

PROSEGUR RESEARCH

Hybrid Security





Index | Hybrid security



This is an interactive document



The changing world



01



The changing world

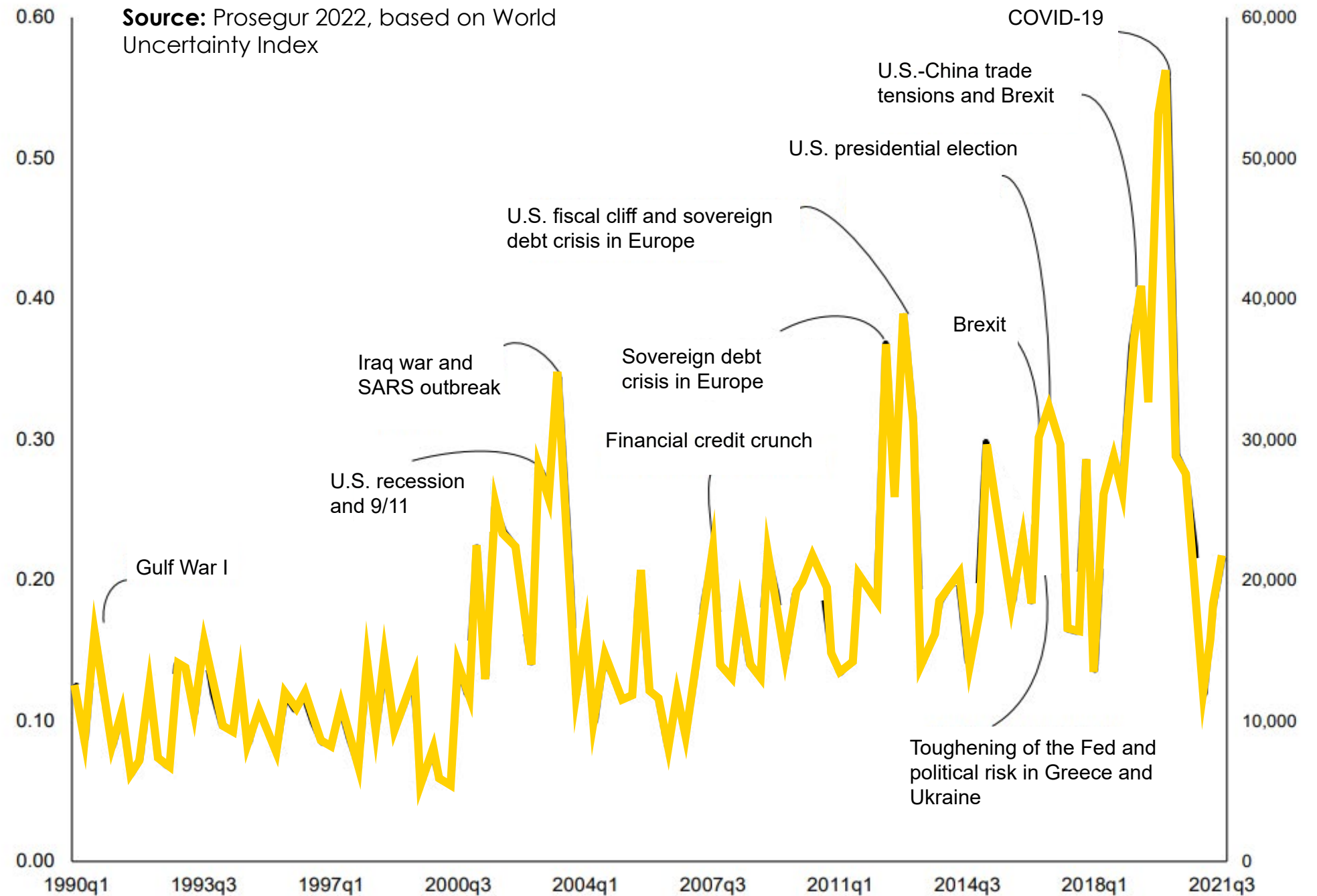
1.1. From the current uncertainty

As the French essayist and poet Paul Valery pointed out, the future is no longer what it used to be. With each present action, new alternatives and scenarios emerge. The future is being built and if this is not done strategically, the waves on the beach can turn into real tsunamis.

The disappearance of entire economic sectors, the working force quitting en masse (Great Resignation), the obsolescence of knowledge and the exponential reduction of time in the life cycles of goods and services are examples of change penetrating our present and rapidly approaching the future.

World Uncertainty Index

Source: Prosegur 2022, based on World Uncertainty Index





The changing world

1.1. From the current uncertainty



Ransomware



Political extremism disruptions



Pandemics and health crises



Extreme weather events



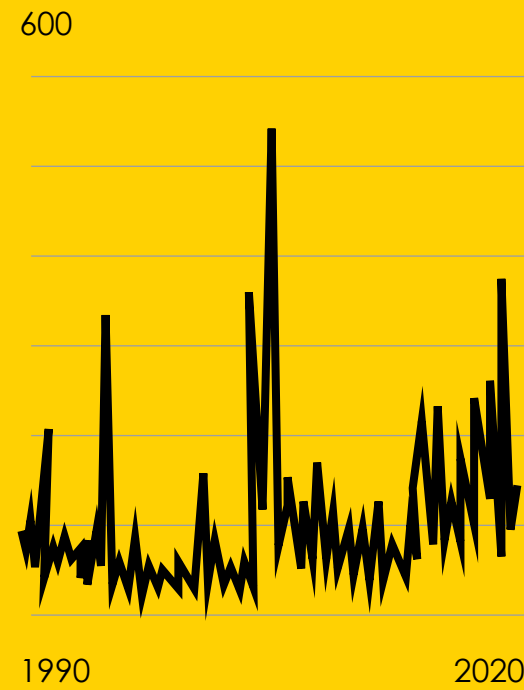
Supply chain crises



High-impact geopolitical conflicts

In parallel, a series of extreme events are destabilizing the world: massive ransomware cyberattacks, extremism, critical supply chain disruptions, extreme weather events, pandemics and conflicts such as the one in Ukraine place us in an environment where change is the constant. Uncertainty indices are at all-time highs, and we do not fully grasp the threats nor how, when and where they will materialize next.

Geopolitical Risk Index according to the Federal Reserve Board



Percentage of companies subject to one cyber breach per year



Number of natural disasters per year



Source: Prosegur 2022, based on Mckinsey, 2021

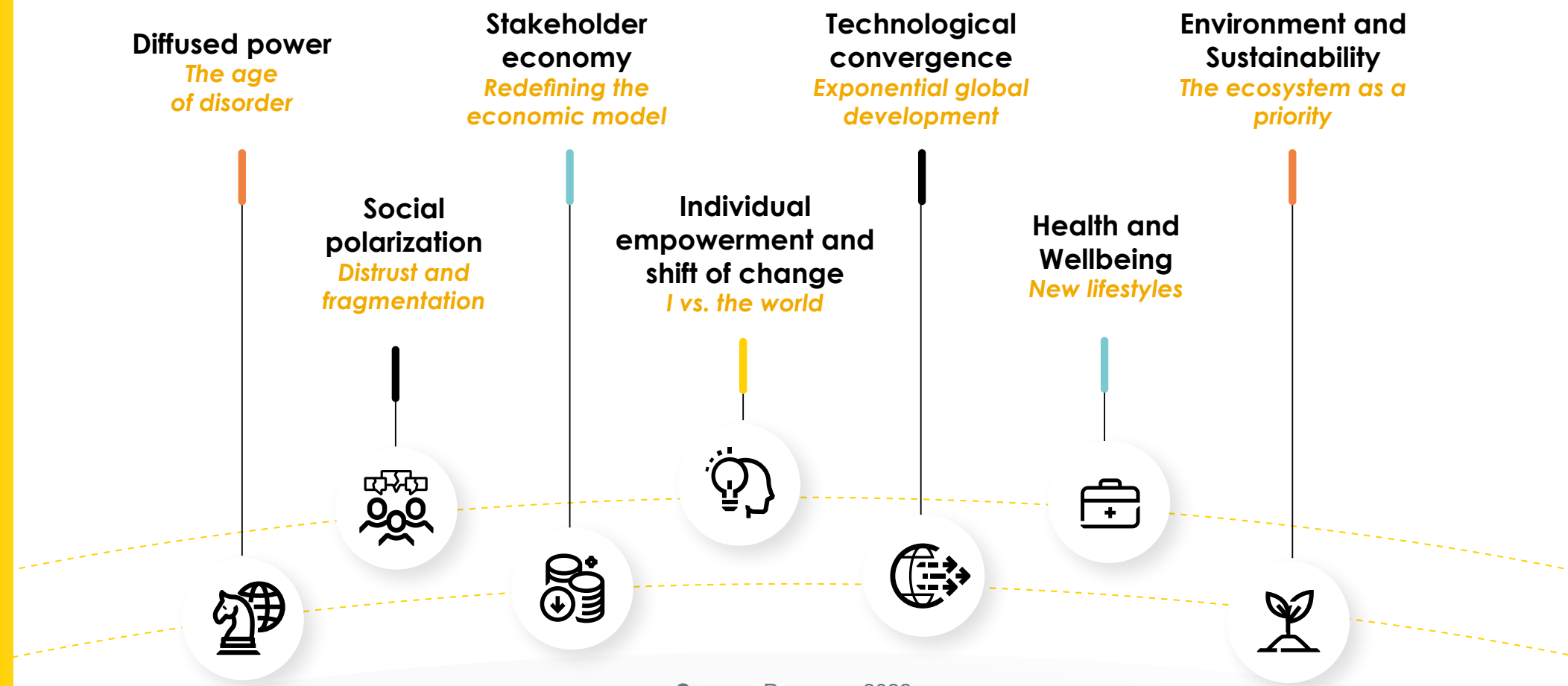


The changing world

1.2. To the 7 keys of future

In this context, Prosegur proposes to study the global trends through 7 keys to the future that allow us to organize the analysis and the monitoring of these changes. It is essential to study and interpret the facts and data at the present time, considered the interim: we are constantly encountering new trends while the old ones are still dying, some are disappearing and others are even recovering more strongly than in the past. We are in a period of latency where trends are rapidly transforming our world: restructuring society, reconfiguring political spaces, even making entire economic sectors appear or disappear. It is precisely **in this chaotic interregnum that opportunities arise**. In the face of rivalries, emergencies, power vacuums and crises, understanding transformations allows us a new approach, under which people, states and companies can completely renew themselves. In the security sector, understanding what is happening in the world becomes a critical issue, and transforming ourselves in conjunction with society is not an option: only by being part of the change can we adapt to the new needs of people and companies.

The document **7 keys of future** details this trend towards the uncertainty of the so-called “new normal”. The nature of the threats, where, when and how they may materialize, cannot be known with complete accuracy. The war in Ukraine is an example of a diffuse power conflict, with multiple repercussions it has had - and will continue to have - on security, economic, political and social issues, among others. In addition, new ecological risks such as the onset of COVID-19 in 2020 have a direct impact on other areas such as empowerment, prioritizing welfare and individualism over other currents such as collectivism. Coupled, in addition, with the increasing global inflation and economic difficulties, social polarization is postulated as one of the main variables for the maintenance of state stability, with other effects such as disinformation and information disorder. **disinformation and information disorder**.



Source: Prosegur, 2022



Security evolves
with society

02



Security evolves with society

2.1. Expanding the spheres it covers

Security is evolving along with society in a **context of great change**¹. Growing uncertainty places us in an environment of enormous challenges for individuals and companies², and logically we see how traditional risks are also evolving.

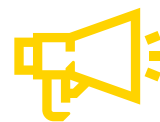
Thus, new risks make **security an evolving and ever broader concept**.

The following are examples of what is being incorporated in security management:

Supply chain attacks affecting business continuity



Cyber-attacks affecting corporate reputation



Attacks on critical or sensitive infrastructure



Intelligence to operate in geographic areas and economic sectors



Theft of data and information affecting industrial property



The concept of security has broadened its horizons as welfare states have developed and citizens have gained access to higher levels of well-being. Having primary needs covered, as far as possible, has led to an **increase in demand levels for security in traditional and emerging areas**.

From security focused on the protection of people, assets or goods, we have moved on to cover areas such as economy, environment, food, legal, data, information and technological security.

Damage to societies and companies is not only manifested through direct physical violence, which undoubtedly continues to exist. There also **new emerging risks**, often with a clear technological component³, which are increasingly diffuse, unexpected and disruptive.

¹ What has sociologically come to be called **Liquid Modernity**.

² As an example, we can cite the **Manual of Living in the Age of Uncertainty**.

³ An interesting read on the subject is **The future goes faster than you think**.



Security evolves with society

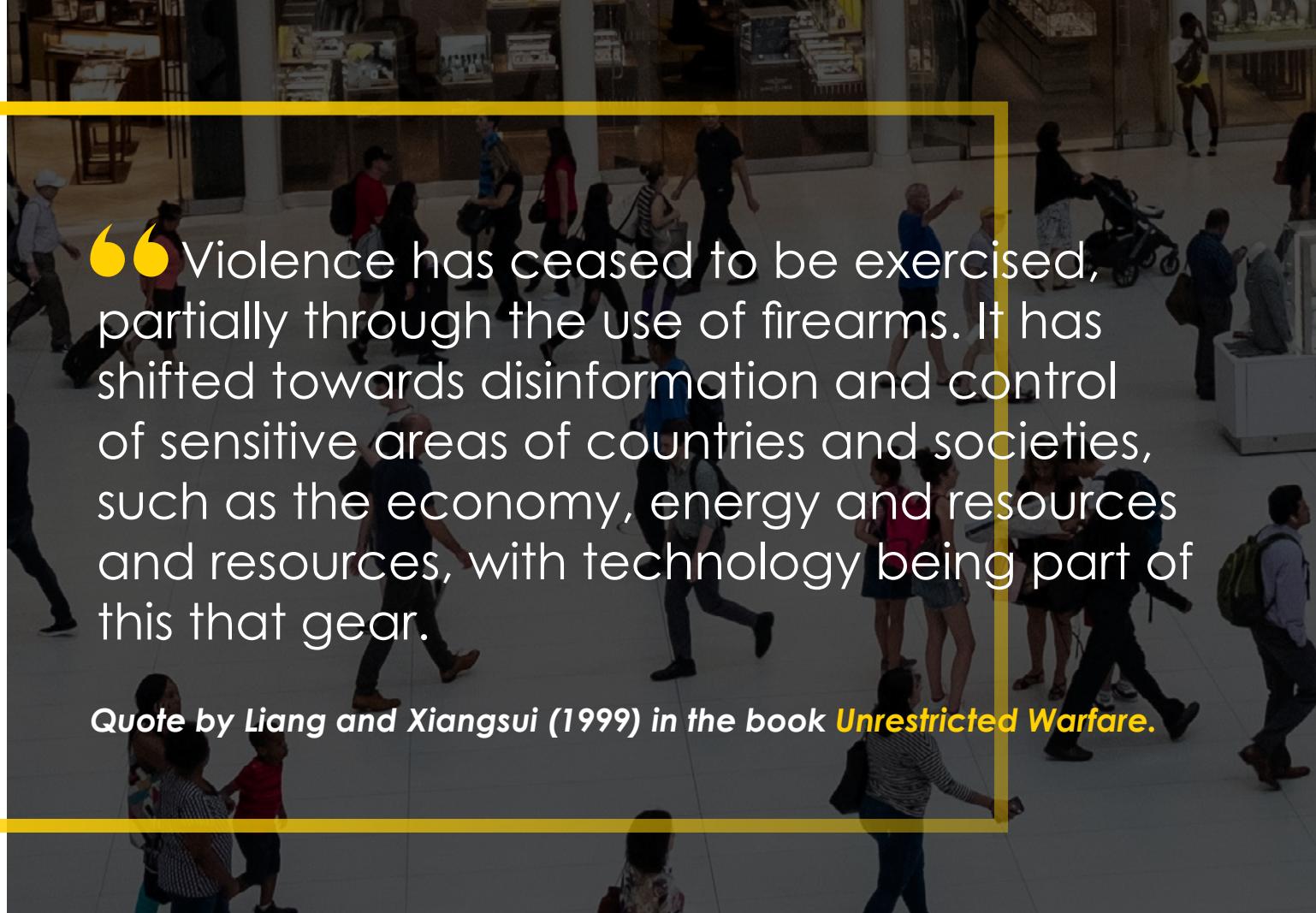
2.2. Facing hybrid threats

Security in today's world must be able to anticipate these risks⁴ in an intelligent and agile way, taking into account the significant diversity of threats from different spheres, sometimes resulting from the hybridization of different environments and actors. This implies working on **corporate foresight**, acquiring skills and abilities to detect patterns of change (exponentially accelerating, discontinuous and interdependent), interpret the impacts on the organization and propose long-term courses of action.

Therefore, we must be aware that we are facing **hybrid threats**. The use of drones by criminal and terrorist organizations, the use of 3D weapons for extremist attacks, criminal crowdsourcing through massive credit card theft, the use of a Security Operations Center (SOC) for a terrorist attack show that this hybridization is already a reality.

Transversally, technology empowers all kinds of processes and behaviors, giving rise to the emergence of new tools such as 3D printers and, consequently, new opportunities for crime, such as the attack in Halle (Germany) in 2019.

In this digital era, where technologies are the clear hub⁵ for growth and their development has been shown to be faster than could be expected, thus **presenting a great accelerated exponentiality**⁶, a nonlinear⁷ is required: only people who learn to take advantage of changes and drive themselves thanks to technological development will make that difference.



“Violence has ceased to be exercised, partially through the use of firearms. It has shifted towards disinformation and control of sensitive areas of countries and societies, such as the economy, energy and resources and resources, with technology being part of this that gear.

Quote by Liang and Xiangsui (1999) in the book **Unrestricted Warfare**.

⁴ The importance of anticipating these changes can be gleaned from the book **Corporate Foresight**.

⁵ As explained in **The Digital Future**.

⁶ We recommend reading **Exponential**.

⁷ For further reading, see **A Thousand Years of Nonlinear History**.



Security evolves with society

2.3. Challenging systemic risks

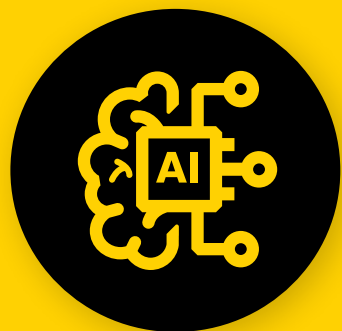
This technological era characterized by disruptive and frequent changes necessarily implies an effort to understand all the actors and forces driving change, thus moving away from the inflated relevance of current factors for future evaluations. It is no longer just a question of financial components, but also of social, environmental⁸, political, geoeconomics⁹ and technological factors, among others, in the short, medium and long term.

All of the above highlights the concept of **systemic risk**: any circumstance, anywhere, is susceptible to generating cascading impacts on nations, industries, sectors, etc. A conflict such as the one in Ukraine affects the activity of companies, global growth forecasts, increases world inflation, causes a food crisis that can lead to social discontent and new “springs” (demonstrations, strikes, etc.), generates opportunities for new forms of criminality, etc.

This means that there is a need to focus on **contextual intelligence**, that is, a need to pivot from risk management to risk intelligence, since any event, regardless of the place where it occurs, is likely to generate new opportunities for societies, governments and, of course, criminal networks.

⁸ As we can identify among the most prominent risks according to the *WEF (2022)*.

⁹ For more information, we recommend reading *The Fat Tail*.



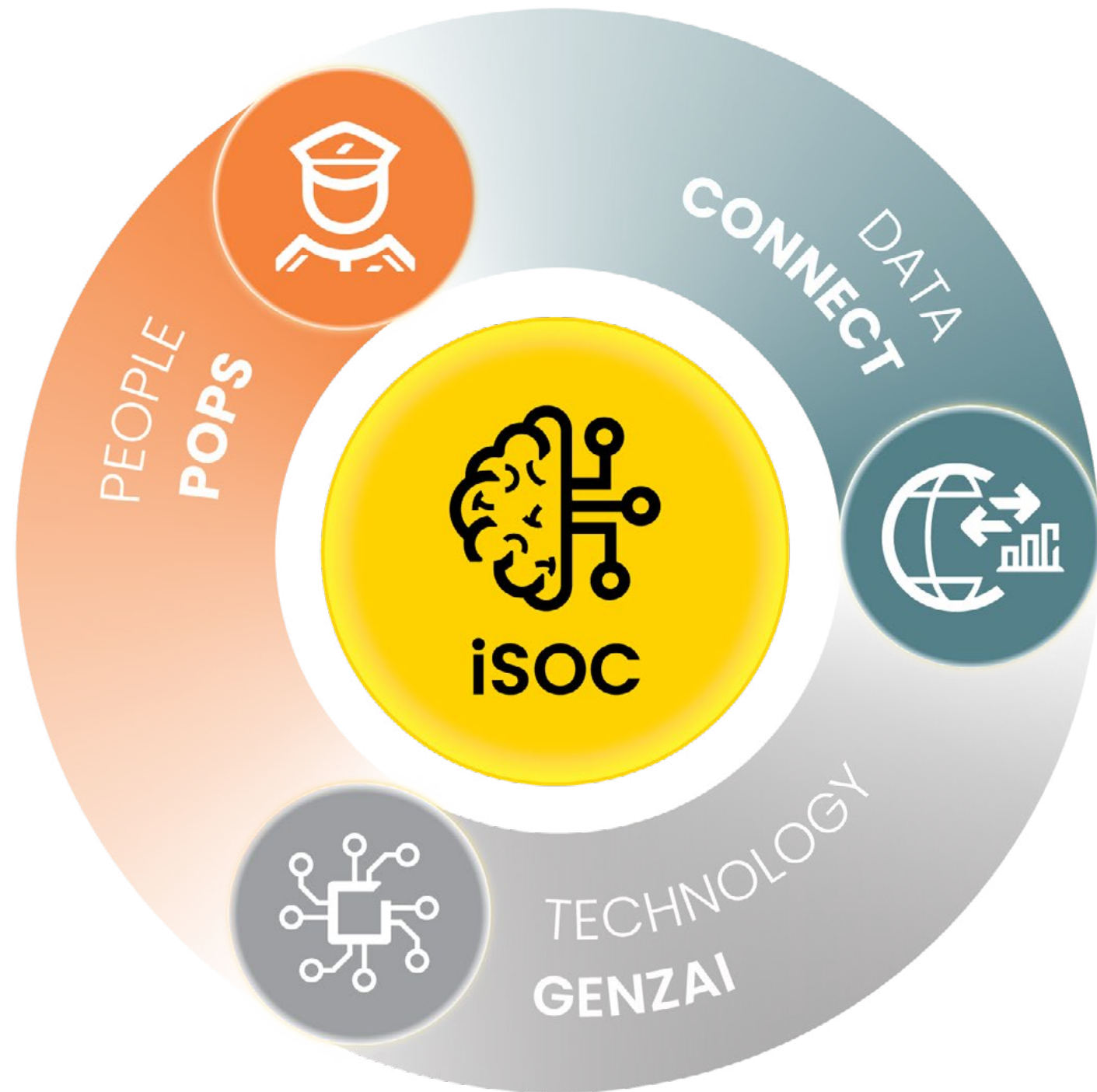
Our vision



03



3.1. Our security model for a hybrid world



In this changing world of hybrid threats and reconfiguration of security parameters, **Prosegur has coined the term Hybrid Security**, to provide security solutions “as a service”:

- That are **continuously adapted** to each client and their environment.
- Executed by **professional experts** with the most innovative **technology**.
- Powered by a **global data and intelligence model**.
- That allows to **anticipate and mitigate risks** by responding in the most **efficient way**.
- That adds **differential value** to the client’s business.

For all these reasons, Prosegur proposes the model that responds to hybrid security, in which **security experts are empowered through efficient and connected technologies that leverage data intelligently**; all this is only possible with the right foundation: an organization with purpose and culture, capable of aligning these three essential elements, through an Intelligent Security Operations Center (SOC) or iSOC.

The SOC is the brain from which the processes that interrelate people, technologies and data are activated, enabling efficient and agile decision-making that responds to the disruptive changes of today’s world.



Our vision

3.1.1. People as the priority

The real key lies in the perfect alignment between human resources¹⁰, endowed with experience and knowledge, technological means and data, all of which are organized for the common purpose of protecting people and businesses in a more personalized way.

In this sense, while technology is the lever of change, **the human factor is at the heart of success of hybrid security**, thanks to the skills involved such as critical thinking and flexibility. Human expertise and skills are irreplaceable since even the finest technological company cannot adapt to the dizzying pace of change that generates today's¹¹ risks without security experts.

Their contribution in terms of contextual intelligence allows us to understand the environment and their transformative intelligence brings innovation capacity to the whole model; these aspects are fundamental from a strategic perspective.

This is what the organization is looking for: to empower people with disruptive technologies. These experts must know ▶

¹⁰ More on the future of work in changing environments can be found in *Work is no longer what it used to be*.

¹¹ To explore more about people in the sector of technology, we recommend reading *More Plato and less tech*.

Experts on Security

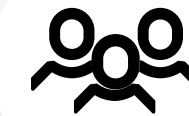
Professionals with extensive international knowledge and experience in risk management and security in adverse environments.

Digital competencies

Linked to the management of organizational technologies: artificial intelligence (AI), virtual reality (VR) blockchain, etc.

Human competencies

Such as complex problem solving, critical thinking, creativity, social influence, etc.



Self-management

To work in a volatile and continuously changing environment they require: resilience, stress tolerance and flexibility.

Source: Prosegur, 2022



Our vision

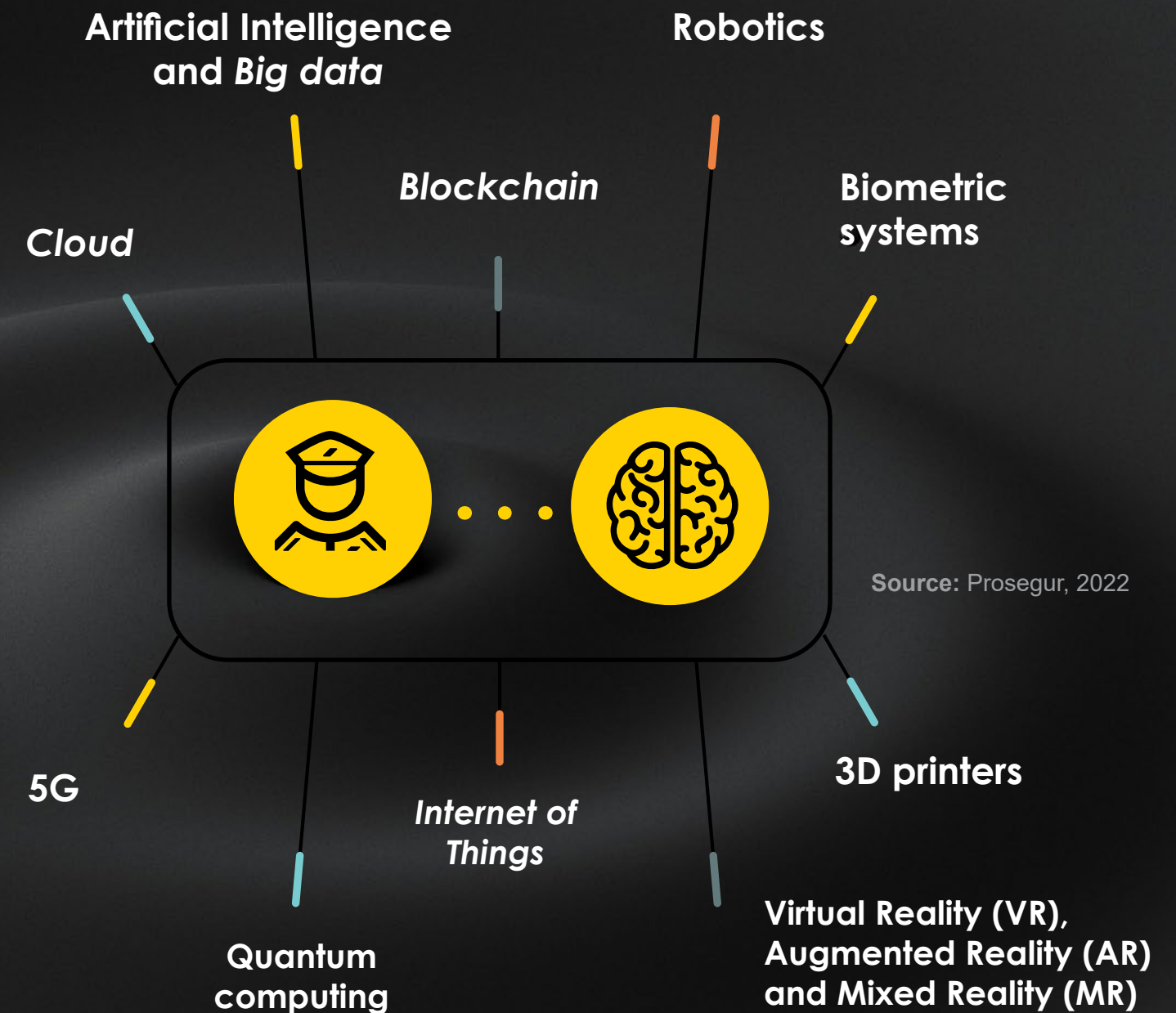
3.1.2. Technologies as the means

Technology is the great game changer of the future and will undoubtedly be one of the main sources for the emergence of **new risks and threats**, but also of business **opportunities and potential improvements** in services and products¹². We rely on technologies that are clearly tested and efficient, far from the usual technological hype:

- Technologies that act in physical environments both to execute tasks and to send information to our SOC: cameras, sensors, drones, alarms, networks and systems, robotics, etc.
- Technologies used in our SOC for information processing and analysis and support to decision-making: artificial intelligence, machine learning, data science, natural language processing, GIS models, cloud computing, virtual and 3D simulators.
- Developments to connect the physical and digital worlds and to interact with the inputs from various information sources and the final recipients of the end product (Genzai, Pops and Connect).

They are disruptive because they burst abruptly as productive forces given their **exponential growth**¹³ and are **convergent** because they enable and enhance each other, further accelerating technological development¹⁴.

When the accelerated quantitative processes reach a certain pace, a leap is generated, a qualitative change that impacts society. This is the true **transforming force of technology**.



¹² For more, the concept and book *Antifragile* is interesting.

¹³ An example of exponentiality is the time of use according to the generation of mobile connectivity: with 3G it took 45 minutes to download an HD movie, with 4G it takes 21 seconds and with 5G less time than reading this sentence (Diamandis and Kotler, 2021).

¹⁴ For example, the development of new drugs is accelerated not only by the exponential advance of biotechnology, but also by the application of artificial intelligence and quantum computing. Advances in drone construction also derive from the combination of machine learning, new materials and 3D printing.



Our vision

3.1.3. Data as the added value

Processing and working with data is no easy task, but it is undoubtedly an opportunity¹⁵ to make a difference with added value in the market¹⁶. It is a matter of analyzing strategically¹⁷ to detect early warnings and weak signals¹⁸, providing prospective vision that allows the adoption of appropriate responses in a timely manner to each incident and, at the same time, generating **ecosystems that interact intelligently** to protect people and companies in changing environments.

The management of high volumes of data allows the establishment of **global and peripheral visions**. It is a capability to be developed at **strategic levels**, based on active monitoring of the environment in order to detect threats and opportunities for organizations. Adopting these visions is what allows us to anticipate **criminal innovations**¹⁹.

¹⁵ On information and data, we recommend reading **Factfulness**.

¹⁶ Data is used to establish risks and identify threats, but it will always be a support system for security experts.

¹⁷ The book **Good Strategy, Bad Strategy** elaborates on a true strategic vision.

¹⁸ This is an observation or piece of information that appears to have no connection or relationship, but can be recognized as a possible pattern if viewed from another point of view or connected to other pieces of information. The detection of weak signals is done through environmental scanning, with capabilities such as peripheral vision and prospective orientation, as referred to by Ansoff in his study on **Managing Strategic Surprise by Response to Weak Signals**.

¹⁹ For example, knowing the thefts occurring in a particular store in a particular part of the country can provide useful information, but managing information on all the thefts occurring in all the stores of a particular business group throughout the country provides hitherto unknown business intelligence. This is how we can anticipate risks and reinforce the security that people and companies need today.





Our vision

3.2. The iSOC as the brain

This transformation and hybridization of the world creates new challenges and opportunities for the security of people and businesses. Consequently, Security Operations Centers (SOCs) are also evolving.

In this context²⁰, our model is based on iSOCs, Security Operations Centers with a differential “i”: with high-value information, international in nature, with an integrated capacity that provides innovation from an intelligent vision. They are all coordinated globally. The iSOCs encompass the integration of people, data and technologies in an intelligent, strategic and prospective manner. This allows us to leverage expertise to generate highly complex, more human-like processing than ever before.

In the hybrid security model, solutions are conceptualized in the iSOC through **sophisticated operational strategies** based on brain functioning²¹: the iSOC is the brain of the model. It allows us to know what is happening in the world in a very agile and adjusted to reality way, and to do so in a preventive and automated way to boost response efficiency. This is achieved by focusing our efforts on the following tasks:

- ▶ Promoting the configuration of a **global and unified** iSOC that contributes in an agile and efficient way to the hybrid security model, guaranteeing the security of people and companies working with global data.
- ▶ Cover the security needs adapted to the requirements of the companies and people affected, **customizing the solutions** without losing the ability to automate strategic improvement processes to generate intelligent responses.
- ▶ Encourage data analysis while **respecting privacy and giving coherence to the comprehensive** management of all organizations and individuals, a SOC that integrates the incidents of the present to protect a common future.

²⁰ Traditionally, SOCs have worked in an incident reaction format based on monitoring capabilities according to the information available. The truth is that from the 21st century onwards it veered towards a reactive monitoring approach with some capacity for vulnerability analysis of the environment. Later it was reoriented towards a proactive approach by applying intelligence to the study of threats. Finally, the inclusion of automated processes allows the inclusion of more complex external risk assessments and a certain degree of orchestration. For a brief but more specific review of SOCs read **ISACA, 2021**.

²¹ Because learning is an exercise in courage and perseverance, the book **Dare to Know** explains how the brain works.



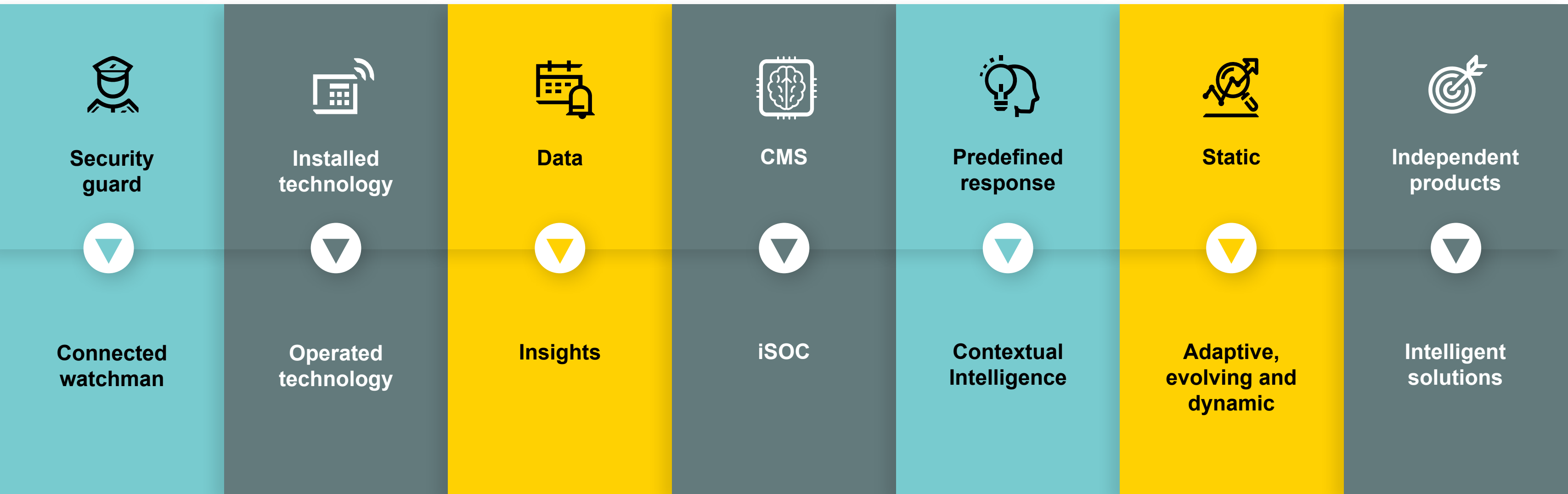
Our vision

3.2. The iSOC as the brain

If we place the iSOC in a corporation with a peripheral and prospective vision, in a model prepared for hybrid threats and changing environments, this brain must think in terms of the future.

Thus, a SOC ready for the future, something that every organization should aspire to, must be revolutionary and transformative, preparing every element of the hybrid security model for change.

Being able to transform people, technology and data, the vertices of its own model, into connected experts, operated and linked technology and insights that add **value in decision making**. This is what derives in a real transformation of the brain, from a response management center to an iSOC, working with contextual intelligence through an adaptive, evolving and dynamic approach; thus, for each problem of each person or business you will be able to find an integral, intelligent and unique solution.





Our vision

3.3. The foundation: an organization with purpose and culture

To accurately consolidate people, technology and data, an organization capable of delivering **security solutions “as a service”** and continuously adapting to people and business environments is essential.

- ▶ Executed by professional experts empowered with innovative technology.
- ▶ Powered by a global data and intelligence model that anticipates and mitigates risks.
- ▶ Responding in the most efficient way and adding value to the business.

Those businesses that have developed traditional security functions covering its various forms and assuming the complexity of risks over a long period of time will have a competitive advantage. Extensive experience to **innovation processes is the differential value**. Having significant security know-how focused on protecting people, homes, businesses and assets is the essence of the hybrid company, as it is the mandatory starting point for the digital transformation of its services.

The foundation of the hybrid security model is the intelligent organization²²: an enterprise that brings its organizational culture and purpose to protect people and businesses while learning from the environment in an expansive way.

²² On what an intelligent organization looks like, the book *Fifth Discipline* is recommended.



Leading hybrid environments



Leading hybrid environments

4.1. Tips for action

Creative²³, courageous and calm leadership will **make the difference** in disruptive environments, and will be key in hybrid security. Here are some tips for action:



²³ We recommend expanding on this idea by reading *Lessons in creative leadership*.



**The books we
have relied on
to build this
model**





The books we have relied on to build this model

**Human capabilities that
make technology work.
Technological capabilities
that make people smarter.**

PROSEGUR RESEARCH

research@prosegur.com
www.prosegurresearch.com