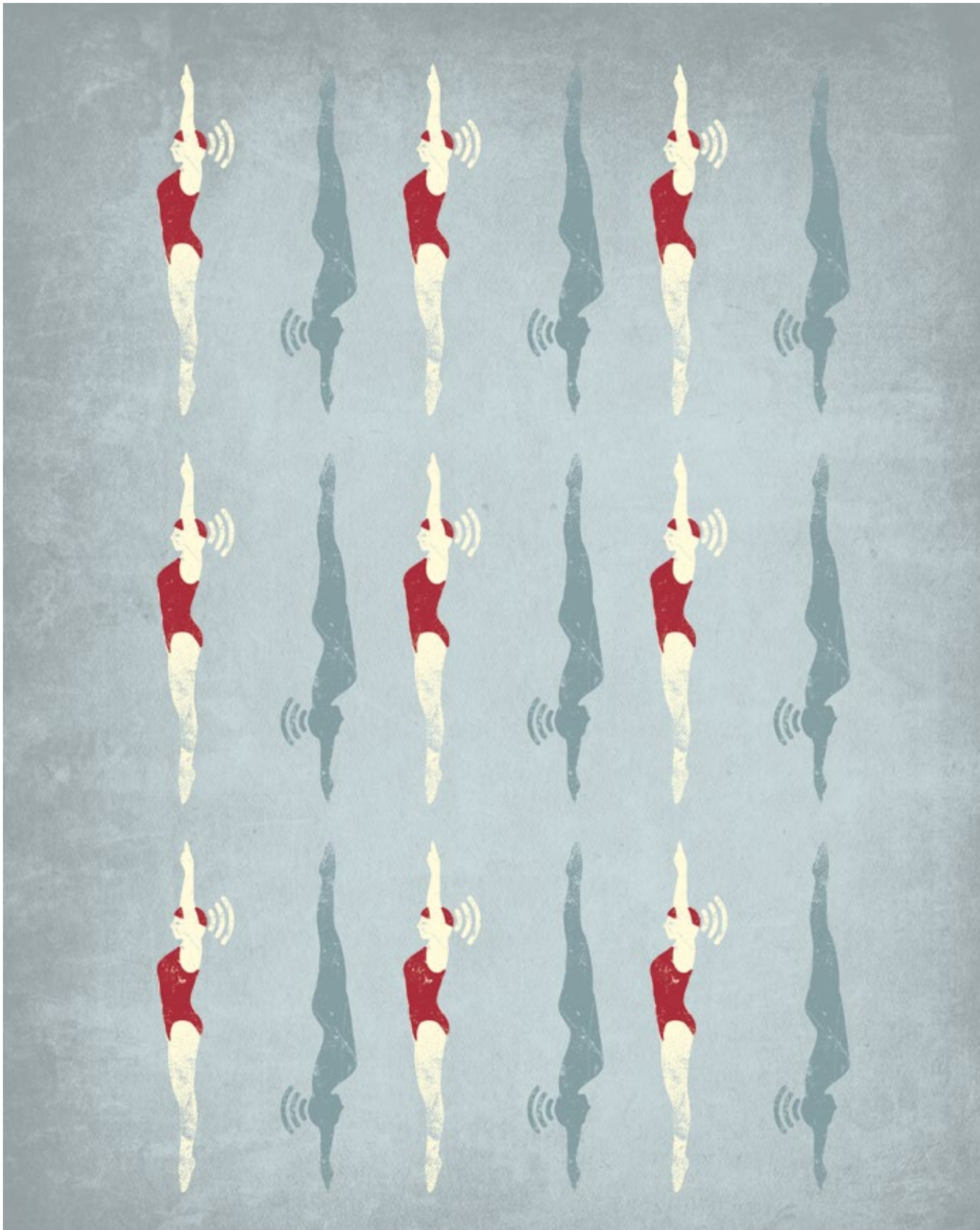
We live in a hyperconnected, hyper-transparent world in which citizens (many of whom have become cyborgs by virtue of their mobile extensions) not only spread information to all corners of the planet in a matter of seconds, but sometimes do so with even greater enthusiasm when the information is false, as recently shown by MIT research. Each and every one of us is a risk vector, as we learned last year with ransomware WannaCry.

In this highly digitalized and hyper-transparent risk scenario, the question becomes, how are companies addressing this hyper-vulnerability? How do they deal with cyberattacks, whose rates double each year? How do they protect themselves from their own employees, who have become de facto unauthorized spokespeople? Do they convert them into collaborators in crisis situations? How much money does the world economy lose from financial risk? Are boards of directors getting ready for this new reality by updating their protocols and installing the best management technology?

But it is not only cyber threats that cloud our future. The lack of protection for our personal data and communications, as well as the surge in fake news, threatens to put pressure on the current system of international global relations, increasing risks for governments, corporations and citizens alike.

How can organizations brace themselves for this reality? Can we prevent or ameliorate any of the effects this change will have on the world? Are we sufficiently ready to handle the crisis when it comes? Would we not save ourselves a lot of money and effort if we were well prepared? Would we avoid the high cost crises have on reputations and businesses if we prepared ourselves before the tsunami of risks came knocking at our door?

Answering these and other questions is why we have come together in UNO 31. Will you join us?



THE *TECHNOLOGICAL* *intrusion*

José Antonio Zarzalejos

Journalist, former editor-in-chief of *ABC* and *El Correo* / Spain

Up until just a few years ago, most technological and social analysts agreed with Al Gore, former U.S. presidential candidate, and his idea of what the internet represented: "The internet is a formidable new medium of communication and a source of great hope for the future vitality of democracy." Those same observers have now turned to the opinion held by Google's Executive Chairman up to 2017, Eric Schmidt, as a more realistic idea. He said the internet was "the largest experiment in anarchy that we have ever had." Between Gore's optimism and Schmidt's wry skepticism, there should be a realistic acknowledgement the internet is an enormous vehicle for knowledge that democratizes learning, connects citizens and societies and has annihilated the concepts of space and time. At the same time, it should be stressed that the internet also brings what we now call vulnerabilities and hazards, and their avoidance and neutralization must come from within.

> *"Digital technology has expanded to such an extent that we could well speak of it as an intrusion that is distorting key values and principles*

The digitalization of the economy, social relationships, communications, knowledge, employment and work are extraordinary achievements of our time, but they entail risks we must address. Digital technology has expanded to such an extent, making the world so dependent on its dictates, that we could well speak of it as an intrusion that is distorting the values and principles necessary for coexistence, social good and people's health. Three types of vulnerabilities are brought about by these new technologies. The first affects citizens in their everyday lives; the second concerns societies dependent on information technologies; and the third has an impact on politics, and especially one aspect of it: defense politics.

The World Health Organization (WHO) does not yet acknowledge people technically suffer from digital addiction. According to the organization, we can only talk of excessive internet use. However, evidence suggests that before long, intense use of networks will be classified as an addiction that can be treated by psychological or even drug therapies, insofar as the new technologies can cause anxiety or serious emotional disorders. Universal use of cell phones, which store a vast amount of personal knowledge and replace memory, is now a habit spanning almost all generations.

The incessantly growing number of applications; the fact cell phones now replace TVs, watches, alarms, voice communication tools and social devices of widely varying natures through WhatsApp; technology's presence as a third (almost physical)

> *"New technologies have become parasitic hosts to types of crime that are forcing police to restructure their preparation and activities*

arm all indicate a dependence—addictive or otherwise—that has changed people's behavior, bringing society new relationship patterns and a new outlook on life. Technological socialization opens the door to another very serious vulnerability, as we saw in March of this year, when data leakage affected as many as 50 million Facebook users. This was a huge blow to global cybersecurity with consequences in numerous areas, especially in political interference.

This digital dependence is being used to commit new crimes (cybercrime), some of which are particularly alarming (such as cyberbullying, which is turning into a plague), as well as other types of especially sordid crimes, including child pornography, pedophile rings, drug and human trafficking… In short, new technologies have become parasitic hosts to types of crime that are forcing police to restructure their preparation and activities, using the opportunities technology offers to their advantage during criminal investigations and arrests.

Institutionalized falsehoods—the second vulnerability—refer to what has become known as *fake news*. This alternative reality is filled with post-truths and untrue "facts" that are difficult to check but appeal to emotions, a plague that would not spread if it were not for new technologies. The problem of misinformation and the distortion of reality is one of the clearest vulnerabilities caused by new technologies, and digital networks have not found any obvious solutions beyond the verification platforms springing up to tackle this abuse. The fact that many politicians and unscrupulous leaders use these deceitful resources in their campaigns or to reinforce their decisions in public opinion introduces a new paradigm in public leadership.

For the first time in its many years of history, the World Economic Forum—which meets in Davos annually and covers an essentially financial agenda—–has set up the Global Centre for Cybersecurity, which has been in operation since last March. This initiative was preceded by the *Global Risks Report* (2018), which recommended making cybersecurity a primary topic at the event because "cyberattacks are perceived as the global risk of highest concern to business leaders in advanced economies." Forum experts have spent an entire year preparing a cyber resilience playbook, identifying 14 areas in which the public and private sectors could cooperate.

We are already seeing vulnerabilities deriving from new technologies affect business and state security, creating the need for close collaboration and a Copernican review of companies' safeguards for digital assets and principles behind strengthening state security measures (both defense and response) against external enemies. The possibility of hacking even the most intimate and strategic secrets owned by large enterprises (data bases, production formulas, marketing networks, patents, etc.) or nations (offensive and defensive nuclear assets, lines of investigation for war risks, classified information on hostile agents, election results, etc.) has become a tactical, strategic, political and business priority. Nobody harbors any doubt about that. In Spain, the monthly reports published in Madrid by The Cyber Security Think Tank, which are conveyed through Instituto Elcano, deserve praise as a true vanguard in analyzing cybersecurity and defense.

> *"Vulnerabilities deriving from new technologies affect business and state security, creating the need for close collaboration and a Copernican review of companies' safeguards*

Broadly speaking, these are the key areas of technological intrusion in our time. It is a new threat tempering the numerous benefits new technologies provide. There has never been a historical phenomenon that has been solely and wholly beneficial. All have their good and bad sides. We are now in the fight against the excesses of digitalization, which presents vulnerabilities that can cause real disasters.

INSTITUTIONAL *COMMUNICATIONS* ON SUBMARINE *San Juan*

Enrique Antonio Balbi

Head of the Institutional Communications Department and spokesman for the Argentine Navy / Argentina

When submarine *San Juan* failed to report its position to headquarters at the stipulated time Nov. 16, 2017, the Argentine Navy commenced search and rescue operations for the vessel and its crew in its sea control patrol area of the South Atlantic.

> *"The magnitude of the resources involved in this search and rescue operation for the damaged submarine made it unprecedented anywhere in the world*

The magnitude of material, human and logistics resources involved in the operation (27 ships, 14 aircraft and over 4,000 people, both military and civil, national and foreign), as well as the length of time of uninterrupted activity, made this search and rescue operation for the damaged submarine unprecedented anywhere in the world.

The Navy faced its most difficult situation since the Falklands War, directing the means deployed mile by mile around the clock, without rest and while using the best technology in the world in a search which, at the time of writing, still continued with the hope of dispelling the uncertainties and fears tormenting the crew's relatives and all members of the Navy.

The *San Juan's* sudden, unexpected crisis had a tremendous social impact. This extraordinary circumstance forced authorities to divide their attention between the search and rescue operation and informing the public, trying to synergize its actions in both areas while protecting the relatives from premature distress for as long as was considered prudent.

Relatives were given priority when reporting daily events. Two visits to the search coordination center at the Puerto Belgrano Naval Base and three trips to deployed units were also arranged to help them understand and appreciate the size of the search operation.

Almost as soon as the search for the submarine was declared, a crisis cabinet was organized. It was made up of the Navy officers responsible for Institutional Communications and authorities from the Ministry of Defense.

The cabinet adopted the strategy of transparently informing the community from a single official source, reporting specific facts that had been reliably confirmed to avoid any speculation and carefully protect sensitive information. This avoided leaks from unqualified sources sharing unfounded information or leading to erroneous conclusions, and explanations were given as new incidents arose.

Once the crisis broke, events happened very fast, taking place on a growing scale with increasing speed and an overriding feeling of

"Relatives were given priority when reporting daily events. Two visits and three trips were arranged to help them understand and appreciate the size of the search operation

urgency. Consequently, press releases were sent for 26 consecutive days, up to four times a day. Information was disseminated through press conferences at the Libertad building (the Navy Chief of Staff's headquarters), supplemented with the daily written releases.

The institutional communications through the media to the community regarding the search for the submarine were accompanied by very good media relationships, but, due to the operation's extended time and the prevailing uncertainty, unspecialized opinions began to appear, giving priority to disconnected facts and seeking news without any serious analysis.

Another activity, just as important, was having to give unscheduled press conferences to provide official information, purely to counter the numerous inaccurate or false versions of facts circulating on social networks, leading the public and relatives to incorrect conclusions that confused them, causing them anguish, generating false expectations and hurting their feelings.

One lesson learned from this was that a single spokesperson should have been established from the outset, or perhaps a crisis committee in Mar del Plata—the submarine's usual station—with the relatives present.

It was a good idea to have set the press conference times for 10 minutes after the hour so as not to interfere with headlines on the TV networks.

In coordination with journalists, infographics were produced to give the public a better technical understanding of the facts. Unfortunately, from an audiovisual point of view and due to the remoteness of the operations, the media had few videos of the units at work, which would have helped people grasp how complicated the search was.

Handling the institutional communications and professionalism in carrying out the search operations consolidated the institution's internal culture, increased member pride and strengthened its image despite criticism, which was inevitable owing to the complexity of the facts, tragic setting and opposing interests.

FROM *HYPER-CONNECTIVITY* TO *hyper-vulnerability*

Guillermo Vidalón

Superintendent of Public Relations of Southern Peru Copper Corporation / Peru

The downside to hyper-connectivity is unquestionably hyper-vulnerability. What has happened? Technology has provided billions of people throughout the world with an opportunity to express their opinions, saying whether they agree or disagree with government decisions or even company regulations with a public reach, either because their products or services do not meet expectations or because, at some point, the government-citizen or company-stakeholder relationship was breached.

> *"Post-truth appeals to emotion, as this is easier to position and have accepted*

When that relationship is upset, the trust between parties is damaged and credibility levels fall. This can have social, political, economic, cultural, religious or environmental implications.

At present, hyper-connectivity means any event, however trivial it may seem to some, is at risk of going viral in a very short period of time, affecting the reputations of individuals or entities. Those who have fallen victim to cyberattacks are often waiting for something else to happen to capture people's attention so their own "virtual presence" will slip into the background. In this circumstance, the "solution" would be finding the next victim.

Within the communications sector and social relationships, we believe the "solution" is to act before a crisis occurs. Nobody wants them, but nor do we know when one might arise. Given the hyper-connectivity we have thanks to cyberspace, the best preventive measure is to be present in that arena continuously, first through active listening and possible issues tracking; then by sharing our "truth" or "post-truth" message. In my opinion, this has nothing to do with correcting a position—even though we know it is not true—but rather with how it is told so it can be understood and accepted by target audiences; to be credible, it must have a logical, coherent structure.

So, the distinction we make between the two concepts is that the "truth" is what can reasonably be upheld with the greatest possible scientific rigor, whereas the "post-truth" is the same truth, but associated with a given perception we want to build up and position within our target audience or stakeholders. In most cases, the post-truth appeals to emotion, as this is easier to position and have accepted. The "post-truth" steers clear of confrontation with the "truth" because it has no depth, whereas those who scrupulously go after the "truth" will always be a minority, but a more demanding one.

Contemporary events prove a short message or quick, timely response is more easily accepted and positioned in public opinion and can recover reputations or reposition authorities or business institutions. Simply recall the mechanisms used

against rumors in the past. The longer passed without an official company or institutional response, the more the rumor grew and the greater the damage—sometimes irreparable—to the latter's credibility. Adequate crisis management is what makes it possible to avert and derail rumors.

A video showing a civil servant or authority partaking in an inappropriate action can generate a wave of disagreement or indignation over what happened, spurring identification with the victim and the person(s) who recorded it with their cell phone, because a high-end video camera is not required. Moreover, beyond the feeling of indignation—a strictly private emotion among individuals—the most challenging thing is how it can get individuals motivated to act, mobilize and carry out acts of violence.

In 2000 and even this year, the Peruvian heads of state were obliged to stand down following the dissemination of a video showing, in the first case, how he won supporters over to the government's cause, and in the second case, intention to dissuade a member of parliament from voting against a candidate in exchange for appointing his friends to public offices and a budget item to finance public works in the town he represented.

Only 24 hours earlier, the former Head of State assured he would not resign. Then the video was distributed by media and through social networks and indignation grew so much that no communications strategy could withstand the onslaught against the president's hyper-vulnerability. By that time he was politically weak, and the president was unable to anticipate or weather the political and reputational reality that befell him. Therefore, he had to stand down.

> *"Hyper-connectivity generates hyper-vulnerability for anyone who has been betrayed or exposed to public opinion through social networks. But in itself, hyper-connectivity is also subject to the vulnerability of its own achievements*

In the private sector, hyper-connectivity has also had a negative impact on companies whose reputations classified them as bearers of a love bite. Last year, a prestigious firm of dairy products had to change the visual identity of one of its brands because outside information went viral in just a few hours. A nutritional compound with properties very similar to milk had been positioned as that product, and its label even contained the picture of a cow. The brand was questioned by consumers so strongly that the company, under pressure from authorities, was forced to withdraw it from the market and run a vast awareness campaign to provide an explanation of the product, presenting human testimonials of the favorable effect its product would have on thousands of humble Peruvian livestock farming families.

Access to technology has empowered a lot of people, encouraging them to express their thoughts, feelings and emotions and to identify and assert themselves. Numerous groups have announced themselves through social networks and attracted attention from other members of the national and international community.

Hyper-connectivity generates hyper-vulnerability for anyone who has been betrayed or exposed to public opinion through social networks. But in itself, hyper-connectivity is also subject to the vulnerability of its own achievements. The more people who are interconnected, the greater the chance one questionable event will be "replaced" by another. Hyper-connectivity generates an exponential wave, but its fall from the spotlight is usually abrupt.

"Public opinion rejects conduct that reveals complicity or shows a superficial or banal attitude toward events that are, in and of themselves, reprehensible

In a sudden crisis of hyper-connectivity, it is advisable to check whether what happened is addressed among your prevention measures. Otherwise, the first thing to do is always to study the situation carefully and possibly have a previously trained spokesperson acknowledge what happened, then announce corrective measures against those responsible. In some cases, unfortunately, a scapegoat must be found, as someone must take responsibility for the incident. Public opinion rejects conduct that reveals complicity or shows a superficial or banal attitude toward events that are, in and of themselves, reprehensible.

GOVERNMENT

CYBERSECURITY, A *priority*

Dionys Sánchez

National Director of Technology and Transformation of the National Authority for Government Innovation / Panama

When the Spanish arrived in Panama in 1501, they saw the country as a natural route to cross from one ocean to another, a strategic role confirmed by the building of the railway during the California gold rush and the opening of the Panama Canal in 1914.

Today, over 500 years later, Panama is a technological hub where seven undersea fiber optic cables converge, carrying millions of megabits of voice and data with information from all parts of the world. We are still a hub of interconnection, a transit point. A country immersed in the digital economy, that opted to democratize the internet, e-commerce and e-government.

But we know this digital transformation also has its risks and challenges. Data protection is a priority for private enterprise, which take measures to avoid falling victim to the cyberattacks affecting their businesses, customers, revenues and reputations. State-owned institutions must also protect citizen information, stored across numerous platforms, and ensure key entities providing financial, logistical, security and medical services are protected from these new cybercrimes.

> *"In Panama, the National Cybersecurity Strategy met its first goals, and we are now updating it*

Accordingly, since 2013, the National Government—through the National Authority for Government Innovation (AIG)—has implemented a National Cybersecurity Strategy to combine the efforts of citizens, businesses and state entities to increase cybersecurity and enable the safe use of communication technologies.

This roadmap summarizes several focal points which, overall, help governments make political, economic, administrative, legal and educational decisions in the face of these new challenges. In Panama, the National Cybersecurity Strategy has met its first goals, and we are now updating it to respond to the new cyberthreats and cybercrimes that could jeopardize public or private information or disrupt critical institutions.

One of the developments will be the enactment of the first local cybercrime law to investigate and punish new cybercrimes, such as denial of service, phishing or ransomware. We have checked the validity of this document with sectors such as banking, one of the most important sectors in our country—and one which has a high probability of being affected.

> *"Panama has achieved a certain cyber maturity, but we are still working to legislate and protect digital society*

Another key point on which we have made progress is regional coordination, with the creation of the Computer Security Incident Response Team (CSIRT) Panama and a subscription to the Forum of Incident Response and Security Teams (FIRST).

FIRST member countries take advantage of the hyper-connectivity in this world without borders to coordinate with other governments and strengthen prevention measures against security incidents or attacks.

For example, through this cross-functional collaboration, we were able to alert the region in advance of the global WannaCry cyber-attack, an extortion virus that affected over 100 countries in May last year. Coordinated action enabled each country on this continent to take preventive measures and actions.

This work also enabled countries to replicate their response protocols and share successful experiences in government protection, as well as identify the investments required to strengthen platforms, including those great vaults of digital information.

Another important point in building and updating a national cybersecurity strategy is preparing civil servants and increasing citizen awareness. It has been proven human beings ("the asset between the chair and the desk") have been the breaking point in all cybersecurity incidents.

The challenge here is to ensure this knowledge and comprehension of cyberthreats reaches everyone on an internal and external level. Bearing in mind that most of the economically active population is not made up of "digital natives," it is difficult to include everyone quickly. However, through constant training of key units and businesses and school support, major progress can be achieved.

Awareness begins in school, where the next generation of cyber citizens is being educated. A young, but more connected digital population will be the next users and civil servants to create new cybersecurity strategies and new technologies.

Panama has achieved a certain cyber maturity, but we are still working to legislate and protect digital society. It is not merely a question of having a modern, robust or fast digital infrastructure; it must also be secure. This is obligatory if, as a country, we want to continue taking advantage of the fourth industrial revolution. Protecting citizens from cybercrime is a duty, a right and a key strategy to continue growing.

DEALING WITH *COMPLEXITY*: IT'S *normal chaos*

Hugo Marynissen
President of the CIP Institute / Belgium

Mike Lauder
Managing Director of Alto42 Ltd / United Kingdom

The world in which we live and work in is complex and driven by forces we often do not see, recognize or appreciate. Moreover, we live in a world of continuous change that thwarts our plans. Therefore, we are constantly forced to adapt them. These adaptive actions, which we often described as "management" or "decision making," have consequences, as all actions have both upsides and downsides—whether these are obvious or not. Because we see the need to expect the unexpected, we put plans, procedures and command and control systems in place that should prevent us from making mistakes that could eventually lead to sliding into a crisis situation. However, the question of whether this will actually prevent organizational failure arises.

> *"If we look at a crisis from this perspective of normal chaos, we see there is very little stability in the environment, which often demands increased improvisations in management solutions*

In recent years, we have been researching whether or not there is a different approach to managing complex situations. In an attempt to move from using complexity as a retrospective explanation to one that facilitates a more proactive management approach, we changed the current cause and effect paradigm and named it '*normal chaos*' to denote circumstances where the daily pattern of interactions within a dynamic system are too complex to be fully appreciated or understood. This, in turn, makes outcomes difficult to predict.

If we look at a crisis from this perspective of normal chaos, we see there is very little stability in the environment, which often demands increased improvisations in management solutions. This makes us ask what effective crisis management looks like in organizations that could one day face a complex crisis situation. In his book *Overcomplicated* (Penguin, 2016), Samuel Arbesman illustrates the complexity of systems we currently deal with. Problems have multiple pathways, diminishing the predictability of future outputs or outcomes. This state of affairs also affects the ability to exert control over these events. Managers actually have less control than outsiders think or expect. These multiple pathways are riddled with uncertainty, disproportionality and emergent phenomena. Instability, in its many forms, is our constant companion.

Linking this to the interactive complexity we have to deal with in today's world, we must acknowledge our understanding of the problems we face will always be only partial. There are a couple of good reasons for that. First, we often see things in patterns. Though this helps us get our heads around complex issues to make them more comprehensible, the flipside of the coin is that the patterns we observe are often temporary,

depending heavily on the context and scale of observation. Therefore, these patterns may simply be illusionary—that is why we need to be cautious about basing our plans on them. Second, there are no ideal solutions to problems! All solutions are contingent on the circumstances to which they are applied. Third, our ability to actually control what happens to our organization and to ourselves us is much more limited than normally assumed. The idea that organizational processes can be made linear and management teams can adequately anticipate crisis situations is a fallacy. In a crisis, organizations deal with complexity verging on chaos.

Let us illustrate this illusion of control with a practical example of crossing a street. You only have partial control of the situation, in that you can control your own activities but not those of the people around you. You can try to influence these other parties, such as by holding up a hand to ask a car to stop and let you cross, for example. But they may ignore you—and they often do. Annually, more than 4,500 pedestrians are killed in traffic accidents in the United States. This averages to one accident-related pedestrian death every two hours. Additionally, more than 150,000 pedestrians went to U.S. hospital emergency room for non-fatal crash-related injuries last year.

This shows the limitations of rules and commands. Likewise, in organizations, leaders need followers to obey their commands. In this case, you command a car to stop but it ignores you. In any organization, there are frequent occasions when commands and rules are either ignored or carried out in a way not intended by the leader, or that was not the aim of the rule. Your 'control' of your own situation may also be partial if you misjudge the closing speed between you and the oncoming car, leading to you getting out of its way just in time. You did not see the woman with the stroller that steps out from behind a bus, which stops you from reaching the safety of the pavement as you planned. You could see crossing the road as a simple activity (by abstracting much of what else is going on), or you could see it as just another manifestation of normal chaos.

"Finding the optimal balance between using rules and regulations and relying on autonomous operations teams' interdependencies is key to anticipating complex situations

Given that, we see having an effective planning process to be more important than simply having a plan. However, this requires a mental shift, one willing to send the Utopian 'perfect world paradigm' (which says we can manage a crises) to the fires below and accept that we actually have very little control. Therefore, we should start to see management as a mix of 'intuitive skills' and compliance with laws and regulations to cope with the prevailing uncertainty surrounding us. Our research indicates that finding the optimal balance between, on one end, using rules and regulations and, on the other, relying on autonomous operations teams' interdependencies is key to anticipating complex situations. Although they will never have 'complete control' in a set of given constraints, it will greatly help teams avoid the cause-and-effect trap and focus on the few simple rules, principles or Critical Success Factors that will guide them through the crisis.

ARTIFICIAL INTELLIGENCE

TAKES US INTO A *new era*: ZERO CLICK

Javier Sirvent

Technology Evangelist / Spain

In *Space Odyssey (2001)*, Arthur C. Clarke introduced us to supercomputer HAL 9000. Since then, technology has advanced in parallel to the famous Moore's Law. But not only has the number of transistors doubled inexorably, the complex algorithms of Artificial Intelligence that give life to voice assistance are going to change our lives again. In three years' time, we will be able to do 30% of the things we currently do via screen directly with our voices.

> *"In three years' time, we will be able to do directly with our voice 30% of the things we currently do via a screen*

Several years ago, when Google photographed and mapped the entire planet (which was not exactly "cheap"), with this operation and its *StreetView*, putting a computer in our pockets with its free Android operating system, it guaranteed it would lead mobility and, together with localization, continue to generate millions in revenues in advertising on any screen. However, after mapping hundreds of thousands of kilometers, it knew anyone using that public data could download it onto a vehicle and start experimenting with autonomous driving. It then created a new product, which it offered for free: Google Images and Google Photo.

Then, whenever we searched for a product or simply associated an image with a word, it showed us hundreds of images and we consciously selected the best one for us—but we were also training and programming Google's artificial intelligence to recognize objects. Google, not content with its billions of daily results, created something for certain security options and to confirm we are human: its new reCAPTCHA asks us to identify a traffic signal, a number or a road in a number of images. Those guys at Google are real stars! They've got us working for them and, what's more, they successfully and cannily protect their main source of income: advertising.

After feeding "the beast" with sufficient information, corrected and supervised by human intelligence, they decided to go ahead with their plan to lead the next screen: the self-driving vehicle. Great idea! If cars are going to be able to drive themselves, what are we going to do in the meantime? Sleep, shop, work, listen to music, maybe view content on the vehicle's internal screens or augmented reality windshield? For this reason, they also bought up several companies related to these technologies, such as Quest Visual and Magic Leap, whose work has recently been kept secret.

The strategy, though discreet, was obvious for those of us who "join things." When Google transformed its SelfDrive Car division into a company called WAYMO, which was worth over $72 billion in just a few months (more than Tesla, Ford or General Motors), their goal was clear: dominate the self-driving vehicles market by giving away their

operating system—just as it did in the smartphone sector—and thus dominating the advertising business, where it aims to be our "next screen."

But even though they are so far-sighted and innovative, making bets with huge sums of money, talented perspectives and the best professionals and market leaders, the guys at Mountain View have come up against a little hitch called Alexa.

Jeff Bezos, the "*Customer Experience*" genius who efficiently manages Amazon, realized that in the near future, many purchases would be made from inside a vehicle, so he jumped in and signed an agreement with Ford, Toyota, Lexus, Fiat Chrysler, Nissan, Hyundai, Daimler Mercedes Benz, BMW and even SEAT. The smart girl from Amazon got in first, racing ahead of Google's imperial plans, and she is already selling. It is her: Alexa.

The war for a new age, the age of the end of screens, has begun among GAFA (Google, Apple, Facebook and Amazon). We rode into 2018 on a new paradigm: voice guides. No more clicking on a physical medium to buy, chat, search for information or simply catch up on your friends' or neighbors' gossip. This is the dawn of probably one of the greatest changes to information access models since the arrival of the internet. A voice, similar to that of HAL 9000 50 years ago, will assist us at all times. *Zero click* is here.

"This is the dawn of probably one of the greatest changes to information access models since the arrival of the internet. A voice will assist us at all times. Zero click is here

SIRI will still be the infiltrated spy Apple needs to continue finding out more and more about its fervent users, but, as of April, it has signed on John Giannandrea, who was previously the Head of Artificial Intelligence at Google. Google had just "pinched" the person responsible for developing Alexa from Amazon. If Alexa is the maid, the saleswoman, the perfect shop assistant, then OK, Google aims to be our butler and chauffeur. Incidentally, what role is left for Mark Zuckerberg's company? Well yes, we will shortly have the new "nosy neighbor," but in digital form. A new being, for the time being secretly called "The Portal" or Jarvis, which will tell us all the gossip about our neighbors and acquaintances: what they buy, what they say and what they do. It will probably even be able to make secure transfers thanks to its biometric camera, in which banks will find a new enemy. The latest surprise Bloomberg has uncovered is that Amazon is working on a new household assistant, but this time, Alexa will have wheels and a robot form so she can chase you around your house to try to make your life easier. What more surprises do AI breakthroughs have in store for us?

CHALLENGES TO *SECURITY* IN DIGITAL *transformation*

Marc Asturias

Senior manager of Marketing & Public Relations at Fortinet for Latin America and the Caribbean / United States

Businesses and government agencies of all sizes are rapidly adopting digital business models, which they can use to quickly respond to changing consumer demands, process transactions and react in real time, increasing agility, productivity (for better commercial results) and service quality. But this transformation goes way beyond the corporate world. The digital transformation is changing society on an unprecedented scale. It is essentially changing how we learn, work, socialize, buy, administer finances and interact with the world around us. The challenge lies in balancing innovation and productivity with functionality and cybersecurity.

> *"The challenge lies in balancing innovation and productivity with functionality and cybersecurity*

As global cyberattacks persist, senior management is focusing attention on cybersecurity. It is no longer a matter of concern only for information technology (IT) teams. Rapid, sophisticated attacks on all industries have proven cybersecurity is the responsibility of an entire organization when attempting to avoid the paralyzing effects associated with data breaches.

Vulnerabilities can lead to fines for noncompliance and reputational damages, which can have lasting effects: 85% of managers working for financial institutions said damage to reputation is the most serious consequence of a data breach when consulted for a recent survey.

HYPER-CONNECTIVITY INCREASES RISKS IN DIGITAL TRANSFORMATION

There is evidence all around us of the potential impact of digital transformation. From smart cars to smart homes and from smart buildings to smart cities, we are seeing traditionally separate networks grow remarkably interlinked. As a result, it will be possible to do things like redirect traffic dynamically, control use of critical infrastructure resources such as water and energy grids, actively monitor city services and respond more efficiently to events of all kinds.

Smart companies are doing things of the same nature. To increase efficiency and profitability, the traditionally isolated Operational Technology (OT) systems are starting to converge with IT networks. Automation can be used to reduce overheads and raise return on investment (ROI). Digital firms will also be more actively connected, both with consumers, to provide services and support on demand, and with critical infrastructures, such as energy and refrigeration, to administer costs. In the same way, networks will expand and contract dynamically through multiple cloud environments to meet changing workloads and computing resource needs.

“Digital transformation vastly improves how we communicate and conduct trade. However, it is also bringing in new security risks and compliance requirements

TRADITIONAL SECURITY STRATEGIES DO NOT SCALE

Digital transformation vastly improves how we communicate and conduct trade. However, it is also bringing in new security risks and compliance requirements. Many traditional ways of protecting IT networks simply do not apply to the current converging networks. Part of the challenge is that the internet, where all of this occurs, still uses many of the same protocols and infrastructures it began with, decades ago. At the same time, the volume of data has increased almost 40 times in recent years, largely due to the explosion of applications, access points and connected devices. But although most data no longer stays in the traditional business network, we still focus on security, using a model that has become obsolete and insufficient. Part of the problem is that we tend to tackle infrastructure changes as individual projects instead of part of an integral transformation. We then tend to implement single, isolated security solutions to protect them, which complicates administration while reducing visibility and control.

CONVERGED NETWORKS REQUIRE CONVERGED SECURITY

Web security must be extended into a single, integrated system. We need to be able to not only see and protect all infrastructures and devices from a single site, regardless of their location or type, but also coordinate resources to improve detection, automate responses and dynamically adapt to network changes.

The best response to increasingly complicated web environments is simplicity. This requires a security transformation that must mirror the pace of the digital transformation. This security transformation involves integrating security into all areas of digital technology, producing a constant, holistic architecture to ensure effective security throughout the life cycle and covering the entire distributed web ecosystem. This includes attack surface identification, protection from known threats, threat detection, fast and coordinated responses to cyber events and continuous assessments.

Innovation and economic growth boosted by digital and security transformation have the power to change our society completely. But to do this without compromising everything we appreciate, the digital industry must reconsider security from a new perspective. And we must begin right now.

SOCIAL MEDIA ACTS LIKE A SELF-CLEANING OVEN FOR *fake news*

María Luisa Moreo

Communications Manager at VOST Spain / Spain

The arrival of social media considerably increased the virality of information, both true and false, plus hoaxes and fake news. The Gutenberg printing press, used by Luther in 1517 to distribute his 95 Theses at great speed, is comparable with the possibility offered today by social media, both to distribute knowledge and win electoral campaigns with invented information or the possibility of spreading hoaxes during terrorist attacks, wildfires and other critical times. Not only are the principles of honesty and transparency that ought to govern any democratic society at stake, but also, in extreme situations, enormous social alarm can be created. This can jeopardize the safety of the emergency services, forces and corps acting during those disasters, all while endangering the people they are trying to protect and to whom they are trying to send self-protection measures via social media.

> *"Twitter is a large-scale processing machine that spreads —then debunks—rumors at a rapid pace*

Although social media has these two facets (that of a high-speed information distribution channel and that of a destructive, or at least unfriendly, weapon), the good news is that it works like a self-cleaning oven: social media tends to self-correct while helping correct other sources. It offers more information than traditional media and acts as a vehicle to authenticate information sources.

This is the thesis Sasha Frere-Jones defended back in 2012 in her article *Good things about Twitter*,[1] published in *The New Yorker*. The journalist explained social media, saying, "It's sort of a self-cleaning oven, where the wisdom of the crowd can work out the kinks. A reliable version of events generally emerges because vanity (in the form of a visible number of retweets for the user who posts the canonical version) fuels the process, much as a writer's byline can press ego into the service of good writing."

In the same year, journalist John Herrman published the article *Twitter Is A Truth Machine*[2] on BuzzFeed News, pointing out that "Twitter beckons us to join every compressed news cycle, to confront every rumor or falsehood, and to see everything. This is what makes the service so maddening during the meta-obsessed election season, where the stakes are unclear and the consequences abstract. And it's also what makes it so valuable during fast-moving, decidedly real disasters. Twitter is a large-scale processing machine that spreads —then debunks—rumors at a rapid pace. To dwell on the obnoxiousness of the noise is to miss the result: that we end up with more facts, sooner, with less ambiguity."

The conclusion of this article could not be closer to the concept of intrinsic transparency of social networks: "Because the internet today, as exasperating as it can be, is very good at one thing: vetting ascertainable facts."

Although I agree Twitter is both the problem and the solution, when we consider emergencies, we cannot overlook the fact that digital volunteer teams arise throughout the world and monitor social networks to correct misinformation shared on them, as well as on mass media and through official reports. As Jeanette Sutton pointed out in 2010 in her article *Twittering Tennessee: Distributed Networks and Collaboration Following a Technological Disaster*,[3] in which the manager of the Risk and Disaster Documentation Center adds that crises favor the emergence of a network of inspectors, the digital volunteers that make up Virtual Operations Support Teams (VOST)[4] appear throughout the world and carry out social media surveillance precisely for that purpose.

If we look at Spain, in August 2012 the digital volunteers in Spain's emergencies imported the VOST model from the United States, where it was created by Jeff Philips in 2011. It was imported to fight against wildfire hoaxes in Carlet, Cortes de Pallas, Guia de Isora and other areas that were devastated in Spain. Dangerous information was being circulated in those regions, creating social alarm. Among other hoaxes, it was rumored the fire was five kilometers from the Cofrentes nuclear power plant, and that chainsaws were needed to control a fire. What would have happened if a hoax like that had not been refuted and hundreds of citizens had got into their cars with chainsaws, turning up at the control post trying to bring a fire under control? To avoid these situations, a group of emergency professionals set up VOST Spain in 2012, with then-Press Manager of the Madrid 112 service Luis Serrano, Fire Analyst Javier Blanco, Civil Protection Officer Rafael Galvez Rivas, and Medical Emergencies Officer Juan Luis de Castellvi, among others.

The main task of the VOST digital volunteers, which are grouped into help teams, is compiling, authenticating and integrating information from a variety of sources during disasters. Thousands of volunteers, in coordination with emergency services from the United States to Australia and the heart of Europe, work to aid civil protection and advise people on how to protect themselves in crisis situations.

If the principal feature of social networks is their enormous capacity to spread messages, VOST works to use that ability to convert Twitter into an ally for civil protection.

As Will Oremus pointed out in *Building a Better Truth Machine*[5] in December 2012, "A redeeming feature of Twitter is the relative speed with which its users manage to sniff out and debunk the most widely circulated falsehoods." Therefore, we must make responsible use of this powerful tool and supervise how it is used by anyone interested in fabricating alternate versions of the truth to suit their interests.

[1] *https://www.newyorker.com/culture/sasha-frere-jones/good-things-about-twitter*

[2] *https://www.buzzfeed.com/jwherrman/twitter-is-a-truth-machine?utm_term=.bkG8dbpbR#.hnDVw0P0o*

[3] *https://www.researchgate.net/publication/228639820_Twittering_Tennessee_Distributed_Networks_and_Collaboration_Following_a_Technological_Disaster*

[4] *https://vost.es/*

[5] *http://www.slate.com/articles/technology/future_tense/2012/12/social_media_hoaxes_could_machine_learning_debunk_false_twitter_rumors_before.html*

"STRATEGIZING" *corporate* DISPUTES

Javier Robalino

Managing partner of FERRERE Abogados Ecuador / Ecuador

In this age of hyper-connectivity, a corporation cannot face litigation without a solid strategy. There is no room for improvisation. This requires planning and laying down the foundation for the dispute strategy: the dispute must be "strategized."

> *"In this age of hyper-connectivity, a corporation cannot face litigation without a solid strategy. There is no room for improvisation*

Corporate disputes require skills that were not common until recently. A multinational, multilatina or local enterprise requires planning, anticipation, financing and/or mitigation of the effects of its disputes. Not all disputes can be settled out of court, so companies should try to apply good prevention practices to reduce and improve their litigations. And there will certainly be better litigations, obviously without guaranteeing a successful outcome. The best litigations will be those that have been "strategized."

So, corporations need to face disputes with sound tools, adequate information and budgeted economic resources. We set out below some ideas or suggestions for "strategizing" a corporate dispute in this hyperconnected era.

DEFINE THE GOALS

What does the corporation hope to obtain with this litigation? Litigation is not a goal in and of itself. Litigation serves a corporation's goal, such as obtaining compensation for damages, defending a market, ending a legal relationship, eliminating a contingency, etc. It is important to understand and define the aim of the litigation and stick to that goal.

IDENTIFY STAKEHOLDERS, THEN MAP THEM AND ASSIGN LEVELS OF IMPORTANCE

The stakeholders of a dispute must be identified—that is, those with an important role in it. Different methodologies consider the following steps:

- Identify parties. The parties must be listed, including both natural and legal persons.
- Define profiles. It is important to know who your allies and enemies are, as well as their backgrounds, experience levels, etc.
- Assign levels of importance. In a stakeholders' map, each player has a level of influence (high, medium or low), affected by their role, position (neutral, for or against) or situation.

IDENTIFY AND ASSESS WEAKNESSES OR RISKS

A corporate dispute may be longstanding and have numerous contracts, sophisticated contractual clauses, etc. Therefore, it is important to start from a humble, critical and realistic point of view. A leader must approach the problem objectively, without prejudice or passion that could cloud their judgment and with the ability to make decisions as to what is best for the corporation.

Review and analysis of both weaknesses and present or future risks involves two exercises:

- Due diligence (the past). The company and its legal, technical and/or financial advisers must study the dispute's evolution in terms of relationships, events and/or contracts to try to identify events that might weaken the corporation's position in the litigation. Those events must then be assessed and prioritized within an integral strategy.

- Identification of future risks. Going into a dispute—as either plaintiff or defendant—is an important decision. Proceedings can often have unforeseen consequences (e.g., a hefty counterclaim or reputational damage). A reasonable and sensible strategy must consider and assess future risks.

Past and future risks must be factored into the strategy's equation and considered in the final decision.

"It is important to start from a humble, critical and realistic point of view. A leader must approach the problem objectively, without prejudice or passion

IDENTIFY AND ASSESS STRENGTHS

Just as with weaknesses, strengths must be assessed. These strengths could also be classified as past or future. What is most important is to understand them, establish their importance and be able to use them to support the litigation.

PROTECT INFORMATION AND FILES

Information is the basis of any dispute, and it must be protected, taking into account the jurisdiction in which it is situated. We suggest considering an information protocol, including backing up the information (preferably via digital means) and establishing, in concert with legal advisers, rules of privilege for the information. Internal training is usually highly recommended.

HANDLE COMMUNICATIONS

A complex dispute requires adequate handling for both internal and external communications to (i) avoid improvising messages, (ii) administer communications according to the goal and (iii) adjust communications according to opportunity and audience.

It is crucial to have an agile, flexible communicator available. With that communicator's support, the leader must name and train spokespeople; build internal and external messages; and develop positioning statements, talking points and Q&As, all with the aim of administering communications for internal or external audiences.

"STRATEGIZING:" IMPLEMENTING THE STRATEGY

The activities explained above are focused on preparing the strategy. They are the strategy's foundation and, at the same time, the minimum requirements for achieving a holistic plan.

Once it has been "strategized"—i.e., the strategy's foundation has been defined—the corporation will be in a position to apply the strategy to the dispute. It should be based on the corporation's goal, consider the stakeholders and their evolution, take strengths and weaknesses into account at all times, look after and use available information and administer communications. This will enable it to better face the dispute and increase the probability of mitigating its effects, or even achieving a successful outcome, be this an end to the litigation or a satisfactory settlement.


16
28
16
28
14
28
31
14

USTO +1

JOSE ANTONIO ZARZALEJOS' INTERVIEW OF
CARLOS PADRÓN ESTARRIOL
Psychiatrist from the Faculty of Medicine of the University of Geneva (Switzerland)

Padron (born in Santa Cruz de Tenerife, 1938) is a **medical doctor with a specialty in psychiatry** who trained at the Faculty of Medicine of the University of Geneva, sharing the department with well-known Spanish psychiatrist Julian de Ajuriaguerra. He was a psychiatrist at the Psyco Social Universitarie Center in Geneva, where he became the clinical chief. He taught at Geneva University's School of Social Studies, also specializing in criminal psychiatry and psychoanalysis. Upon his return to Spain in 1973, he began organizing the psychiatry section for the Puerta de Hierro Clinic in Madrid. He has continuously taught at the Autonomous University of Madrid, where he was appointed head of the Psychiatry Department. Since 1980, he has devoted his time to clinical work, research and teaching at the Psychoanalytical Association of Madrid, a member of the International Psychoanalytical Association. He has written over a dozen publications—some in French—and is a speaker and lecturer at numerous conferences and seminars in the field. Among other distinctions, he has been awarded the Legion of Honor of the French Republic.

"New technologies have changed the parameters of ethics"

Carlos Padron does not lend himself to ordinary journalistic interviews. He has experienced and read so much and has so many interests that the only way to interview him is by holding a stimulating, and often fascinating, conversation with him. He is one of the very few Spanish psychiatrists to have practiced psychoanalysis, and he has a profound knowledge of human behavioral patterns. His work has consisted—and still consists—of understanding the depth of emotions and feelings, treating them in such a way as to bring out the best of each individual. So talking to him about vulnerability and the strength new technologies provide in present-day society, a subject on which he holds a profound, documented opinion, was a very enriching experience.

> "The vulnerabilities new technologies, especially social networks, expose us to has a name: lies. Over time, individual and collective weaknesses change, and now we face the spread of news we cannot check, generating mistrust and making us suspicious, and that are often false."

Are we vulnerable because there is a mass conveyance of lies?

> "Not only for that reason, but also because the experience of time has changed. Everything is faster, and the equation between what is urgent and important has been altered such that everything is peremptory and immediate, to the detriment of what is substantial or momentous. It is a very deep change in the norm: past, present and future, each of them linked to the others."

Padron continues, and I barely have to interrupt him with questions.

> "That new communication, that hyper-connection, is conducted through new languages, different from those used before. The problem is not whether the language is correct (the Royal Language Academy is there to sort that out), but that language is not only a system of communication, but something that also exerts a modeling effect on mental structures. Language remodels the mind and influences affections, feelings and emotions. All this runs a risk of being altered by new technologies. For example, does a tweet incorporate language? I don't think so. A tweet is the conveyor of a fact, true or otherwise, but it is not a sentence in an ordinary language in a conversation, and that affects how we understand what happens; it affects how the relationship between the external and internal worlds is organized; it affects the art of creating the world and society."

I wonder about this and ask him whether this is, perhaps, a very negative view of the contributions to our world from technology, digitalization of the economy and society.

> "No, it has positive aspects too, the greatest of which is that it stimulates creativity and assists knowledge. All the hazards of technological power must be neutralized with countermeasures—also technological—such that the solution lies in the problem. And that should be taken into account by states, societies and individuals. We are in a crisis situation, and crises are a breeding ground for creativity."

I mention states are arming themselves against cybercrime, cyberterrorism and political interference from other states.

> "Yes, that's why the countermeasures to neutralize the risks are within the technologies themselves. This has always happened in the past: there is a solution for every problem. There is, and should be, a tendency to make beneficial use of technology."

But Padron is, after all, a psychiatrist, and cannot disengage himself from his own experience, which I ask him about. Does digital dependence create harmful addictions?

> "Yes, of course it does. An addiction is the need to do something imperatively. But that drive is not enough to call it an addiction. In addition to the imperative, there is the increasingly more quantitative. In other words, a cellphone causes addiction not only because people look at them dozens and dozens of times a day, but because the number of consultations increases until it becomes an obsession. That is an addiction which, as such, is a pathology, and is treated psychiatrically. We do not do it in Spain, but it is done in the United States, for example, where psychiatry has reached certain extremes, such as treating dogs for anxiety. The therapy is behavioral, but it can become pharmacological."

Because it creates anxiety?

> "Yes, anxiety due to an information overload must be treated. Our brains aren't able to handle, to manage, such an enormous quantity of information. The brain is selective, grasping certain data for various reasons, such as affections or feelings of proximity. I repeat, the brain processes excessive information badly, because it does not manage to make certain associations—the most complex ones—and reacts by blocking decisions."

True, we live in an anxious society.

"As digitalization progresses, the generations using them are coming in and those who don't are dying off, so a time will come when everyone is using new technologies

"Excessive anxiety has a very negative quality. Namely, it blocks individuals, creating unease, confusion and information overload, which has a lot to do with all of this. Hyper-connection does not allow the brain to absorb so much data. But if you ask me about the most powerful effect social media and information technologies have had, I will say that it is, without doubt, the change in the parameters of ethics. Or to be more precise: it has become very difficult to make out what is ethical and what is not."

I guess it would not be a question of not knowing what is right or wrong, good or bad, but identifying it because everything comes in an unfiltered deluge. Padron nods.

"That's right."

I ask him about the social duality regarding new technologies—that is, the digital generations and those illiterate in this area. There must be a gap, I tell him.

"Social dualities have always existed. The one you mention has one characteristic: it is temporary. As digitalization progresses, the generations using them are coming in and those who don't are dying off, so a time will come when everyone is using new technologies."

But we will have to wait for that, I suggest.

"Yes, of course, but the end of that duality, that gap, is qualified by the fact that the new technologies appeal to the gregarious instinct of those who live in society. That is an irrepressible and often negative trend. Nazism, for example, was, among other things, a phenomenon of gregariousness, or herd instinct, despite its perversity."

What is the solution to the vulnerabilities to new technologies expose us to?

"I told you earlier it is lies, but I should also add lack of trust."

Padron's final appreciation effectively refers to an absolutely common phenomenon: citizens have adopted an attitude of caution, withdrawal and, in short, distrust. Padron reminds me that:

"We see some digital phenomena arising out of infuriation and anger. We must bear very much in mind that these tense, uncontrolled expressions separate and break, and those that arise out of love create ever-growing groups."

And naturally, this is what we need, for the instruments of progress to create groups of harmony, understanding and citizenship.

"Correct."

Padron agreed, while he showed me an essay that he was reading.

"I re-read the classics on ebook and the newspapers on paper."

He will shortly be a splendid 80-year-old and his lucid mind makes him a man in the prime of life. He is now engrossed in an essay that is fairly advanced, with the (provisional) title.

"*La creencia, lo religioso y lo sagrado. Ensayo psicoanalítico sobre el fanatismo*" ("Beliefs, the religious and the sacred. Psychoanalytical essay on fanaticism").

HYPERCONNECTED AND *HYPER-VULNERABLE*?
THE RISKS OF DIGITAL *Misinformation*

Alex Romero

Founder & CEO of Alto Data Analytics / Spain

INTERNET AND DIGITAL MEDIA

The consolidation of internet as a global phenomenon is unstoppable. The number of people in the world connected to the internet has more than doubled since 2009, going from 1.5 billion to 3.4 billion by the end of 2017. The social platform Facebook had 2.2 billion active users in the last quarter of 2017, which reflects the principal role of this player in the new internet ecosystem.

"Through our clicks we constantly contribute to a fantastic global business that brings together users, technology, data, advertisers and online service platforms

The internet is already essentially mobile. The global number of smartphones is over 2.8 billion, and of the 5.6 hours (on average) a U.S. adult spends connected to digital media and the internet each day, at least 3.1 hours are on their smartphone.

ADVERTISING AND MICRO-SEGMENTATION

The growth of the digital advertising business has closely followed the exponential growth of the population connected to the internet. In 2016 alone, online advertising exceeded $73 billion in the United States. 85% of the growth of this business was concentrated in two companies: Google and, mostly, Facebook.

We could think the business is now consolidated. All forecasts take for granted the global advertising costs spent on the internet has exceeded or is about to exceed those spent on television. However, the digital advertising business still has a long way to go. In the United States, though users spend more than 28% of their time on mobile devices, only 21% of advertising investment is currently spent on this medium. The business opportunity in mobile advertising is estimated at over $16 billion.

We are hyperconnected, and the great technological and social revolution brought about by the internet is founded on that hyper-connectivity. The digital giants feature an offer of mostly free services that enable them to collect huge volumes of data on those same hyperconnected users. This data, processed using algorithms, permits companies to offer sophisticated advertisers ways to profile their target audiences into micro-segments and precisely measure the effectiveness of their campaigns. Thus, data provided by users is the fundamental base of the business model.

> *"In a recent analysis for Bloomberg, major anomalies were detected in the shaping and development of the digital public debate*

HYPER-CONNECTIVITY AND MISINFORMATION: *YOU ARE FAKE NEWS!*

We are constantly bombarded with news and content through multiple digital contact points—social networks, digital media—but almost always through our favorite digital device, the cellphone, making the experience both personal and immediate. Thanks to that interconnection, through our clicks we constantly contribute to a fantastic global business that brings together users, technology, data, advertisers and online service platforms.

When we interact or distribute content, it is difficult to understand the full scope of our individual actions. How far do our likes go? What impacts do our retweets have? And to what extent do we understand the effect others have on us in the digital world?

In this hyperconnected society, the effects are not linear, but potentially exponential when what we do is amplified through the network to which we are connected.

This hyper-connectivity also makes us more vulnerable. It is easy to sense that in this context, just as anyone can be subjected to a micro-segmented advertising campaign, they can also be on the receiving end of a misinformation campaign.

We are constantly discovering, especially in the wake of the Facebook-Cambridge Analytica crisis, how strategic digital communications are used by state and non-state organizations to shake up and alter public opinion.

For example, in a recent analysis[1] for Bloomberg, focusing on Italian public opinion on immigration—which has proved to be a key factor in the latest elections—the Alto Data Analytics team detected major anomalies in the shaping and development of the digital public debate in the months before the elections, with a high polarization among those for or against immigration. Although those in favor were double the number of those against, their activity rate was 2.5 times lower. In other words, those against immigration were abnormally active, flooding the digital environment with their messages.

These and other similar dynamics contribute to raising the noise level in what has been defined as information pollution, a form of achieving misinformation.

In other words, our hyper-connectivity potentially exposes us to highly sophisticated, progressive manipulation and propaganda, to which we could unwittingly be contributing when we interact through digital media. The key question is: To what extent are we aware? And how much do we care?

[1] *https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/*

COMMUNICATIONS REFLECT *conscious* MANAGEMENT

Vanessa Silveyra

Manager of User Care and Services of ALEATICA / Mexico

Three years ago, ALEATICA commenced a transformation process that began with the incorporation of corporate governance, social responsibility and compliance policies and actions. During this stage of the transformation, I was invited to join the corporate team to oversee the well-being of the users and people in the firm responsible for providing mobility services.

"Our users place their trust in and pay for the services we provide, committing us to reciprocity

Our company provides the fundamental service of mobility, with over 287.1 overland kilometers under six concessions, roads with average daily traffic of 576,083 vehicles and 1.6 million tags accepted in 1,255 lanes on the most important motorways in the country; and air mobility for an average of 725,563 passengers each month at the International Airport of Toluca.

The users on our roads place their trust in and pay for the services we provide, which commits us to reciprocity to match the toll paid with top-quality service. Together with users, who must comply with the necessary self-care and safety measures, we are responsible for offering conditions necessary to better their lives and safety, as well as those of our operators.

To do this, we must have efficient, precise processes that consider the risks assumed, situations that occur and controls to prevent, detect and correct issues and risks. This practical sense of the operation and the pillars guiding the company are the key elements for developing conscious management.

Thinking of any other company in any other sector, quality of management is equally reflected in both the communications it issues and those received by its customers. On the one hand, company communications, as one of its internal and external functions, must be backed by actions, and the company must ensure it is coherent in what it says and does. On the other, communications a company receives are a projection of what it does and how.

For a company to have optimum management, it must believe it is doing things to serve the greater good. In our current case, that means serving people. If our everyday activities focus on that goal, our work takes on a new dimension, and any function we perform becomes a personal and institutional mission.

Users let us know if what we do and say is clear, positive and useful for them and, in turn, for us. Users also amplify that message, since, thanks to the immediacy of social media, any company action is instantly discussed far and wide, affecting its reputation. It is impossible not to make mistakes; what is essential is to realize and do everything possible to remedy them.

Collaboration between areas and teams is vital to offering the best possible service through conscious management. Being familiar with the processes in each of these areas; identifying the nodal points in which collaboration is triggered and ensuring it occurs naturally, without restriction, personal ambition or limits on power; making sure the information flows, coordination happens and headway is made towards the solution… All of this is necessary to communicate what we are—not what we want people to think we are.

At ALEATICA, we belong to a sector that transgresses. We cross territories, and in so doing, we encroach on people's lives, which requires dialogue and agreement. We thus have an opportunity to make a positive impact on those lives. Doing so means every one of the parties involved in our sector is responsible for their actions, with each and every person performing our function.

In my case, the company has put me in charge of user services, which means I must endeavor to ensure management is conducted in accordance with the principles of integrity and be partial to decisions made for this purpose. However, the culture of doing things well, keeping within the law, rules, processes and approved metrics and sticking to the essential company pillars must penetrate all an organization's personnel.

"At ALEATICA, we belong to a sector that transgresses. We cross territories, and in so doing, we encroach on people's lives, which requires dialogue and agreement

Workspaces are where people have values and, therefore, may or may not adhere to the culture of lawfulness, civility, productivity, development and healthy coexistence. Therefore, a company's responsibility is enormous, vital for shaping the country and international business community we want to generate.

Our everyday work will determine whether we can turn the block of marble in our hands into a work of art we can be proud of, through which we convey who we really are, inside and out, assuming the privilege of serving and contributing while we generate jobs, connect places and people and work toward sustainability for our business and all those fortunate connections.

HYPER-DISPERSED

Werner Zitzmann

Executive manager of the Colombian Information Media Association / Colombia

One of the great challenges of communications today is, undeniably, brevity. To achieve it, one must be extremely precise, which requires a great deal of clarity. Nowadays, in the world of immediate obsolescence and disruptive circumstances, clarity—by definition—does not exist.

> *"In the gleaming environments of innovation, it has been assumed convenient to start from scratch, to reinvent oneself and think differently*

This difficulty raises an even greater challenge, consisting of the need to recover our awareness of the importance of fundamental principles and values as essential prerequisites when considering any human activity.

When it comes to principles, values and essential prerequisites, brevity and simplicity emerge from conceptual synthesis skills that can only be acquired through reflection, study, experience and wisdom.

In the gleaming environments of innovation, so widespread and fashionable, it has been assumed convenient to start from scratch, reinvent oneself and think differently. A dangerous simplicity, especially for young people, which has been misinterpreted as an insane invitation to improvise and be flippant.

The world where information technologies act as an unlimited repository of fonts and files has brought about a shift in the skills of comprehension, knowledge and analysis, giving way to those of data management as a methodological tool. That dynamic has become a patent for ignorance and intellectual frivolity, because, since knowledge stored can be accessed anywhere at any time, it no longer seems important to take it in.

The massiveness and immediacy of new technologies, coupled with the overwhelming dynamic of languages, users and contents that stretch beyond conscious comprehension, learning and retention snatch at us from the past, lose us in the present and shoot us into an uncertain future, one with uneasiness, confusion, anxiety and dispersion.

This is where media and communicators—those who have taken up the fight for freedom of opinion, analysis and reporting; the right to question; freedom of the press; journalism; and communication involving information, education, guidance, pedagogy, influence and representation—are called to unite behind a deep and constant warning of the inconvenience of social and cultural massification through hyper-connection and addiction to technology, per se.

For millennia, the transmission of knowledge was reserved for great minds, able to assume the responsibility and challenge of doing so while

contributing to its evolution. The oral tradition gave rise to imperishable languages, the production of physical registers gave rise to writing, and the construction of structures and preservation of libraries and spaces where knowledge could be immortalized gave rise to cultures.

We cannot now resign ourselves to allowing all this to become immaterial, reduced to a function on a smart device with which anyone, by clicking on a button, can believe they have and can use the knowledge of mankind. Many people consult sources that are largely discredited, irrelevant or inconclusive, often forming part of a chain marketing the interests of those who always capitalize on the naivety, superficiality and ignorance of others.

This strategy of constantly and massively connecting people with the largest amount of useless information possible, overloading their cognitive abilities, memories and reflections with purely commercial, banal interests, must be questioned by all those involved—that is, all of society.

In the middle of this machinery that keeps us hyper-dispersed—although it is true that we have never had a better world, so advanced, full of information, knowledge and participation—the future of mankind clamors for leaders, seeking media and communicators who are able to draw the attention of society and demand, every so often, that people pause to think, set a healthy pace for their reality and point it in the right direction.

> *"Media cannot succumb to the dynamics of immediacy, massiveness and financial hardship of the changing landscape. Their mission must take priority*

Media cannot succumb to the dynamics of immediacy, massiveness and financial hardship of the changing landscape. Their mission must take priority. Social leaders cannot allow themselves to be underrated. Those guides, news providers and opinion leaders must be the first to rescue the principles, values and essential prerequisites of the human race's reason for existence.

And to rehumanize this vital dynamic, a large dose of disconnection, balance and weighing will be required to support well-understood innovation processes and check the dispersion currently preventing us from seeing clearly.

CYBER-RISK AND CYBERCRIME: THE *GREAT CHALLENGES* IN THE CONTEMPORARY *business* WORLD

Olga Botero

Founding partner and director of C&S Customers and Strategy / Colombia

In the business world, we have always had to deal with risk management. There is no business with no operational, financial, market, strategic and reputational risks associated with it. But as we have become digitalized, more interconnected and dependent on technology and information, our attention has turned to cyber-risk. And associated with cyber-risk, there is cybercrime, where crimes threaten technology and information.

"It has been suggested that cybercrime will be more profitable than drug trafficking and the sale of illegal drugs, causing damages to the tune of $6 trillion by 2021

It is not easy to understand. In the past, we considered this the responsibility of technology areas, but we have since realized cyber-risk runs right through our organizations, always there. Its impact can be devastating and may have operational, financial and legal effects, as well as—what is most difficult for us to gauge—disastrous consequences for our reputations.

It is a matter that affects us all and in which the ultimate responsibility lies with managers and directors. For this reason, we must make an effort to understand it and prepare to tackle its effects.

WHERE DOES CYBER-RISK START?

Cyber-risk starts in the use of technologies and information, digital strategies and the ecosystem to which we are interconnected via the internet. We use information, operational and business technologies to automate and control what we do, develop products and services and direct our relationships with clients and third parties. Technologies disruptive to traditional business models give rise to new models, such as Cloud platforms, the Internet of Things (IoT), artificial intelligence (AI), machine learning and automation, leading us into a new industrial age. There is blockchain, which allows us to distribute processing more securely. There are platforms that allow us to have almost anything as a service (XaaS), including virtual assistants. There is interaction with devices by touch and voice, as well as visual.

Cyber-risks also arise from all the data we store and handle—mostly obscure data, which is to say, data we do not use or understand the meaning of. It is calculated that obscure data represents almost 70% of data stored today: e-mails, documents, contracts, text, structured and unstructured data.

"We must make the management of cyber-risk a priority in our corporations' daily work and the responsibility of the senior management or board of directors

Data that incorporates hidden messages we do not analyze or interpret where, by using big data tools, artificial intelligence, natural language processing and analytics, we could generate information that leads us to take actions. Highly provocative data for cyber-crime.

The risk is the possibility of financial loss, operational disruption or reputational damages, caused by faults in technology and information, systemic vulnerabilities or weaknesses or attacks by third parties, including internal individuals, states, hacktivists and hackers, among others. Ransomware, botnets and malware are terms we now read and hear in the media, that even we non-techies are able to understand.

HOW BIG IS CYBERCRIME TODAY?

There is no homogenous legislation for disclosing breaches and incidents or reporting associated losses—incidents that compromise the integrity, confidentiality or availability of information. In breaches, information is disclosed to unauthorized third parties. Huge figures are estimated. In Verizon's recent study, Data Breaches Investigation Report 2018, it is calculated that in 2017, there were 53,000 incidents and some 2,216 breaches in 65 countries, motivated primarily by financial interest (76%). Breaches vary according to the industry, but among the most affected were governments, the health sector, financial services and manufacturing. No geographical area or industry was spared. Almost three-quarters of breaches were committed by outsiders, and, although an incident only takes a few seconds, it takes us months to realize we have been affected. It is also rather disquieting that 4% of employees in our companies still click on malicious emails and phishing attempts.

It has been suggested that cybercrime will be more profitable than drug trafficking and the sale of illegal drugs, causing damages to the tune of $6 trillion by 2021, which is double the 2015 figure.[1] These are truly alarming numbers.

[1] *Cyber Security Ventures, October 2017*

WHAT MUST WE DO?

We must make the management of cyber-risk a priority in our corporations' daily work and the responsibility of the senior management or board of directors.

We must also:

1. Ensure we have a clear cyber-risk program, starting with identifying the information and systems we want to protect: the crown jewels. Identify the associated risks and mechanisms for managing those risks, be it through mitigation actions, rejecting them or transferring them to, for example, cyber-risk policies.

2. Focus not only on protecting information and technology, but also on strengthening our ability to detect, respond and recover, making ourselves resilient to possible incidents and breaches.

3. Convert people into our first line of defense, raising awareness of the huge challenge we face and making them parties to our protection and detection activities.

4. Store only the data strictly necessary to achieve our business goals, and control who can access it through strong authentication mechanisms. Encrypt as much as possible.

"Convert people into our first line of defense, raising awareness of the huge challenge we face and making them parties to our protection and detection activities

5. Include cyber-risk management and cybersecurity in our strategy and make security part of the design and operation of everything we do.

6. Do not forget the ecosystems used by third-parties, clients, suppliers and others. When we interconnect, the risk is aggregate, and as such, it increases the risk to our organizations.

Let's work together, both public and private sector, since this is the most effective way to confront the enormous challenge we face.

IOT: *INNOVATION*, *opportunity* AND *risk*

Emanuel Abadía

Country Head & Managing Director at Marsh Semusa / Panama

We live in a world characterized by unprecedented technological hyper-connectivity, and, as an intrinsic part of this, the Internet of Things (IoT) is an indisputable, irreversible convergence of the physical and digital worlds. The line between the two worlds is becoming increasingly fuzzy. The interconnection of billions of intelligent machines, operating systems, devices and sensors generates and receives an extraordinary quantity of information, with a direct impact on the structure of social spaces, interpersonal relationships and business models.

> *"Latin American companies' lack of awareness regarding the complex risks arising from being part of an IoT system is alarming*

Microsoft[1] recently announced a $5 billion investment in IoT over the next four years to offer its customers the tools to transform and innovate their own companies using interconnected solutions. Microsoft is just one of the thousands of visionary companies adapting and innovating in the face of this inevitable reality. To the extent that companies—regardless of size or industry—are able to assess, anticipate and prospect the risks emerging from this technological transformation, not only will they have greater control over decision-making regarding business security, continuity and sustainability, but this will also lead to greater innovations, increased returns and new commercial opportunities.

Marsh's most recent 2018 *Communications, Media, and Technology Risk Study*[2] (CMT) reveals fascinating results in risk assessment and the identification of IoT opportunities. For example:

- There will be 30 billion IoT devices connected on average by 2030, and the number could grow to over 100 trillion devices by 2050.
- 65% of respondent companies considered IoT to be a great opportunity in the short term (3-5 years), and 50% said that their organization has already created or provides products and services for IoT devices.
- 52% of risk professionals said they did not know whether the IoT products and services offered by their company were used by other companies.

The last percentage is particularly disturbing, as it shows companies' lack of awareness of the full risks' spectrum that come with being part of an IoT system, highlighting companies' ignorance of the financial losses in this area.

[1] *1https://blogs.microsoft.com/iot/2018/04/04/microsoft-will-invest-5-billion-in-iot-heres-why/*

[2] *https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/2018%20Communications%20Media%20and%20Technology%20Risk%20Study.pdf*

Almost 75% of survey respondents indicated their companies considered risk professionals to be key partners for innovation. Although that percentage is encouraging for risk management experts, we should not overlook the huge challenges of increasing our importance in the dynamic, evolving, disruptive world of technology. In other words, if we are to exercise a direct influence on companies' strategic decisions, we must reiterate and prove our expertise to lead discussions on how these technologies will affect our companies' risk profiles and commercial strategies. And if we hone in on Latin America, there are clear areas to work on.

- 74% of respondents in Latin America—versus 60% on a global level—indicated they needed more human talent with expertise in cybersecurity to manage and analyze the gigantic quantities of data generated by IoT solutions.

- 34% of respondents in Latin America did not have the necessary technical skills to guarantee the success of their IoT projects.

These figures are revealing, but unfortunately not surprising. When compared to other markets, we in Latin America are at a disadvantage when it comes to managing emerging risks, and even more in CMT risks. The reasons for this regional lag fall outside the confines of this article. However, the most recent Benchmark of Risk Management[3] summarizes the three main challenges to an effective, strategic implementation of risk management in Latin America: (1) Organizational culture and values (51%); (2) Its perception as a compliance, not strategy, issue (46%); and (3) The lack of key knowledge regarding its importance and the value it brings (46%).

"When compared to other markets, we in Latin America are at a disadvantage when it comes to managing emerging and CMT risks

Faced with this regional landscape, what must risk specialists do to lead change and exert a direct influence on strategic decisions in companies?

- Conduct ongoing training, local market research and comparative studies to position ourselves as leaders on the subject. As the saying goes, the truly transformative changes come from within. We will thus be able to implement measuring and prospecting tools strategically and efficiently and, above all, customize solutions to suit each client's needs.

- Latin American companies' lack of awareness regarding the complex risks arising from being part of an IoT system is alarming, especially when coupled with their ignorance of how to manage and analyze the overwhelming quantity of data IoT solutions generate. The latter, in addition to the lack of up-to-date IT infrastructure, is even more worrisome when companies in the region have a shortage of human talent trained in cybersecurity, technological transformation and data science and analysis. Our role, therefore, is to insist on the importance of risk management as an integral, decisive process in all areas of the company.

[3] *https://www.marsh.com/pa/es/insights/research/iii-benchmark-de-gestion-de-riesgos-en-latinoamerica.html*

Finally, it is essential to design an action plan that includes the incorporation of risk management experts in key areas of the business model, such as the management board, product development, integration of risk solutions in product and service offerings, attracting and training of human talent and promoting investment in risk mitigation technologies or applications.

The key is to insist on risk management as a strategic issue, proving its worth through its applicability in the company's organizational chart and, naturally, defining opportunities for growth and innovation.

LITTLE *TRUTHS* AND BIG *lies*

Roberto Dias

Editorial Manager of *Folha de São Paulo* Journal / Brazil

Absolute objectivity does not exist.

This is something one learns when venturing into journalism, as subjectivity emerges when deciding on the topic, focus and even photo of a piece, as well as what information should be omitted.

Despite these judgment calls, it is an overall technical process. Journalists are trained to discern between what draws public interest and what has too small an impact to deserve the sacred stamp of "news." They look for different versions of the same fact, listening to people affected or harmed by certain information. They try, sometimes arduously so, to translate their findings into a clear and interesting story.

Like many professionals, sometimes these journalists make mistakes. These errors, however, do not delegitimize or diminish the importance of their work, which serves as a guiding thread for the advancement of society. Unfortunately, the industry's most serious flaw is it has failed to convince society of this.

It is precisely at this information "blind spot" where the cancer known as fake news formed. After all, most people do not have the necessary tools to discern between professional journalism and blatant lies spread for political purpose, for example.

> *"Folha de São Paulo became the first major newspaper in the world to stop updating its Facebook page, believing the social media service distances its readers from what can be considered a universal goal of good journalism: quality information for as many people as possible*

This lack of public defense, so to speak, used to be a rather marginal issue now amplified by the growth of social media. Such platforms gave individuals a megaphone of a size previously known only by big media. Instead of fomenting the much discussed citizen journalism, it paved the way for a serious confidence crisis capable of eroding society.

WHAT TO DO?

A single actor cannot control the problem, but the way out largely depends on the industry itself.

It will require more than just propagandizing the importance of professional journalism and its role in society. Neither is it limited to changing production and distribution chains to keep up with technology-driven changes to match new consumer behaviors. While these are not small tasks, they are not enough. It must be understood that content production takes money and the way to finance said production has changed radically.

These ideas must produce practical changes, because the quality of journalism is anchored in the financial independence of the company that houses it.

One of these changes is internal: the chain of incentives that has moved the gears of journalistic companies needs to adapt to this new reality. Another change concerns the relationship of content producers with the outside world. It will be necessary to be smarter than the perpetual concept of doing things in a specific way because "it has always been done that way."

This is the path Brazil's largest newspaper "*Folha de S.Paulo*" has tried to tread. Its decisions surprise and provoke debate when viewed in isolation but are embedded in easily understandable logic focused on defending their own production.

The newspaper was the first to adopt a "porous" paywall six years ago, a move that greatly predicted the country's market direction. Since then, it has been a leader in the defense of journalistic content copyright, making it difficult to copy content off their site and suing those who do so on a regular basis. The newspaper also assumed the rare position of refusing to provide free content for Facebook's Instant Articles platform.

More recently, it became the first major newspaper in the world to stop updating its Facebook page, believing the social media service distances its readers from what can be considered a universal goal of good journalism: quality information for as many people as possible.

But the courage to face this issue cannot be monopolized by a single entity, for it would be an inglorious battle, nor should the industry face it alone, since not even its strong will to defend its interests can take on a social issue of such magnitude.

Restoring a reasonable clarity level with regard to the information circulating across countries requires changing the social media business model. There is no middle ground here. It is useless to expect the initiative to come from companies themselves, for reasons that by now should be clear. It is urgent the State act, even with all the risks involved in this type of interference. It is necessary to create within social media ways to hold people responsible for disseminating false information, so the incentives for this practice are significantly diminished.

Elections are an appropriate time for this kind of public action, not only because of the role journalism plays in the decision-making of millions of people, but because the line between disinformation out of ignorance and lies programmed to reach a large number of voters is less blurred. Countries such as Brazil, with 150 million voters and a population highly engaged in the use of social media, have a very important chapter ahead on the future of democracy and professional journalism.

THE NEW *PARADIGM* FOR *crisis and risk* COMMUNICATIONS

Iván Pino
Partner and senior manager of the Digital Area at LLORENTE & CUENCA / Spain

Luis Serrano
Global leader of the Crisis and Risk Area at LLORENTE & CUENCA / Spain

We are experiencing a change in the communications paradigm. Society has become digitalized. Citizens, as pointed out by cyber-anthropologist Amber Case, have become cyborgs by virtue of their mobile extensions. Smartphones have changed how we obtain information and relate to our surroundings. We are connected from the moment we get up until we go to bed. True, we are changing the ways in which we establish these connections. Before, we interacted more through open social networks, which took up a lot of our free time. We are now more focused on seeking quality information, perhaps tired of spending so much time on these networks. Therefore, we now pay more attention to *dark social*, referring to closed, interpersonal instant messaging networks, according to a recent study by Buzzsumo.[1]

> *"Hyper-connectivity makes it impossible to separate crisis evolution and management from a digitized scenario*

The hyperconnected world in which we live offers enormous benefits in terms of instant access to information, wherever we are. We have access to such a large volume of information that we are unable to digest the details when thousands of fresh news items replace those the networks just served. It is this same hyper-connection that has made society hyper-vulnerable—hyper-vulnerable to misinformation, hoaxes, rumors and all kinds of cyberattacks.

Cyborg-citizens are also cyber-employees. Thanks to their mobile extensions, they have become unauthorized company spokespeople. We experienced this in May 2017 with WannaCry. Employees disclosed confidential information through *dark social*—the same employees who have become the priority vulnerability vector through which hackers gain access to the hearts of businesses through emails and, nowadays, essentially via smartphones. So, society's digital transformation into a transmedia communications environment produces cyborg citizens who are genuine risk vectors. This is no longer a small enemy. Any of us can be the origin of a serious reputational crisis for a brand.

The continuum of the crisis we are in, to quote Jose Manuel Velasco, has led to a scenario of distrust in institutions, companies and their messages. General belief in the system has been undermined. Cyborg-citizens have grown suspicious and skeptical. Everything is now questioned and analyzed. The business model for crises in media has contributed to this. Underfunding in editorial offices has led to less rigorous reporting and serious errors in news productions that have affected all the media, including even known quality press.

[1] *http://www.elmundo.es/papel/futuro/2018/03/06/5a9d3897e5fdeacb398b45d5.html*

Cyborg-citizens have organized themselves into a new system of digital communities. They chat within territories. The leaders of the communities they live in direct the conversation and act as standardbearers for their common cause. Adequately mapping these communities and having a good knowledge of their conversations are essential, not only to identify risks and opportunities, but also to forge alliances (especially with their leaders) and try to neutralize the enemy.

CYBERSPACE AS THE NEW BATTLEFIELD DURING CRISES

Crises have mutated. They are nothing like they were 10 years ago, before the appearance of the first smartphone. Hyper-connectivity makes it impossible to separate crisis evolution and management from a digitized scenario. In fact, many crises are first made public through social networks. In other words, cyberspace is the chessboard on which the conflict will be settled, where cyberspace is considered to be the close connection between digital and analog space, where cyborg-citizens' relationships are conducted.

Our conversations can no longer be separated. They occur continuously, jumping from analog to digital and back. There are no online and offline crises, only crises settled in the analog-digital space through which we interact with our surroundings.

> *"Crises are asymmetrical and mutate rapidly. There are no longer online and offline, local and national crises; they are all able to mutate rapidly due to our hyperconnected cyberspace*

In this environment, crises are asymmetrical and mutate rapidly. There are no longer online and offline, local and national crises; they are all able to mutate rapidly due to our hyperconnected cyberspace. All crises are settled in a digitalized space, because citizens are cyborgs.

We have gone from a traditional conflict, where states strive to control citizens, to a new model. Earlier, conflicts were vertical and based on media control. It was an analog scenario, where data prevailed over emotions.

The new conflict model is multidirectional and digital. It is settled in cyberspace. Its evolutionary structure favors social distrust, the questioning of shared beliefs, changes in values and the undermining of the system. They are conflicts inoculated from the top down and bottom up, mutating rapidly through multiple platforms with global consequences, where the main viral vectors are emotions.

The major global crises are often hybrid. Major crises may develop through combined actions that may include, alongside traditional military methods, manipulation of information or economic pressure, coupled with cyberattacks to generally destabilize the system. The alleged Russian interference in the last U.S. electoral campaign is just one example of this.

The new crises are fast and self-replicating. The ability to grow exponentially and get out of control in just a few minutes makes an immediate response capacity essential to successfully implement any prevention policy or action. Constant risk monitoring through a complete early detection and alert system is vital for organizations. Technological solutions that analyze huge packages of data and automated screening processes are crucial.

Moreover, crises feed off and deepen one another autonomously. They often self-replicate in a random and uncontrolled fashion. Once again, this is an effect of the cyber scenario in which they develop, driven by cyborg-citizens.

UNO´S
AWARDS

SILVER WINNER
In the category
Best In-House Publication

EIKON AWARD 2016
In the category
Institutional Publications - Multimedia

2016 AWARD OF EXCELLENCE
In the category
Websites - Magazine

SILVER WINNER
In the category
Design – Illustration

GRAND WINNER
In the category
Best Overall Magazine Presentation

GOLD WINNER
In the category
Best In-House Publication

LLORENTE & CUENCA

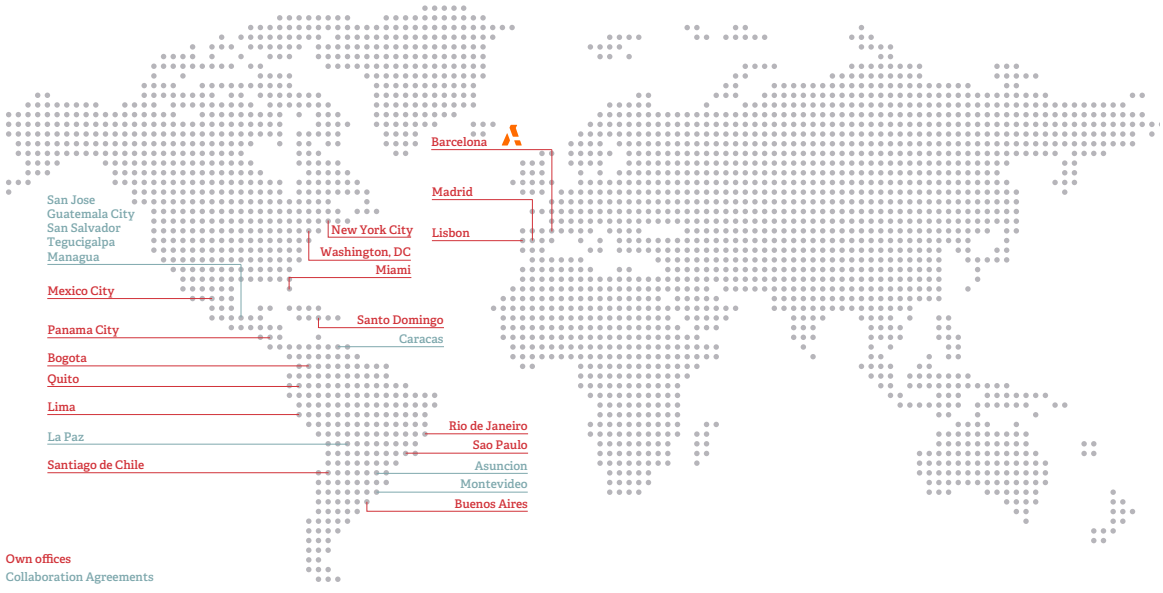
LLORENTE & CUENCA is the leading **reputation management, communication, and public affairs** consulting firm in Spain, Portugal, and Latin America. It has 21 partners and more than 500 professionals who provide strategic consultancy services to companies in all industries, with operations aimed at the Spanish-speaking and Portuguese-speaking world.

LLORENTE & CUENCA currently has offices in **Argentina**, **Brazil** (São Paulo and Rio de Janeiro), **Colombia**, **Chile**, **Ecuador**, **Spain** (Madrid and Barcelona), the **United States** (Miami, New York, and Washington DC), **Mexico**, **Panama**, **Peru**, **Portugal**, and the **Dominican Republic**. It offers its services through affiliates in **Bolivia**, **Paraguay**, **Uruguay**, **Venezuela**, **Costa Rica**, **Guatemala**, **Honduras**, **El Salvador** and **Nicaragua**.

LLORENTE & CUENCA is member of AMO, the leading global network in corporate and financial communications. Other partners are: **Maitland** in the United Kingdom; **The Abernathy MacGregor Group** in the United States; **Havas Worldwide** Paris in France, Belgium and Dubai; **Hirzel.Neef.Schmid. Counselors** in Switzerland; **SPJ** in the Netherlands; **Porda Havas** in China; **NATIONAL Public Relations** in Canada; **Hallvarsson & Halvarsson** in Sweden; **EM** in Russia and **Deekeling Arndt Advisors** in Germany. Every year, AMO is ranked in the top of the Advisors Global Ranking of M&A, conducted by Mergermarket.

amo
strategic advisors

www.amo-global.com



CORPORATE MANAGEMENT

José Antonio Llorente
Founding Partner and Chairman
jallorente@llorenteycuenca.com

Enrique González
Partner and CFO
egonzalez@llorenteycuenca.com

Adolfo Corujo
Partner and Chief Talent and Innovation Officer
acorujo@llorenteycuenca.com

Carmen Gómez Menor
Corporate Director
cgomez@llorenteycuenca.com

Juan Pablo Ocaña
Director of Legal & Compliance
jpocana@llorenteycuenca.com

MANAGEMENT - AMERICAS

Alejandro Romero
Partner and CEO Americas
aromero@llorenteycuenca.com

Luisa García
Partner and COO Latin America
lgarcia@llorenteycuenca.com

José Luis Di Girolamo
Partner and CFO Latin America
jldgirolamo@llorenteycuenca.com

Antonieta Mendoza de López
Vice President of Advocacy LatAm
amendozalopez@llorenteycuenca.com

TALENT MANAGEMENT

Daniel Moreno
Chief Talent Officer for Europe
dmoreno@llorenteycuenca.com

Karla Rogel
Chief Talent Officer for Northern Region
krogel@llorenteycuenca.com

Marjorie Barrientos
Chief Talent Officer for Andean Region
mbarrientos@llorenteycuenca.com

Laureana Navarro
Chief Talent Officer for Southern Region
lnavarro@llorenteycuenca.com

SPAIN AND PORTUGAL

Arturo Pinedo
Partner and Managing Director
apinedo@llorenteycuenca.com

Goyo Panadero
Partner and Managing Director
gpanadero@llorenteycuenca.com

Barcelona

María Cura
Partner and Managing Director
mcura@llorenteycuenca.com

Óscar Iniesta
Partner and Managing Director of Arenalia
oiniesta@llorenteycuenca.com

Muntaner, 240-242, 1º-1ª
08021 Barcelona
Tel. +34 93 217 22 17
Tel. Arenalia +34 660 201 020

Madrid

Joan Navarro
Partner and Vice-president of Public Affairs
jnavarro@llorenteycuenca.com

Amalio Moratalla
Partner and Senior Director of Sport and Business Strategy
amoratalla@llorenteycuenca.com

Iván Pino
Partner and Senior Director of Digital
ipino@llorenteycuenca.com

Lagasca, 88 - planta 3
28001 Madrid
Tel. +34 91 563 77 22

Impossible Tellers

Ana Folgueira
Managing Director
ana@impossibletellers.com

Lagasca, 88 - planta 3
28001 Madrid
Tel. +34 914 384 295

Cink

Sergio Cortés
Partner. Founder and Chairman
scortes@cink.es

Muntaner, 240, 1º-1ª
08021 Barcelona
Tel. +34 93 348 84 28

Lisbon

Tiago Vidal
Partner and Managing Director
tvidal@llorenteycuenca.com

Avenida da Liberdade nº225, 5º Esq.
1250-142 Lisboa
Tel: + 351 21 923 97 00

UNITED STATES

Erich de la Fuente
Partner and CEO
edelafuente@llorenteycuenca.com

Miami

Erich de la Fuente
edelafuente@llorenteycuenca.com

600 Brickell Avenue
Suite 2020
Miami, FL 33131
Tel. +1 786 590 1000

New York City

Gerard Guiu
Director of International Business Development
gguiu@llorenteycuenca.com

Abernathy MacGregor
277 Park Avenue, 39th Floor
New York, NY 10172
Tel. +1 212 371 5999 (ext. 374)

Washington, DC

Ana Gamonal
Director
agamonal@llorenteycuenca.com

10705 Rosehaven Street
Fairfax, VA 22030
Washington, DC
Tel. +1 703 505 4211

MEXICO, CENTRAL AMERICA AND CARIBBEAN

Javier Rosado
Partner and Managing Director North Region
jrosado@llorenteycuenca.com

Mexico City

Juan Arteaga
Managing Director
jarteaga@llorenteycuenca.com

Rogelio Blanco
Managing Director
rblanco@llorenteycuenca.com

Bernardo Quintana Kawage
Non-Executive Chairman
bquintanak@llorenteycuenca.com

Av. Paseo de la Reforma 412, Piso 14,
Col. Juárez, Del. Cuauhtémoc
CP 06600, Mexico City
Tel: +52 55 5257 1084

Havana

Pau Solanilla
psolanilla@llorenteycuenca.com

Sortis Business Tower, piso 9
Calle 57, Obarrio - Panamá
Tel. +507 206 5200

Panama City

Pau Solanilla
Managing Director
psolanilla@llorenteycuenca.com

Sortis Business Tower, piso 9
Calle 57, Obarrio - Panamá
Tel. +507 206 5200

Santo Domingo

Iban Campo
Managing Director
icampo@llorenteycuenca.com

Av. Abraham Lincoln 1069
Torre Ejecutiva Sonora, planta 7
Tel. +1 809 6161975

ANDES' REGION

Bogota

María Esteve
Partner and Managing Director
mesteve@llorenteycuenca.com

Av. Calle 82 # 9-65 Piso 4
Bogotá D.C. – Colombia
Tel: +57 1 7438000

Lima

Luis Miguel Peña
Partner and Senior Director
lmpena@llorenteycuenca.com

Av. Andrés Reyes 420, piso 7
San Isidro
Tel: +51 1 2229491

Quito

Carlos Llanos
Managing Director
cllanos@llorenteycuenca.com

Avda. 12 de Octubre N24-528 y
Cordero – Edificio World Trade
Center – Torre B - piso 11
Tel. +593 2 2565820

Santiago de Chile

Constanza Téllez
Managing Director
ctellez@llorenteycuenca.com

Francisco Aylwin
Chairman
faylwin@llorenteycuenca.com

Magdalena 140, Oficina 1801.
Las Condes.
Tel. +56 22 207 32 00

SOUTH AMERICA

Buenos Aires

Mariano Vila
Managing Director
mvila@llorenteycuenca.com

Av. Corrientes 222, piso 8. C1043AAP
Tel: +54 11 5556 0700

Rio de Janeiro

Cleber Martins
clebermartins@llorenteycuenca.com

Ladeira da Glória, 26
Estúdio 244 e 246 - Glória
Rio de Janeiro - RJ
Tel. +55 21 3797 6400

Sao Paulo

Cleber Martins
Managing Director
clebermartins@llorenteycuenca.com

Juan Carlos Gozzer
Regional Innovation Officer
jcgozzer@llorenteycuenca.com

Rua Oscar Freire, 379, Cj 111,
Cerqueira César SP - 01426-001
Tel. +55 11 3060 3390