

# National Intelligence: Present and future challenges for enterprises in the era of rising technology

-By Manuel Balcazar (CESIG/ITAM)-

## I. General landscape

Security Intelligence at private sector has records to be present since 19<sup>th</sup> century, with Eastern Indian Company, since then intelligence has been present, more with an operational than strategic perspective at private sector, chiefly used by major companies as an exceptional resort.

With the challenges on international landscape in the 20<sup>th</sup> and 21<sup>st</sup> centuries<sup>1</sup>, the use of intelligence in private sector has widespread in many industries and countries, driven perhaps by the rise of uncertainty in the environment, mixing of new and old threats -as cyberattacks, ransomware, social manipulation, misinformation, terrorism, organized crime, and war-, all enhanced by emerging technologies-, that challenge personnel, assets and operational concerns about security.

This mix of threats has been fostered by technology, that has worked in a dual role: while has let the companies advance to production models as industry 4.0, and let an increasing and specialized production on many areas (industry, agriculture and services); but also has exposed the productive production to cyberattacks, and but the technology on criminal hands as well, on an increasingly way that escapes ordinary capabilities at companies, and in some cases, governments.

The emergence of social media and digital platforms has also meant an additional source of risk for companies, including data thefts, brand and reputational damage, leaks of information, fraud and scams, high level executives' data exposure, misinformation and new challenges for digital management and cyber assets management, like access to high-speed internet or super computers.

On synthesis, the current emerging technologies, distinguished at the top by LLM and virtual realities, contain a mixture of options and choices not seen before by most of the board members or CEOs at companies, leading to a main stage known as *cognitive overload*, where intelligence areas can bring support to set a framework an a mind set to process the changing and challenging reality for companies security processes. By its side, governments in democratic countries keep as an ally to many companies, but are also facing their own challenges, like cryptocurrencies and their impact on local economies, besides the criminal use cryptos might have.

---






<sup>1</sup> The I and II World Wars; Cold War; falling of USSR; terrorist attacks; Arab spring; rise of radical populism; rise and develop of social media; major scale immigration; massive access to technology and online contents, and COVID19 pandemic, among the major ones.






The rise of virtual communities, integrated mostly by self-identities or ideologies, regardless of being physically at some specific country, the spread of misinformation and sentiment manipulation, together with cyber defense and digital irregular warfare, has its capabilities limited to fully orientate private sector to deal with emerging threats and risks.

## II. Private Sector Intelligence Challenges

Due to the generational and technological gap, the main task for intelligence in the private sector is to develop the capabilities at executive levels to fully understand (minimum 80%) the risks associated with technologies, as well as the opportunities to protect their personnel, assets and operations.

Over the last five years it has been possible to observe how technology is pushing and challenging private sector intelligence capabilities, by presenting an array of risks, threats and damage linked to technology in a different manner, that shows the need to bolster widely due to a diverse nature of cases, as presented on next chart:

Case	Year	Type of risk	Level	Est. Damage
<b>Colonial pipeline<sup>2</sup></b>	2021	Cyberattack: ransomware	Strategic, Tactical and Operational	
<b>United Healthcare<sup>3</sup></b>	2024	Physical attack: shooting using a 3D weapon	Strategic	
<b>Spotify: misuse in Sweden<sup>4</sup></b>	2023	Criminal finance: money laundering with crypto currency	Tactical-Strategic	
<b>Drones with IED at wind farm (Mexico)<sup>5</sup></b>	2024	Criminal attacks: use of drones to	Operational-tactical	
<b>Samsung engineers: source code leaking<sup>6</sup></b>	2023	Data leak: sensitive material exposed at chat GPT test	Tactical-Strategic	

 Very high   
  High   
  Medium   
  Low   
  Very low

Source: own creation with open information

<sup>2</sup> In May 2021, Colonial Pipeline was hit by a ransomware attack that forced the company to shut down operations for several days, leading to fuel shortages and panic buying. The hacker group was *DarkSide*. The impact was the shutdown fuel distribution, affecting 17 states and Washington, D.C. Ransom Paid: \$4.4 million in Bitcoin (later, U.S. authorities recovered a portion).

<sup>3</sup> On December 4, 2024, Brian Thompson, the CEO of UnitedHealthcare was shot and killed in New York (Manhattan). The authorities arrested a person with a 3D printed gun and a 3D suppressor.

<sup>4</sup> Swedish criminal gangs have reportedly (2023) exploited Spotify's streaming system to launder money by inflating play counts through artificial streaming practices, a method that mirrors broader fraudulent activities observed globally. These gangs purchase fake streams for tracks associated with gang-affiliated artists. Spotify, acknowledging the existence of such practices, has recognizes the challenge of combating artificial streaming.

<sup>5</sup> Drones were used by rival cartel cells to drop IED on a disputed ground by its crossroads, in the middle of a wind farm in the northeaster of Mexico.

<sup>6</sup> Samsung workers semiconductors branch leaked unwittingly source code of a test project, and internal meeting notes to create a presentation. After the incident the company banned the use of chat GPT and develop its own LLM.

The landscape for the next five years is unlikely to become easier for companies as they navigate complex, diverse, evolving, and often unpredictable security intelligence challenges. This increases the need to develop and standardize internal intelligence capabilities—or criteria for external vendors—and enhance liaison with governments under a specific agenda to address upcoming risks.

Another concern for the private sector is the need for recording and systematizing internal information for risk management, particularly at foreign locations and field deployment, where own data might be wasted in terms of generating a clear depiction of operational areas and concerning risk with technological origins, but mixed with social, security, economic and political fields.

The presented cases point at the need to change traditional organizations of looking at the risks and intelligence services, highlighting the opportunity to develop corporate security intelligence at the companies, focusing on risk prevention and crisis management, by recognizing the function and products of intelligence; use of inner information, undertake the develop and adoption at the executive level of a basic body of Knowlagent, as a point to leverage technology on a safe manner, to protect personnel and operations, and link with government agencies to deal with emerging threats or stages that will emerge, as part of a paradigm shift.

### III. Companies and governments: a shared strategy?

Although with a different nature, companies and governments share the same purpose to serve national interests, each one at their area of interest, and nowadays pressured by uncertainly and emerging technologies on a “race” among nations, highlighting Iran, China and Russia, that are driving their agendas mostly based on technological stage.

From the review of the risk cases to companies associated with technology, most of them involve human behaviors, pointing out that social field can be considered as a common point to develop a shared agenda among governments and private sector, linked to technology.

Tough military, economic and political fields also could be an engaging point, the purpose of private sector and government constraints, make the social and technological fields the most suitable to develop a shared agenda, considering the World Economic Forum (WEF) Risk Report 2025, as a starting point, highlighting:

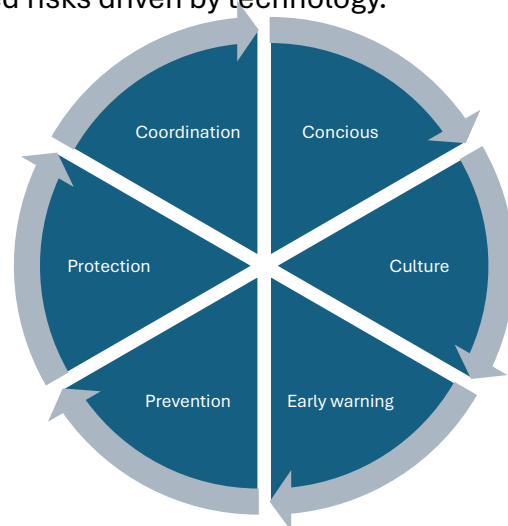
Social	Technological
- Inequality	- Misinformation and disinformation
- Societal polarization	- Cyberespionage and warfare
- Lack of economic opportunity or unemployment	- Adverse outcome of AI technologies.

It must be said in the era of information and high exposed technology, social risks are involuntary enhanced by the nature and design of certain platforms, as Tik-Tok, rising the need to develop measures to prevent catastrophes, and destabilization based on misinformation, disinformation or genuine confusions, like the *Fever number* in Philippines (1992), where a confusion on a prize contest, promoted by a beverages company, led to violent protests, many injured and at least 5 kills, plus losses estimated on 15 million dollars.

So, the blend among social and technological fields might drive into a major change of paradigm, that in the end represents a cognitive security issue, that represents a challenge to both: government and companies, rising the need for a common strategy.

The shared strategy should include a top executive level at companies' conscious about security intelligence and the enhanced risks driven by technology.

Once established the base, the next step should be the development of a corporate intelligence culture, considering producing early warnings to be shared with other industry partners, stakeholders and national authorities, to prevent incidents that might affect business dynamics or local governments agendas at the areas where the business has operations.



The early warning will bring guides to develop preventive actions inside the companies or businesses clusters, to protect personnel, operations and assets, and take specific protection measures in the interaction with local or global environment, and linking areas as security and marketing or sales, to algin -by coordination- all the efforts on the same direction to protect the whole business against emerging and automatized actions that could impact, willing or unwillingness to a whole community, as the *Cobalt 60* incident (1983).

With the author's experience and evidence over the last 11 years, it would be possible and necessary to develop a shared strategy among governments and private companies to use intelligence as a leverage to face and tackle technological risks and reduce the uncertainty gap about future challenges and actions needed to be taken.

## IV. Conclusions

In the last decades of the past Century, there were small and focused threats for private sector, belonging to the national reach of the companies, but by getting global, then the threats and risk also get global, but perhaps on an exponential scale.

With technological rise, the risks not only are higher, they are permanent and can be generated in any part of the world, with effects in places physically very distant, but in somehow engaged with companies, leading to a dilution of certainties and rise of uncertainty.

This might lead to a permanent thrill and emotional state, instead of rationality that used to be present due to the understanding of the operation environment for the companies and world geopolitics, making cognitive security a field to consider and develop with the assistance of two major tools: intelligence and technology.

Today challenges reflect a kind of paradox, due to even when we have more elements, information and Artificial Intelligence, but still the future is worrying us, and there is a lot of uncertainty, rising the need to know. Exercises like *Crystall ball*<sup>7</sup>, where newspaper financial information is given to the participants *in advance* for one day to take financial decisions, show that information gathering might be the least of the challenges, leading to analysis and intelligence production and dissemination of the major tasks.

For the future, the forthcoming 5 years will shape a new era, where risks as the ones reviewed previously, might be the least of the problems, due to a massive expansion of them, or an emerging combination of all of them, as it seems to be, enhanced by cognitive bias and overload, opening a new stage for security cognition.

Technology is, until now, a powerful tool to anticipate adverse trends for companies and governments, but it requires integrating a strategic approach, where intelligence is the way to deploy a new partnership.

---

<sup>7</sup> When a crystal ball is not enough to make you rich. <https://elmwealth.com/crystal-ball/>