The T-Factor – New Technologies and Intelligence Analysis Learning

José María Blanco
Guardia Civil, Spain[1]

Jéssica Cohen
Yaiza Rubio
Félix Brezo
Private Sector, Spain

Abstract
The world is continuously evolving in regards to the so-called VUCA environments (volatility, uncertainty, complexity, and ambiguity). If we adopt a PESTLE analytical model (which includes political, economic, social, technological, legal, and environmental factors), we can see that new technologies are the great "game changers". This concept, usually considered in foresight and future studies, can be defined as a new introduced element of factor that changes an existing situation or activity in a significant way. This technological factor (T-factor) is changing the way that we live, think, interact, communicate, or access services in an increasingly digital society.
Considering what Lowenthal (2013, 2015) has pointed out, intelligence tradecraft is in a permanent process of *"fatigue reform"*. This paper will identify how Information and Communication Technologies (ICT) are: first, affecting the so-called intelligence cycle; second, offering new opportunities to collect, evaluate and integrate old and new sources of information; third, generating new corporative and personal risks for intelligence analysts, especially in the cyberspace; fourth, introducing new bias; fifth, modifying classical skills usually developed in intelligence analysts; sixth, offering new tools to support the daily work of the analysts: big data, predictive systems, semantic analysis; and seventh, changing the way in which intelligence products are disseminated, with more visual contents: maps, infographics, and diagrams.

Keywords: Intelligence, analysis, technology, VUCA, learning

1 Corresponding author's email: blanco.josemaria@gmail.com

"Whatever the complexities of the puzzles we strive to solve and whatever the sophisticated techniques we may use to collect the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme"

(Kent, 1965, p. xviii).

1. Technologies affecting the so-called "Intelligence Cycle"

The accelerated process of innovation also affects criminal phenomena. It is not a coincidence that EUROPOL has chosen *"Crime in the Age of Technology"* as a subtitle for this year's SOCTA report (2017, p. 24), stating that *"for almost all types of organised crime, criminals are deploying and adapting technology with ever greater skill and to ever greater effect. This is now, perhaps, the greatest challenge facing law enforcement authorities around the world, including in the EU"***.** In its report *"Exploring tomorrow's organized crime"*, EUROPOL identifies eight key drivers for change. All of them are linked to information technologies and other related technologies: internet and deep web, social media, big data, cloud computing, mobile applications, Internet of Things, nanotechnology and smart cities.

Considering that technologies are a key factor in new criminal trends, Law Enforcement Agencies need to strengthen their efforts in order to improve their intelligence capabilities. Professionals from police forces and/or criminal intelligence departments need continuously new and specialized training to counter new threats and to take advantages of new opportunities. New technologies are at the same time both part of the current security problem and part of the solution as well. Since the 9/11 attacks (National Commission on Terrorist Attacks, 2004), there has been a continuous effort to improve the capabilities of intelligence analysts. The intelligence community has been always questioned after the attacks, due to the simple fact that it is too easy to carry out analysis from outside, always after the main event has happened and once all the information is available. This situation which originates intense media chatter.

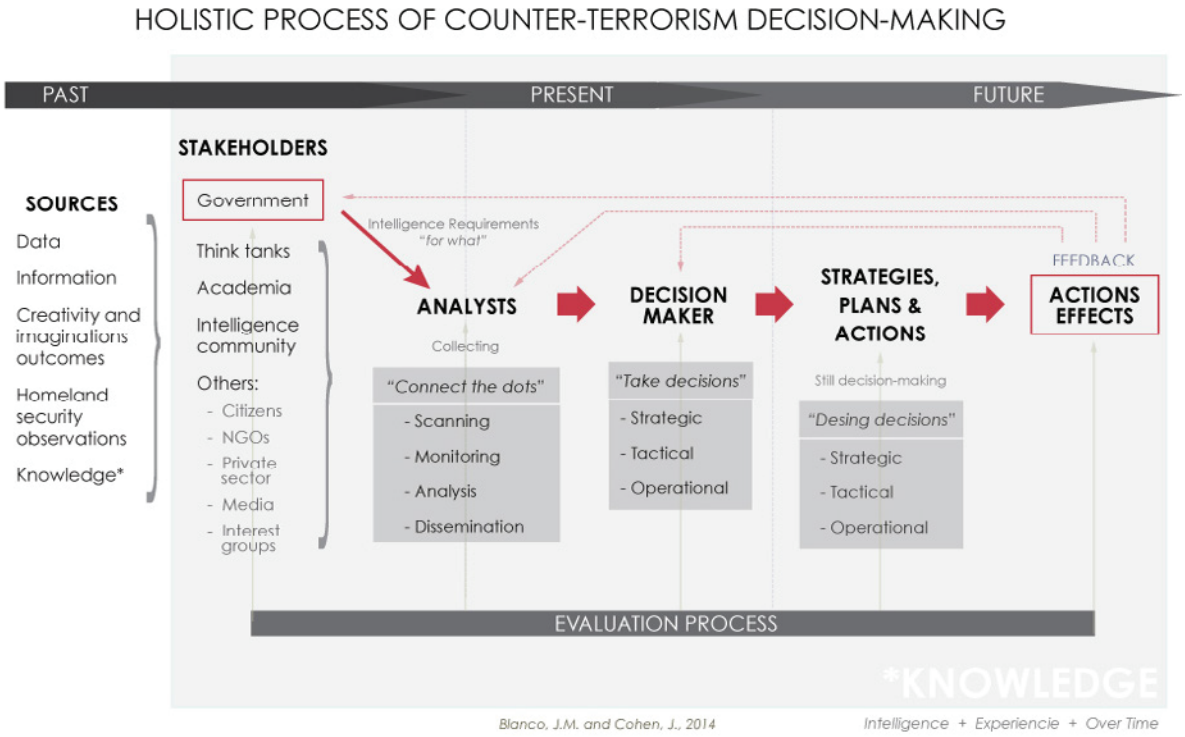
1.1 The end of the intelligence cycle

The intelligence cycle appears in many manuals, articles and training courses as the center of the whole intelligence discipline. It is pointed out that the cycle is an excessively theoretical construction that translates an unreal image of work into intelligence, leading to thinking that it is sequential, and cyclical. Several official models do not incorporate key tasks such as evaluation. As far as this chapter is concerned, and with the idea of "tools" in mind, it is evident that the current technological development is modifying the whole process in its classical conception:

- New technologies allow the incorporation of new tasks in the phase of collecting, including some tasks that had always been considered part of later steps. For example, open source management systems allow the extraction of entities and are able to immediately perform information integrations based on them. New technologies are capable, with an increasing degree of success, of synthesizing texts, as well as translating information into maps and other geolocation applications. We also work on approaches to automate the evaluation of information, for example, contrasting the same facts in different sources.
- The monitoring of information is becoming by itself a whole specialization. Systems can be feeding other basic and current intelligence systems on a continuous basis.
- Several technologies can support analysis tasks: ACH, decision support systems, statistical packages or integrated platforms (IBM i2).
- Technologies also modify the way in which information is presented, with a growing incorporation of visual and multimedia elements in intelligence reports, to the detriment of the text, which makes the work of analysts and decision makers easier and saves time.
- Technologies can also be useful in the training of intelligence analysts, improving their skills: serious gaming, simulations, or case studies.

Because of these reasons, we propose a broader concept such as the process of intelligence, which can be defined as the *"set of activities developed in an organization, by analysts, and aimed at obtaining information and analysis to support decision making in time, place and form"* (Blanco & Cohen, 2014, 2016).

Figure 1. Intelligence Process. Source: Blanco and Cohen (2014 & 2016)



1.2 The need to avoid "technological solutionism"

Our current society is characterised by the intensive use of technologies, especially in the field of ICT. Their contribution has been fundamental in providing new services and features to citizens, who can interact at any time and place. But they can also generate new risks and threats. New technologies are the great "game changer" of our time.

Among the critical views, or at least those that try to warn of the negative effects of the technologies, we can highlight the works of Eugeny Morozov. In 2013, Morozov criticized what has been called "technological solutionism", i.e., the vision of technology as an objective instead of a means to get different objectives. For Morozov, every problem has a technological solution. There are even technological solutions aimed to face problems that do not exist. In the field of intelligence analysis, it is possible to find technological warnings, such as those pointed out by Lowenthal in reference to Big Data (2013). Perhaps the most coherent position would be to rely on the benefits of the technologies, but maintaining a "situational awareness" towards them. New technologies are the source of new threats and risks, but, at the same time, they are part of the solution.

The possible debate on technologies and intelligence analysis raises two possible scenarios: technological automation of the analysis versus technological support to the analysis (or enhancers of the analysis through technology). Intelligence analysis is a human-driven process, and can be technology-enabled at the same time.

In the field of innovation in Europe, some projects have been financed by the European Commission, such as RECOBIA, which have shed a light on the difficulties faced by organizations in the identification of tools that meet analytical needs. Proprietary applications are expensive and require time for development. Commercial developments present additional risks, including: high prices due to the short life cycle of technological innovation, risks in information and data security, or technological proposals that cannot yet be considered mature. This situation leads to a situation of technological paralysis.

Intelligence analysis tools, in the opinion of the analyst community, are not being effective in separating *"the signal from noise"* (Silver, 2015) or in reducing uncertainty. There is a clear gap between what is offered technologically and the analysts' expectations.

Badalamante and Greitzer (2005, p. 5) pointed out that *"the complexity, uncertainty and ambiguity in which the analyst moves to reach judgments about future events and actions will remain for a while despite the improvement of the capabilities of the software tools"*.

There is, however, a high degree of consensus on the technological support for intelligence analysis, as a way to:

- Manage complexity;
- Limit cognitive biases: warning about them and their impacts;
- Manage volume, volatility and variety of information, especially in its unstructured character (text format, imagine, video, etc.);
- Overcome the human limitation to process and interpret large amounts of data and information;
- Support analytical tasks;
- Improve the presentation of intelligence products, especially through the support of visualization tools;
- Training and developing new skills, through simulations and serious gaming.

It is possible to differentiate between two large groups of technological challenges in intelligence analysis, external (environment and specific current characteristics of information) and internal (organizations and analysts).

Table 1. Technological challenges in intelligence analysis

External	Environment VUCA	Identification of trends	Prospective challenge
		Wild Cards	
	Information	Infoxication	Quantitative challenge
		Reliability of sources and credibility of information	Qualitative challenge
Internal	Organization	Leadership Change management Digital transformation	Organizational challenge
	Analysts	Cognitive biases Impacts of technology on cognitive skills Obsolescence of knowledge and skills Cybersecurity concerns	Cognitive challenge

External challenges

In a VUCA environment, there are two main challenges for analysts. On one hand, they must detect technological trends that affect either the subject matter of the analysis or their own function as an analyst, under a dual perspective in both cases: new threats and new opportunities. On the other hand, it is advisable to develop a prospective exercise that allows to anticipate technological "wild cards" (Petersen, 1997), facts of low probability and high impact, in order to adapt the present strategies.

It is understood by infoxication, infobesity or information overload the situation produced because of having too much information to follow a topic or support the decision making. The incessant generation of content, a low relation between signal (valid information) and noise (disposable information), and the ignorance of the average citizen on how to handle information contribute to this effect, which in its English terminology ("information overload") was coined in 1970 by Alvin Toffler in "The Shock of the Future", although it was previously mentioned by Bertram Gross (1964, *The Managing of Organizations)*.

The current world, in which the concept of post-truth has recently been coined, shows us how the invocations of emotions are above the facts themselves. Lies, propaganda, misinformation, and deception often find support in new technologies, both as facilitator and enhancer (Viner, 2016). The great challenge a decade ago was managing the amount of information. Now, we face another difficult challenge: the evaluation of all this volume of information when, increasingly, part of it is false or has been manipulated.

Internal challenges

Internally, the new environment affects both the intelligence organizations (thinking both of the public and private sectors) and the analysts themselves. Organiza-

tions, as part of today's society, must develop a continuous monitoring of the desires and expectations of the people that they serve. Again, the technological component is a key factor, leading to the development of ambitious digital transformation strategies and plans. Organizations must promote and manage change. Surely, success will be in the hands of those organizations that change the rules of the game, and not in those who only know how to adapt. The digital transformation requires an external dimension (towards the client) but also an internal one, taking the digital gap among its workers as one of the biggest challenges to face.

Biases are unconscious mental errors resulting from the instinctive propensity to simplify decision-making, leading to shortcuts or deviations in judgment. They are usually based on memory, experience, education, cultural baggage or ideologies. Biases are a consequence of the quantitative and qualitative challenges presented by the information. Kahneman (2012) has detailed that there are basically two types of thinking, one fast and intuitive, and other slow and logical. The first is useful to tackle known and familiar environments, being a thought that is always activated and does not generate fatigue. The problem is to respond in the fast mode to complex problems. For that purpose we need to activate slow thinking, which is exhausting, demanding high cognitive resources and cannot be kept active continuously. Admitting the existence of biases should lead analysts to be cautious.

Some of the bias inducted by technologies are originated by the way in which search engines are used. Eli Pariser (2012) has pointed out the "filter bubble". Algorithms guess what information a user would like to see based on previous information about them, such as their location or their search history. Users become isolated from information that disagrees with their viewpoints, keeping them in a bubble. Technologies could strengthen other classical biases: proximity of information, confirmation (Cook and Smallman, 2008), completion, anchoring or heuristics.

In the same way, technologies may already be affecting some of the analysts' cognitive abilities. Some effects have been pointed out in recent times. As an example, because they are well known, we will highlight:

- "Google effect": We use Google and the Internet in general as a supplementary memory. We reduce the personal demands of memorization, trusting that we can easily recover information on the Net.
- "The Shallows" effect: Nicholas George Carr (2010) develops an argument: The Internet can have detrimental effects on thinking that damage the capacity for concentration and contemplation, which causes a deficit in the memory's storage capacity and in the processing of the information. Reading long articles and books has become an arduous task. Precisely, multitasking, a sign of our times, is a possible cause.
- "Focus effect": Goleman (2013) highlights the difficulties in focusing on a single task, a situation in which the great human technification and its dependence on a multitude of informational inputs greatly influence our cognitive capabilities. The solution he proposes is meditation, in order not to damage this human and necessary capacity. For Goleman, multitasking does not exist, it is not a human capacity.
- "Addiction effect": Dopamine is asking us to receive continuously new informational inputs. This limits our capabilities to analyze and to go deeper inside them.

These observations, controversial in part, but very popular nevertheless, require to look for points of consensus. Technologies do affect the brain, but it may perhaps be noted that there is no loss of mental abilities, but rather an adaptation that, in addition, only occurs in the long term. The plasticity of the brain causes an adaptive process.

This situation presents specific challenges in the intelligence process:

Table 2. Technological challenges in the intelligence process. Blanco and Cohen

TASKS	CHALLENGE
Planning and direction	Technological surveillance Technological requirements Identify end-user requirements Option: own development or commercial product Cost-benefit analysis Security concerns
Collecting, monitoring and processing	Collecting tools. Crawls. Entity extraction. New demand in intelligence services: Tools for verification Training using OSINT tools Security concerns
Analysis	Previous agreement: human-driven analysis and technology-enabled analysis Training using analytical tools. Complex, because implies knowledge in different domains (data mining, statistics…) Develop computer support for structured and advanced techniques of analysis (for example ACH with Bayesian support)
Dissemination	Developing of visualization tools, integrated with analytical capabilities Complexity needs training (for example Tableau)

2. The T-Factor - New skills for intelligence analysis

In the 1990s, the US Army outlined what would be a new military training program. Its parameters were defined with a clear objective: to develop the capacity of its members to act under highly complex contexts. This was a new need that emerged after identifying the main characteristics that would determine future scenarios, coined as VUCA environments (acronym for volatility, uncertainty, complexity and ambiguity, see figure I). As a result of this initiative, in 2004 the first results of a new program known as Thinking Training Method and Think like a Commander (TLAC) were published. The final conclusions were defined in the first lines of the document: "*Success in future operations will depend on the ability of leaders and soldiers to think creatively, decide quickly, take advantage of available technology, adapt easily and act as a team*".

This scenario is not an option but a reality, and is a challenge for analysts, with the added complexity of not being trained for it, as if it were the TLAC program.

Table 3. VUCA elements

COMPLEXITY Each event is conditioned by a multiplicity of causes and factors, each of which is interrelated with third events. This situation generates a high level of confusion that prevents us from having a clear vision of the situations that we face.	**VOLATILITY** Changes are rapid, almost unpredictable, making it difficult to identify trends or patterns and reducing the stability of processes. The type, the magnitude, the volume and the speed with which they occur make analysis tasks difficult.
AMBIGUITY The answer to the key questions (who, where, why, when...) is difficult to establish. Errors of interpretation and the plurality of meanings is a cause and effect of confusion, resulting in an increase in imprecision.	**UNCERTAINTY** Many of the changes that take place are disruptive, evidencing that the past does not have to be an indicator of the future, and hindering our preparation in the face of future scenarios.

If we do not have this VUCA environment in mind, it is impossible for the next generations of analysts to be well trained. In the same way we will fail in the recruitment processes. It is very complex to properly select a profile of analysts when there is blindness to the tasks that they are supposed to do.

Therefore, it is necessary to consider, not only the limitations of the present, something that is already conditioning us, but also what the future will be like: understanding what challenges and opportunities it will offer us and what skills we have to train in order not to be overwhelmed by its complexity.

Precisely to respond to these limitations, a second acronym of VUCA emerged, as an antonym, trying to focus on the perspective from which these environments must be understood, "VUCA Prime": vision, understanding, clarity and agility (Figure 2). It is configured as a set of inexorable skills needed in the present and future times of our societies (Blanco & Cohen, 2017).

Table 4. VUCA Prime Responses

CLARITY over COMPLEXITY Even chaos can make sense. Generate knowledge maps. Make a dynamic tracking of the existing analyses to detect new evidences (monitoring). Understand each phenomenon from within and from the global perspective simultaneously. Do not use simplistic, mono-causal or mere chance explanations, trying to answer all possible questions. One of the great challenges is knowing and knowing how to use constantly changing information from disparate sources.	**VISION over VOLATILITY** Think in future as a habit. Imagine scenarios and analyze them in a back-casting process to detect indicators, in order to avoid future risks and threats. The objective and methodology applied must be clearly defined. We must be able to rapidly integrate large amounts of information without the process or tools used, resulting in less precision and speed.
AGILITY over AMBIGUITY Maximize the ability to learn, make mistakes, communicate, respond and adapt. It requires rapid problem solving and constant decision-making. It must be proactive and be focused on the problem to anticipate the effects even before adopting the answer. The technologies used as support have to be agile and adaptable to users and needs, leaving behind generalist solutions.	**UNDERSTANDING over UNCERTAINTY** The phenomenon that we face must be fully understood. The answer should go beyond our own previous experience and knowledge. It needs to build knowledge networks, with trust and credibility, and use new technologies to strengthen the whole process and progressively improve reasoning skills.

Taking into consideration these previous definitions about the way in which the future has materialized, from our daily experience as analysts, but also as managers of analysis units and professionals of new technologies, we point out the need to use new principles for training new analysts: the use of serious gaming, the focus on skills and not only on knowledge, the shift of the teaching approach in favor of the learning approach (empowering students) and the need to consider any organization as a center of continuous learning, without leaving this work (responsibility) only in the educational sector.

2.1. Game as a transversal skill

When we refer to the game, we allude both to the need for its existence in the training processes (serious gaming), and to its value in terms of attitude, which we will call gaming-mind.

The training in which the game is allowed goes beyond the theoretical content, making it easier for the analysts to put into practice, both individually and as a group, the skills that are required before a given question or problem, without being exposed to the risk that would involve doing so in a real situation. It is a "learning based on experience" process that makes it easier to immediately obtain feedback and that also trains the agility of response and allows the analyst to be exposed to rapidly changing dilemmas. These demands are highly related to the growing demand for discovery, collection, evaluation, integration and synthesis of data from the use of new technologies.

Under this type of activities, the didactic level is maximized, because not only the theoretical content is contemplated, but also its development and use, having to deal in a simulated way with the problems that the reality would generate.

However, this problem is evident from an early age, where the anachronistic teaching methodology of the current educational centers detracts from this component, perhaps because it is perceived as a waste of time, perhaps due to not knowing how to visualize it outside the children's environment.

While it is true that agencies like the CIA have been using games for years as a training tool for their agents, the use of these techniques is not widespread. This is even more palpable in general formations of profiles that, a priori, have not decided to focus their professional career within the intelligence analysis, as is the case of the police bodies, whose position is finally defined by many other rather organizational criteria (conditioned by vacancies, promotions, countries of work, categories, etc.).

However, this not only facilitates the highlighted processes, but can work as: a source of ideas; an improvisation generator; and a creativity enhancer. It can also facilitate the search for alternatives; the decision making; as well as contribute to an improvement of the social skills and a greater training in the control of biases. All of them are relevant areas for every intelligence analyst.

Highlighting among these benefits human ingenuity, experience and creativity, is a relevant factor in intelligence analysis, but also in our need to work with machines and to be different from them. If the empowerment of people that is today allowed by the use of new technologies is answered with greater creativity, not only at the individual, but at the organizational lev-

el, it will be easier to make smarter decisions, to solve more complex problems.

2.2. Abilities and skills, not only knowledge

In 1970, Alvin Toffler described the symptoms of the "shock of the future". The speed at which the change occurs comes to generate greater implications than the direction in which it materializes. Events happen so quickly that we have to be able to talk about the past and the future simultaneously. Managing complexity, Toffler pointed out, would be the major problem for societies in the future. A context that, by pure definition, is being harmful to those people and organizations that are rigid and have difficulties adapting to vertiginous change. This context is having a great impact on an essential element: knowledge.

The creation, transmission and assimilation of knowledge advances and is modified in the same way as society, science, technology as or communications. In this sense, Toffler himself stated (p. 414) that *"the illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn"*. He was using words from the psychologist Herbert Gerjuoy of the Human Resources Research Organization[2]: *"the new education must teach the individual how to classify and reclassify information, how to evaluate its veracity, how to change categories when necessary, how to move from the concrete to the abstract and back, how to look at problems from a new direction—how to teach himself. Tomorrow's illiterate will not be the man who can't read; he will be the man who has not learned how to learn"*. Toffler added that training persons would not be based on immovable knowledge that you have in your mind, but in function of the abilities needed at every moment

Years later, in the conference "*New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*" (Rome, Italy, 31 March - 2 April 2004), it was showed that, after the fall of the Iron Curtain, the intelligence requirements changed completely. It was not a sudden transformation, but it was a challenge in terms of the training of the analysts, who were forced to pay attention to other environments hitherto neglected, such as larger, global scenarios that require both short and long term for their understanding, with multiple new cultural connotations and linguistic differences.

Imagining, listening, experimenting, making mistakes, creating and destroying creatively, using intuition, are key skills to live in the future. Knowledge will become a set of skills, not of immovable knowledge and its use, in line with the opportunities provided by new technologies, will be a key factor of success. The objective will be to create differential value through a specific skill at a given moment. As Toffler said, by teaching students how to learn, unlearn and relearn, new dimensions can be incorporated into education.

2.3. Learning, not teaching

The aim of education is learning, not teaching. The book *"Turning Learning Right Side Up: Putting Education Back on Track"* (Ackoff and Greenberg, 2008) focuses precisely on trying to answer why we keep trying to teach people to be machines and not to enhance their abilities as humans, as highlighted in the previous section.

Memory is confused with learning and that conditions us so that we will hardly remember in our adult life what was taught to us. However, what was learned (talking, walking, how to dress) will remain, in general, in our imprint in a perennial way.

It is about generating the same dynamics that generate learning before a new job. In this process, the teaching, if any, is minimal. However, learning arises from the observation, imitation, the need, the explanation of reference examples, but not the talk.

Learning escapes the standardized and standardized formats of what an adult is supposed to be in society. You learn by trying, failing, sharing, interacting informally to get answers and sharing what you have internalized.

Learning through explanation is another pillar of this vision. The "explainer" is required an extra effort that the teacher is not required, the need to put themselves in the mind of the other to be able to answer their question. A practice that involves developing "environmental culture": not only taught based on what is known, but it is explained based on the difficulties that a third party poses. You learn to "learn from others". In this context there is a need to use experienced analysts as mentors for those more novices, thus sharing experience, training and skills.

2 The book's notes state that Gerjuoy's comments are from an interview with Toffler.

2.4. Learning organizations

Following the previous scenario and taking into account that new technologies allow us a greater daily diffusion between the biological, the physical and the digital, it is also possible to talk about the learning needs within organizations.

Peter Senge's vision of a learning organization as a group of people who are continually enhancing their capabilities to create what they want to create could have a clear use in intelligence analysis teams. According to Peter Senge (1990, p. 3) learning organisations are: *"…organisations where people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective aspiration is set free, and where people are continually learning to see the whole together" (The Fifth Discipline)*. For this to happen, it is argued, organizations need to *"discover how to tap people's commitment and capacity to learn at all levels"* (*ibid.*: 4).

Senge points out different ways of learning. *"Survival learning"* or *"adaptive learning"* is important and necessary, but it is not enough, and organizations need to develop a *"generative learning"* that enhances the organizational capacities. This is why an intelligence department must be continuously looking for the way it can improve knowledge and especially develop new skills.

This concept has several links with the new skills needed to survive in VUCA environments. For this purpose, organizations should cultivate five disciplines:

1. Systems thinking: ability to comprehend and address the whole, and to examine the interrelationship between the parts.
2. Personal mastery: organizations learn only through individuals who learn.
3. Mental model: learning to unearth our internal pictures of the world, to bring them to the surface and hold them rigorously to scrutiny.
4. Building shared vision: unearthing shared "pictures of the future" that foster genuine commitment and enrolment rather than compliance.
5. Team learning: aligning and developing the capacities of a team to create the results its members truly desire.

All of these 5 disciplines are key elements in intelligence analysis, in which there is a need of holistic approaches to have the "big picture" about security phenomena, and a strong critical thinking philosophy to challenge previous or intuitive judgements. Individual and team learning must be balanced, taking into consideration that intelligence analysis is a team work.

This learning must be guided by the shared vision about their mission, and the aim of improving the intelligence process and the intelligence final product, in order to facilitate decision taking. This must be favoured not only by governments or institutions, but also by teachers, human resources, managers and analysts themselves.

Table 5. How to survive - abilities needed in a VUCA world

CLARITY over COMPLEXITY	VISION over VOLATILITY
Adaptive thinking Lateral thinking Knowledge Management **Information overload management** Diversity management Intellectual curiosity Star-busting creativity techniques Cognitive biases management **Data analysis** Operating with estimates (Lowhental[3]) General / holistic approaches as well as **t**echnical vision **Information media literacy** Observation Explainers (Ackoff & Greenberg)	Learn to learn Knowing how to unlearn Continuous training Anti-fragility (N. Taleb, 2013) Creativity Agility Motivation humility Cognitive adaptability Collaborative intelligence Knowledge management based on the team Diagnosing collaboration barriers **Self-taught use of new technologies** **Gaming-mine** Evaluative vision **Social media relations ability**
AGILITY over AMBIGUITY	**UNDERSTANDING over UNCERTAINTY**
Critical thinking Experimentation Learned lessons Learn to doubt Dismisses the superfluous Self-driven learning Social pressure management Proactivity **Decision-making engineering** Team-based decision making quality Adaptation of the methodologies to the study objective Finding solutions Intelligence analysis process development Crisis management Time and priorities management **Serious gaming techniques** Talent management Critical writing Resolution / decision-making	Transparency Confidence Managing overconfidence (honestly introspective) Collaboration / teamwork **Technological awareness** Creating scenarios / simulations Idea Generation **Validation of acquired knowledge** Inter-personal skills Intelligence of the crowds **Leadership In virtual and transcultural teams** **Information visualization techniques** High performance team development **Management of virtual teams**

The future, no matter how disruptive or distant it may seem, is not immune to our control. As organizations, analysts and citizens, we all have the ability, if not the responsibility, to intercede in their evolution with our decisions. Having the necessary skills to make these as accurate as possible is only the beginning, having become a condition *sine qua non* to our future.

3. OPSEC and privacy in online investigations

Operational security (OPSEC) is a process designed to protect intelligence analysts from being identified by third parties. Its implementation results in the development of countermeasures, which do not have to be necessarily technical, in order to prevent possible leaks. We are now going to discuss some examples of this.

3.1. Identity management in the network

When carrying out research activities on the network, the analyst will need to authenticate in certain services in order to obtain additional information. In this process, the management of numerous identities can be an obstacle if it is not properly planned from the very moment of the creation of those profiles.

The reuse of real profiles implies the risk of exposing the analyst's identity through their usernames, emails, photographs, comments, affiliations or even IP addresses. The large number of leaks of information made public over these years, which have involved top-tier companies such as LinkedIn, Adobe, Dropbox or Yahoo are just a reflection that the exposure of sensitive information of users is not only possible in low-profile websites. Websites like HaveIBeenPwned.com[4], maintained by Australian security specialist Troy Hunt, or Hacked-Emails.com[5],by José M. Chia, are some examples of this.

A protection tool for analysts is the use of password managers like KeePass[6]. These managers are applications in which the user can store different passwords for each profile that will be used, generating them randomly and storing them in a database encrypted with military standards such as AES256. As a consequence, the analyst will prevent the leaking of information in one of the resources they use from exposing sensitive data from other platforms, as the passwords for every platform are different from each other. Obviously, the user will have to take care of the security of this database, using a very robust password to prevent that, in case of loss or theft, a third party has access to their data.

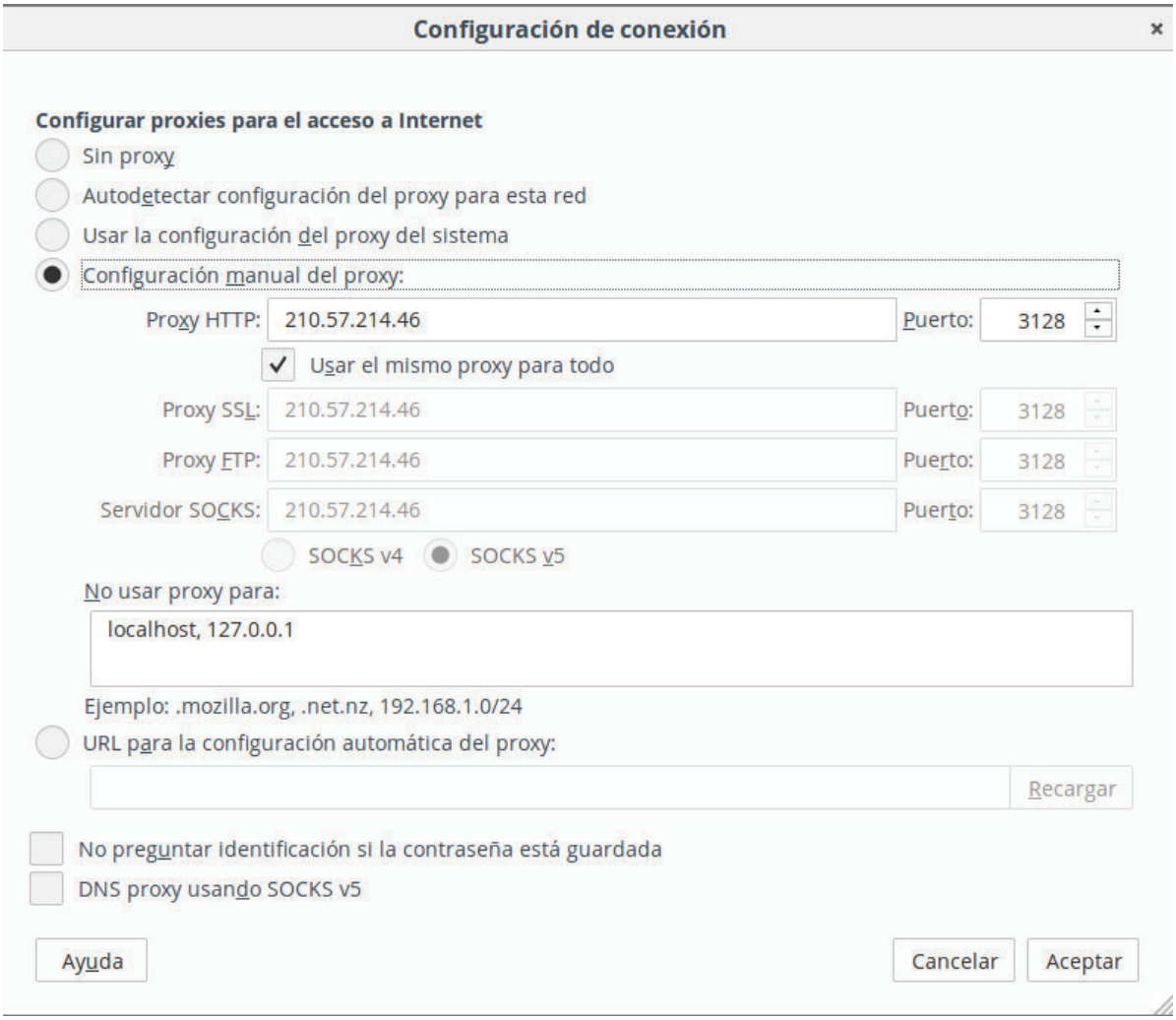
3 http://www.tandfonline.com/doi/full/10.1080/02684527.2017.1328856

4 https://haveibeenpwned.com

5 https://hacked-emails.com

6 https://keepass.info

Figure 2. Configuration window for HTTP, HTTPS, FTP and SOCKS proxies in the Firefox browser.



Creating profiles on the best-known social networking platforms can be difficult if the analyst's aim is to act as anonymously as possible. The analyst has to be aware that platforms like Twitter will offer recommendations based on the account's location, its activity, the people it follows, the accounts with which it interacts, the *tweets* in which it participates or the email address used in the registration process, thus establishing links with real contacts of the original profile. Mail providers such as Gmail or Outlook request numerous personal information and establish a series of mechanisms that are difficult to dodge from the moment they begin to suspect that too many accounts are being created from the same location. Therefore, many end up opting for email providers such as ProtonMail[7] (or mail2tor.org, cock.li, airmail.cc, mailcatch.com or guerrillamail.com) that will offer email accounts without performing too many checks.

7 https://protonmail.com

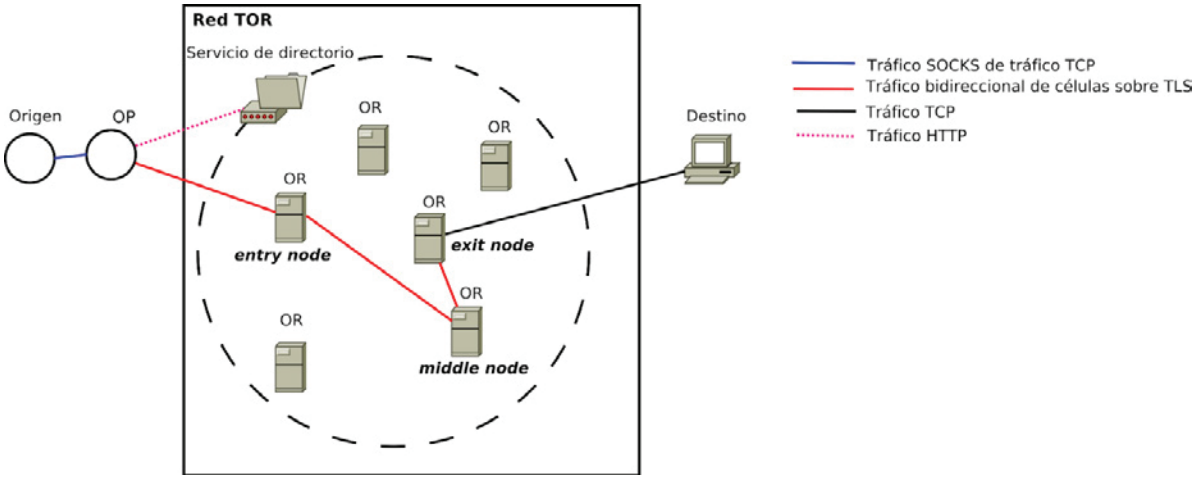
3.2. Masking the identity of the analyst

One of the problems that analysts have to face when conducting an investigation is the masking of the connections' origin. Normally, the IP addresses from which we connect are visible to the services we visit, since the point from which the requests are made can be registered.

The use of proxies

A proxy server is an element that acts as an intermediary between two systems, so that both ends of the connection do not interact except through this intermediate agent. In this regard, each system only has visibility of this intermediate agent, which in practice has the effect of masking the origin. There are a lot of lists of public proxies located in different places like free-proxy-list.net or freeproxylists.net.

Figure 3. Operation diagram of the Tor network. Source: Fercufer (Wikimedia)



The configuration of these proxies in the browser is quite simple. Just take note of the country from which you want to exit and adjust the parameters of the proxy settings. For this case, we have chosen a proxy from Indonesia, whose IP address is listed as 210.57.214.46 through port 3 128.

The main problem presented by these lists, regardless of their availability and latency, is that the user has no real way of knowing what these intermediaries do with their data.

VPN

While *proxy* servers only act as intermediaries between two points, a VPN is a more complex technology that allows extending the extension of a domestic or corporate local network beyond its physical location. Although they can also be used as a gateway to avoid revealing the real IP address, their functionalities go far beyond those of a mere intermediary, since they allow, for example, that employees working outside an office have access to shared resources. The connection between the user and the physical network itself is tunneled so that the traffic circulates in an encrypted and safe way.

The Tor network

The Tor project[8] was conceived with the aim of offering users an additional layer of privacy in the use of the internet. Thus, the use of the Tor network for conventional navigation protects the origin of the real user's request by exposing only the output node requesting a particular resource. Tor is a free *software* designed to help activists, journalists and Internet users to evade mass surveillance by routing encrypted traffic through a series of nodes that make up this network.

The user, instead of connecting directly to his destination, chooses a node of the Tor network as an entry node after connecting to a directory of available nodes. The exit node is the one that will connect to your destination and your IP address will be the only one that the destination will have a record of.

Navigation through Tor is not an absolute guarantee for 100% anonymous navigation. Unfortunately, a recently discovered bug related the way publish local links are published could expose the user's real IP address of the user on Mac and GNU / Linux systems. The bug has been quickly corrected not only in Tor Browser Bundle but also has been moved to the project on which it is based, the Firefox browser itself.

Footbridges towards the Tor network

To facilitate access to the hidden services without having to configure any software, there are known as Tor gateways that act as an intermediary between the user who tries to access a resource.onion and the resource itself, collecting the result and serving it again. There are multiple platforms on the internet that offer these services, mainly based on the Tor2Web project. Examples of this type of platforms are onion.city, onio.cab, onion.plus and onion.link among others.

However, the use of gateways implies that the user renounces to a significant part of their anonymity by granting the intermediary information that was not available to the final server. For the user, these practices carry the risk that, not only the requests made may be registered by a third party together with their real IP address, but also that the responses received have been adulterated by the intermediary.

8 https://torproject.org

Other alternative networks

Apart from the Tor network, there are other types of networks that can be mentioned, such as I2P (Invisible Internet Project)[9]. This project focuses on offering a layer of abstraction of communications within the network in order to offer anonymous web pages, chat clients or file transfer platforms. The main difference with the Tor network is that I2P has been conceived to be used as a gateway to the conventional network. Lately, the IPFS system has also been gaining importance[10], Inter Planetary File System. It is a distributed protocol in which the different nodes of the network share disk space and replicate the content for all the nodes of the P2P network. The project is used in combination with blockchain technology to store content on a continuous basis.

3.3. Operating systems

There are some operating systems whose main objective is to preserve the user's safety. Although each of them puts the focus on a different aspect of security, they all assume that the user will be exposed to vulnerabilities and failures that can compromise both their identity and the integrity of their system. Some of these operating systems are:

- Tails[11] (acronym for The Amnesic Incognito Live System). This is a distribution designed to protect privacy and anonymity by requiring that all connections of this Debian system be made from the Tor network through the use of Birdy[12] (a plugin to use Tor with Thunderbird), with Pidgin or KeePassX for managing passwords. Unlike conventional operating systems, it has been specifically designed to be executed from a Live CD or USB so that it leaves as little fingerprint as possible in local storage;
- Whonix[13] is distributed in a virtualized environment with two virtual machines. One of them has the sole mission of acting as a gateway to the Internet, routing all the traffic generated by the other, which acts as a work station, towards the Tor network;
- Qubes OS[14],an operating system that has been designed with security in mind and that implements the concept of security by isolation and is defined as a "reasonably secure operating system". If an application is compromised, it cannot affect other applications outside the domain in which it is present. Different security levels are applied, for example, to execute banking transactions or consult mail.

Conclusions

This paper has identified how technologies are affecting the so-called intelligence cycle. New technologies offer new opportunities to collect, evaluate and integrate old and new sources of information, to analyse data and information third, and to disseminate the final product in a seductive way.

But, on the other hand, new technologies are generating new corporative and personal risks for intelligence analysts, especially in the cyberspace, and introducing new bias. Clearly, it is possible to point out a set of technological challenges in intelligence analysis. Some of them are external factors: the technological landscape in continuous evolution and the characteristics of information (infoxication and increasing difficulties to evaluate sources and pieces of information). Other factors suppose internal challenges, both for organizations and analysts: digital transformation, new leadership, new cognitive bias, obsolescence of knowledge and skills, or new security concerns.

This paper proposes a roadmap to improve the learning of intelligence analysis, with three main pillars: first, focus on learning instead of teaching; second, focus on organizational learning; and third, focus on learning by gaming and doing. Agreeing that technologies are a key factor in new criminal trends, Law Enforcement Agencies need to strengthen their efforts in order to improve their intelligence capabilities. For this purpose, an adaptive VUCA framework can show us the main challenges we face to analyze and interpret this world, and especially its criminal phenomena, letting us to identify new knowledge and new skills needed to tackle old and new threats and risks.

Finally, intelligence analysts face new concerns, because of their possible high digital exposition. Operational security (OPSEC) is a process designed to protect them from being identified. In this process of continuous evolving technologies, cloud computing, artificial intelligence, OPSEC is a relevant content training for new and old intelligence analysts.

9 http://geti2p.com/

10 https://ipfs.io

11 https://tails.boum.org/

12 https://addons.mozilla.org/en/thunderbird/addon/torbirdy/

13 https://www.whonix.org/

14 https://www.qubes-os.org/

REFERENCES

- Ackoff, R. & Greenberg, D. (2008) Turning Learning Right Side Up: Putting Education Back on Track. FT Press.
- Badalamante, R. V. & Greitzer, F. L. (2005) Top Ten Needs for Intelligence Analysis Tool Development. Proceedings of the First Annual Conference on Intelligence Analysis Methods and Tools. Richland. Pacific Northwest National Laboratory, 2005.
  Available from: https://www.pnnl.gov/coginformatics/media/pdf/topten_paper.pdf [Accessed 10th September 2017]
- Blanco, J. M. & Cohen, J. (2014) The future of counter-terrorism in Europe. The need to be lost in the correct direction, *European Journal of Future Research*. Vol. 2, No. 1.
  Available from: from: https://link.springer.com/article/10.1007%2Fs40309-014-0050-9 [Accessed 10th September 2017]
- Blanco, J.M. & Cohen, J. (2016) Knowledge, the great challenge to deal with terrorism. Revista de Estudios en Seguridad Internacional, RESI.
  Available from: http://www.seguridadinternacional.es/revista/?q=content/knowledge-great-challenge-deal-terrorism [Accessed 10th September 2017]
- Carr, N. (2010) The Shallows: What the Internet Is Doing to Our Brains. W. W. Norton & Company.
- Cook, M.B. & Smallman, H.S. (2008) Human factors of the confirmation bias in intelligence analysis: decision support from graphical evidence landscapes. *Human Factors* 2008 Oct, 50(5): 745-54.
- EUROPOL (2017) SOCTA: Crime in the Age of Technology.
  Available from: https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017 [Accessed 10th September 2017]
- Global Futures Partnership of the Sherman Kent School for Intelligence Analysis (2004) New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities. Conference Rome, Italy, 31 March - 2 April 2004).
- Goleman, D. (2013) Focus: The Hidden Driver of Excellence. Harper Collins US Brand Code.
- Gross, B. (1964) The Managing of Organizations: The Administrative Struggle. The Free Press of Glencoe.
- Kent, S. (1965) Strategic Intelligence for American World Policy. Hamden, Conn., Archon Books.
- Khaneman, D. (2012) Thinking Fast and Slow. New York: Farrar, Straus and Giroux.
- Lowenthal, M. M. (2013) A Disputation on Intelligence Reform and Analysis: My 18 Theses. *International Journal of Intelligence and Counterintelligence,* Vol. 26, pp. 31-37.
- Lowenthal, M.M. & Marks, R.A. (2015) Intelligence Analysis: Is It As Good As It Gets?, International Journal of Intelligence and CounterIntelligence, 28:4, 662-665.
- Morozov, E. (2013) To Save Everything, Click Here: The Folly of Technological Solutionism. Public Affairs.
- National Commission on Terrorist Attacks (2004) The 9/11 Commission Report. New York: Norton.
- Pariser, E. (2012) The Filter Bubble: What The Internet Is Hiding From You. Penguin.
- Petersen, J. (1997) Out of the Blue How to Anticipate Big Future Surprises. The Arlington Institute, 2nd ed. Lanham: Madison Books.
- RECOBIA. REduction of COgnitive BIAses in Intelligence Analysis. FP7-SEC-2011-1.
  Available from: http://cordis.europa.eu/project/rcn/102068_en.html and https://www.recobia.eu/ [Accessed 10th September 2017]
- Senge, P. (1990) The Fifth Discipline: The Art and Practice of the Learning Organization. Currency.
- Silver, N. (2015) The Signal and the Noise: Why So Many Predictions Fail--but Some Don't. Penguin Books.
- Toffler, A. (1970) Future Shock. Random.
- U.S Army Research Institute for Behavioral and Social Sciences (2004) Think like a Commander.
  Available from: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425737 [Accessed 10th September 2017]
- Viner, K. (2016) How technology disrupted the truth. *The Guardian* (12/07/2016).
  Available from: https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth [Accessed 10th September 2017]