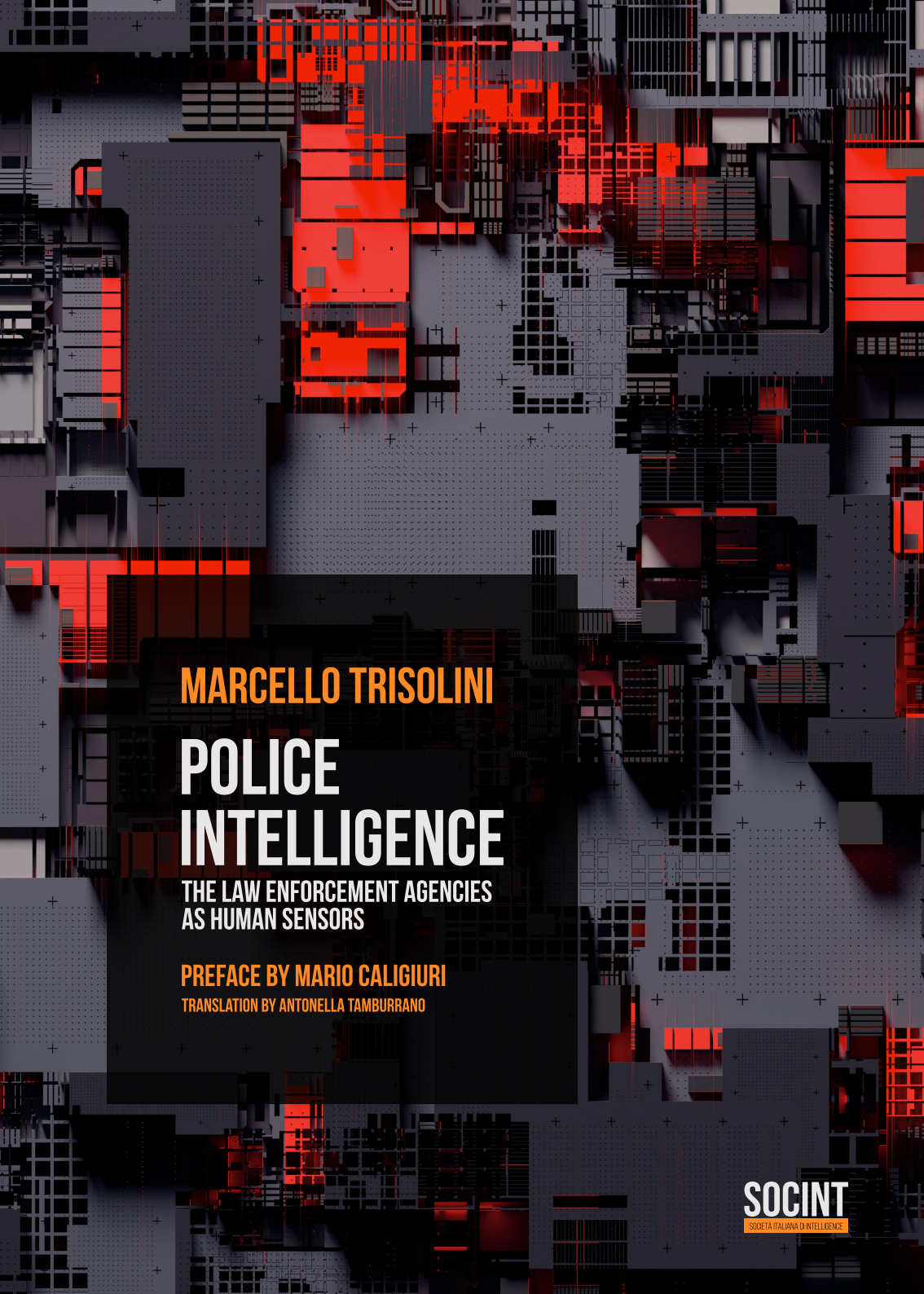

MARCELLO TRISOLINI
POLICE INTELLIGENCE
THE LAW ENFORCEMENT AGENCIES AS HUMAN SENSORS
PREFACE BY MARIO CALIGIURI
TRANSLATION BY ANTONELLA TAMBURRANO
SOCINT
SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT Società di Intelligence Italiana - ***Press***

Original title:
Intelligence di Polizia
Le Forze di Polizia come Human Sensors
December 2020, February 2021,

© Marcello Trisolini September 2023
Società Italiana di Intelligence
c/o Università della Calabria, Cubo 18-b, 7° piano
via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia

https://www.socint.org
DOI: 10.36182/2023.02

ISBN 9791280111401

Socint Press
Translation by Antonella Tamburrano

Cover Design: BESKEIE

CREDITS
Font family: Roboto Light
Cover picture: Unsplash.com - Computer generated image of a city with red lights
by Risto Kokkonen

Marcello Trisolini

Police Intelligence

The law enforcement agencies as human sensors

Preface by Mario Caligiuri
Traslation by Antonella Tamburrano

SOCINT Società Italiana di Intelligence
Press

INDEX

Abstract p. 6

Preface by Mario Caligiuri p. 9

Introductory notes p. 18

CHAPTER 1
WHAT IS THE HUMAN SENSOR

1.1 – From the symmetric war to the asymmetric war p. 27

1.2 – The antiterrorism and the asymmetric war: the Isralian experience p. 30

1.3 – Human Sensor and the 4th battalion p. 33

1.4 – Fundaments of the activity of the Human Sensor p. 38

CHAPTER 2
A DIFFERENT VISION OF THE POLICE FORCES

2.1 – Intelligence of the Information Services and of the Police forces p. 43

2.2 – The OES (observation, elicitation and surveiilance) activity p. 47

2.3 – The Police forces in Italy p. 53

2.4 – The police activity outside of the service p. 60

2.5 – The implementation of the OES model in the Human Sensor activity: a matter of social psychology and statistics p. 63

CHAPTER 3
THE HUMAN SENSOR IN THE ACTIVITY OF POLICE INTELLIGENCE

3.1 – Police Intelligence and National Security p. 78

3.2 – The investigative and informative model in the practical activity of the Police Forces p. 86

3.3 – The importance of the Human Sensor in the new demographic and technological scenarios p. 98

Conclusions p. 111

Glossary p. 115

Preface sources p. 117

Bibliography p. 119

Index of names p. 124

ABSTRACT

If everyone is looking at the virtual world,
who is looking at the real one?

Police intelligence
The law enforcement agencies as Human Sensors

by
Marcello Trisolini

All human activities, whether they are social, economical, political or military depend on internet more and more. Nonetheless, governing and controlling the virtual world (or *cyberspace*) mean governing and controlling the real one. And for this reason, States and privates are steering the main resources and intelligences in this direction. However, not everything happens or will happen on internet. Actually, precisely because the attention is mostly pointed towards the virtual world, possible scenarios of danger to the National Security might occur in the real world. So, this implies not just the necessity of finding an efficient way not to leave totally defenceless this enormous front, but that it is also economically convenient given the constant disengagement of resources from the real world to the advantage of the virtual world.

In such circumstances it's always suitable to evaluate and to give value to what you already have in your organization, before embarking on new paths.

Italy is the third State in the world with the largest number of Police forces in relation to the population and it remains the only country to have four law enforcement orders of national nature. This is an organization that, in spite of the fact that it raises problems of effectiveness of the informative, investigative and coordinating activity, could be used to determine better results in reference to the National Security, all thanks to this particular structure.

The law enforcement agencies in Italy, in fact, are a force: numerous (more than 300 thousands of units), present and distributed throughout the national territory, with basic military training already available and without major costs of employment to be added.

Therefore, if the Police forces were trained in a "specific" way, extending the training to all its members in a generalised way, it would be possible to implement those skills of observation, elicitation and surveillance (OES) of the territory that very often not all police officers possess. These are skills that each operator would exercise in a more or less effective way not only when on duty, but especially when he is a simple citizen. This new orientation would not only give the Police forces a greater information capacity, useful in the fight against organized crime, but would also significantly increase the chances of the Intelligence activity to intercept those "weak signals" that are as difficult to recognise as they are dangerous for the National Security.

Every day, members of the Police forces are naturally immersed in real and dynamic places such as cities, towns, streets, stores, churches, museums, etc.; they talk to acquaintances and strangers, they observe, listen and receive infor-

mation of all kinds, but not always and not all of them know how to obtain useful information. So, it's just a matter of telling them what and how to do. A "large army" already scattered throughout the territory and ready to be activated as if they were many human sensors (Human Sensors - a theory already used in the military), able not only to monitor a larger portion of the population and territory, but to understand the subtle nuances.

Humans differ from other artificial collection systems in that they interact with each other and their surroundings in the most unpredictable ways and more than any artificial sensor ever will. Hence the concept that every law enforcement worker is a human sensor on the ground.

While technology will impact the future of each State's Homeland Security, its success will continue to be determined by its most important resource, weapon, and sensor: the human.

PREFACE
by
Mario Caligiuri

9/11 was considered an international intelligence failure, as the technological prevalence in the defence of national security had not prevented the most sensational terrorist attack of all time. Yet information, in various ways, had been gathered beforehand but unfortunately was only interpreted after the event[1].

We are currently experimenting with technologies to defend ourselves against the pandemic that has brought the planet to its knees, and the various solutions do not always yield appreciable results. In Italy we have the largely disappointing example of the "Immuni" app[2].

Both cases demonstrate that relying almost entirely on technology is not the appropriate strategy to deal with the dimension of risk that will be increasingly endemic in the 21st century[3].

So, a kind of paradox seems to be emerging that shows how the irrepressible invasion of technology and artificial intelligence is matched by the need to increasingly comple-

---

1 W. Lawrence, *Le altissime torri. Come al-Qaeda giunse all'11 settembre*, Adelphi, Milan 2007.

2 Among others, see: *Il fallimento di Immuni è costato molto caro. L'equivalente in Germania funziona benissimo*, 9.11.2020, https://www.nonsprecare.it/fallimento-app-immuni; Lo spettacolare fallimento delle app contro il coronavirus,-9.7.2020,-https://www.repubblica.it/dossier/stazione-futuro-riccardo -luna/2020/07/09/news/lo_spettacolare_fallimento_delle_app_contro_il_coronavirus-261374292/

3 U. Beck, *La società del rischio*, Carocci, Rome 2000.

ment the human factor. It is no coincidence that, in order to ensure fundamental national security, Israeli intelligence has been hiring hackers and philosophy graduates at the same time for a while now: the former to locate information in the innermost recesses of the Web and it the latter to interpret it[4].

In our age, social manifestations take place, directly and indirectly, to a considerable extent in cyberspace, as more than half of the world's population is connected to the Web, which represents the prevailing sphere from an economic and political, communicative and educational point of view.

Crimes are also exponentially increasing on the web, so much so that cybercrime represents the second largest source of income for mafias after the drug trade[5].

Therefore, the issue of cyber security is central[6].

It is no coincidence that just recently in Italy the Italian Institute of Cybersecurity was created by law under the direct emanation of the Prime Minister's Office, which is a clear indicator of how national security activity must necessarily be oriented towards the cyber space[7].

Indeed, the national interest will increasingly be secured

---

4 M. Caligiuri, *Intelligence e guerre dell'informazione nel XXI secolo: come respingere più efficacemente le minacce cyber*, in U. GORI (a cura), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Angeli, Milan 2019, p. 55.

5 It is not easy to estimate the rising cost of cyber espionage, which would amount to $445 billion and which for General Keith Alexander, Director of the National Security Agency (NSA) from 2005 to 2014, represents the 'largest transfer of wealth in history'. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

6 One of the most attentive scholars of the phenomenon is Umberto Gori, of whom among many see U. Gori, L.S. Germani (a cura), INFORMATION WARFARE 2011, *La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale,* Angeli, Milan 2012.

7 M. Caligiuri, *Istituto Cyber? Modello Mossad*, 15.11.2020, https://formiche.net/2020/11/istituto-cyber-modello-mossad-scrive-caligiuri/.

to a large extent by cyber security, on which a country's *rating* could soon depend[8]. It is no coincidence that the de facto wars we are fighting today, starting with the Covid-19 war[9], are above all wars of information, internal and external to nations and people[10].

Another aspect that needs to be considered is the constant urbanization, since in a few years the majority of the world's population will live in megacities organized by increasingly powerful technologies, the so-called *smart cities*. This will inevitably pose significant security problems[11].

Smart cities will be cities that will make the quality of life easier for citizens, who will, however, be constantly monitored, delineating a surveillance society[12].

In the strategic areas of smart cities, the mobility, public works, energy and waste sectors will be central, with foreseeable encroachments of organized crime linked to corruption[13].

Within this framework, the use of artificial intelligence

---

8 This is what the Ministro degli Esteri of the Monti's Government, Giulio Terzi from Sant'Agata claims. P. Fiore, *Il rating di uno Stato dipenderà presto dal suo grado di cybersecurity?*, 3.12.2018, https://www.agi.it/innovazione/rating_sicurezza_informatica_difesa-4694301/news/2018-12-03/.

9 Caligiuri Mario (a cura), Post Covid-19, Analisi di Intelligence e proposte di policy 2020-2021(2020), annex a "Formiche", n. 5, May 2020.

10 G. Gagliano, *Guerra psicologica. Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco, Rome 2013.

11 M. Caligiuri, *Potere e sicurezza nelle smart cities*, in "Limes", 5, May 2019, pp. 231-236.

12 Z. Bauman, D. Lyon, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014. The 'surveillance society' is in turn producing 'surveillance capitalism': S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Rome 2019.

13 G. Galli, *Il golpe invisibile. Come la borghesia finanziario-speculativa e i ceti burocratico-parassitari hanno saccheggiato l'Italia repubblicana fino a vanificare lo stato di diritto*, Kaos, Milan 2015.

technologies in the field of crime prevention is rapidly developing[14].

Pre-crime algorithms, however, must be used with great care because they could turn into their opposite, posing the central problem not so much of privacy, which in fact does not exist, but of the human management of institutions and political elites[15].

Therefore, referring to what used to be considered science fiction, human qualities will be more and more fundamental.

In the futuristic 'Minority Report', Philip K. Dick's 1956[16] short story that became a blockbuster film in 2002[17], there is an anti-crime police unit called the 'Precog', in which through the powers of the minds of a few super-gifted people, crimes are predicted before they are committed. So, security is still

---

14 " Among others, in Los Angeles with the Predpol programme, in Chicago with the definition of algorithms for analyzing urban crimes, and then in Germany with the Pre Crime Observation System activities and the London Metropolitan Police using Accenture software to detect gang members who may commit a crime in advance. In Italy, too, these experiences are developing. It started in 2007 in Milan with Key Crime, which calculates the most at-risk targets, and then later in Trento with the Predictive Urban Security Laboratory 'Esecurity', while in Venice on 16 November 2018 an algorithm had already predicted a theft and in Naples an inspector of the police headquarters, Elia Lombardo, developed the 'XLaw' system based on the four P's: prevention, prediction, proactivity, participation". M. Caligiuri, *Potere e sicurezza nelle* smart cities, cit., p. 234. Elia Lombardo specified his project in E. Lombardo, *Sicurezza 4 P. Lo studio alla base del software XLAW per prevedere e prevenire crimini*, Mazzanti, Venice 2019.

15 " In the long run, the question will not be who or how, from time to time, should be in charge, but whether, and if so how, anyone will still be willing to obey". G. Azzolini, *Dopo le classi dirigenti. La metamorfosi delle oligarchie nell'età globale*, Laterza, Rome- Bari 2017, p. 161.

16 P. K. Dick, *Rapporto di minoranza e altri racconti*, Fanucci, Roma, 2002, Original Edition is from 1956.

17 *Minority Report*, film directed by Steven Spielberg (2022).

guaranteed by people and not by algorithms[18].

In this broad and overwhelming cultural context is the innovative work of Marcello Trisolini who, as the culmination of a brilliant course of studies, delves into the figure of the *human sensor* in the Police forces[19].

The author interprets Police forces as *human sensors* in intelligence activities, through the interdisciplinary approach of statistics, social psychology and economics. In particular, he proposes specific training methods to develop observation and surveillance skills[20], using the model pioneered by the US 4th Infantry Battalion during the Second Gulf War in 2003[21].

---

18 This literary fiction, however, brings attention to the powers of the mind that were explored by intelligence agencies during the Cold War. See L. Buchanan, Il settimo senso. I segreti delle spie psichiche dell'esercito americano, Edizioni Il Punto di Incontro, Vicenza 2010; S. Ostrander, L. Schroeder, Scoperte psichiche dietro la cortina di ferro. URSS/BULGARIA/CECOSLOVACCHIA, MEB, Turin 1975; A. Lissoni, Psicospie. Viaggio negli archivi segreti del paranormale in America, Russia e Medioriente, Editoriale Olimpia, Sesto Fiorentino 2003. See also A. Teti, PsychoTech. Il punto di non ritorno. La tecnologia che controlla la mente, Springer Verlag, Milan 2011, where an entire chapter is dedicated to remote viewing, citing experiments such as Semipalatinks. In addition, the 2009 film The Man Who Stare at Goats by Grant Heslov is an ironic parody of the activities of a secret department of the US military that aims to use paranormal activities for war purposes.

19 Marcello Trisolini obtained his Master's degree in Intelligence at the University of Calabria in the academic year 2018-2019 with a mark of 110 academic honours, discussing a thesis entitled "*Intelligence di polizia. Le Forze di polizia come human sensors nell'attività di Intelligence*", with supervisor Marco Valentini. A summary of the work will be included in the forthcoming volume M. Caligiuri (a cura), *Studi di intelligence 3. Avvicinarsi alla realtà*, Rubbettino, Soveria Mannelli 2021.

20 The capacity for 'observation, elicitation and surveillance' is referred to by the acronym OES. The term elicitation from a psychological point of view means stimulating questions, asking oneself questions.

21 On the occasion of the Second Gulf War, the realization dawned on all soldiers that their daily observations played an essential role in providing the 'contextual information' that more advanced intelligence systems were unable to provide.

The text argues that the use of technology may prove ineffective in gathering information in the face of the transformation of cities into boundless suburbs, populated by an underworld made up of criminals and terrorists, the socially disadvantaged and lone wolves. A 'real' world that is difficult to penetrate by technologies, but those in charge of human control should be enabled to identify useful information, grasping nuances and identifying contexts.

Hence the concept, and the consequent proposal, that every police forces operator should be trained to be a *human sensor* on the ground because humans interact with each other and their environment in the most unpredictable ways and more than any artificial device ever could.

As a framework there is precisely the Police Intelligence understood in terms of National Security, considering that the continuous transformation makes threats less and less identifiable.

Within this framework, the figure of the *human sensor* can represent an outpost of security, a guarantee for citizens who increasingly need 'human symbols' to refer to.

Worthy of note is the author's in-depth study of the Israeli experience, which, by constantly having to deal with non-state combat organizations, has gained important experience in irregular warfare and counter-terrorism. Operating in a reality that is difficult to prevent and cope with by conventional methods, the Israelis implemented a broader contextual intelligence gathering, involving not only defence, police and intelligence forces, but also the private sector and the entire population, creating a highly effective integrated collaboration.

All this highlights the need to review the current and prevailing bureaucratic and legal formation of the Police forces,

which is increasingly called upon to predict rather than to repress.

To do this, it is necessary to develop a tendency that is peculiar to Intelligence, which is to pick up 'weak signals', the opposite of those that process Big Data.

Therefore, the *Human Sensor* figure is required to be able to contextualize, connect the dots, start from facts to interpret and anticipate reality[22].

Ultimately, this figure takes note of the changes and debate of the role of security over the last 30 years, projecting into the future where the growing presence of mafias taking advantage of the prevalence of economics over politics can be expected.

It is no coincidence that, as early as the mid-1990s, the director of German espionage Eckart Wertherbach claimed: 'With its colossal financial power, organized crime secretly influences our entire economic life, social order, public administration and justice, in some cases dictating politics its law, its values. If this development were to proceed, the State would soon be incapable of guaranteeing the civic rights and freedoms of its citizens'[23].

The asymmetries of globalisation actually favour organized crime[24],which is often ahead in its use of technology and behaviour, as it adopts flexible strategies of communicative retreat in order to be less identifiable: famous is the case of

---

22 H. Rosling, *Factfulness. Dieci ragioni per cui non capiamo il mondo. E perchè le cose vanno meglio di come pensiamo*, Rizzoli, Milan 2018.

23 E. Wertherbach, *Organisierte Kriminalität, in "Zeitschrift für Rechtspolitik"*, 1994, n. 2.

24 M. Naim, *Illecito. Come trafficanti, falsari e contrabbandieri stanno controllando l'economia mondiale*, Mondadori, Milan 2006.

the 'pizzini' used by mafiosi to avoid being intercepted[25].

In this scenario, Intelligence is increasingly characterized as the time of the future, since it is a technique and knowledge that keeps humanity at the centre of the social processes, so as to remove it from the irrelevance of superfluous peoples to which it seems to be inevitably destined[26].

As is well known, cinema, like art, often anticipates what is to come. And I believe that the 2012 James Bond film *Skyfall*, where 'M', the head of Her Majesty's Secret Intelligence Service, expresses herself before a parliamentary committee, can be considered in this category: 'I see a different world from yours. And the truth is that what I see scares me very much. I am scared because we no longer know who our enemies are. They are no longer traceable, they are not nations. They are individuals. Our world is no longer transparent, now. It is more opaque. It is in the shadows. It is there that we must fight'.

And this is precisely the idea of Marcello Trisolini's essay, which has a high civil value because it believes in the role of the State and identifies the human dimension as the most feasible one for defending security.

---

25 "In mafia jargon, each of the notes exchanged between the bosses and their affiliates (to avoid being intercepted, by telephone or telematically), through a dense network of intermediaries, to give information or issue directives, adopting for security reasons a coded language, however cryptic". Vocabolario Treccani, https://www.treccani.it/vocabolario/pizzino/. Vedi C. Faverzani, D. Lanfranca (a cura), *La storia, le storie. Camilleri, la mafia e la questione siciliana*, Quaderni Camilleriani 2. Oltre il poliziesco: letteratura/multilinguismo/traduzioni nell'area mediterranea, Grafiche Ghiani, Monastir 2016.

26 "When algorithms will have excluded humans from the labour market, wealth and power could be concentrated in the hands of a tiny elite that owns the very powerful algorithms, creating the conditions for unprecedented social and political inequality". Y.N. Harari, *Homo Deus. Breve storia del futuro*, Bompiani, Milano 2017, p. 490.

Police Intelligence

The law enforcement agencies as Human Sensors

Introductory notes

In the last thirty years, since the end of the *short century*, the real world seems to be becoming an ersatz world, where there are no more boundaries, no more matter, no more time, and where everyone is interconnected and interdependent.

A world that is increasingly taking on the connotation of a 'super-brain' endowed with 'its own intelligence', but of which no one can yet say to whom it really belongs or will belong in the future, and where each individual who's connected to it by means of a PC, *smartphone* or other *device*, is nothing more than a simple 'neuronal element', necessary to branch out and enhance its own structure[1].

According to recent surveys[2], in fact, there are about 4.4 billion individuals connected to the Web in the world and this number is constantly increasing: this means that more than half of the world's population is connected to the Internet. The other side of the planet, on the other hand, the one that does not have access to the digital world, remains excluded mainly for two reasons: because of the limitations imposed by some countries on the freedom of their citizens and because of eco-

1 Just think of artificial intelligence (AI), the Internet of things (IOT), augmented reality (AR) and virtual reality (VR), smart cities, information and communication technologies (ICT).

2 ITU (International Telecommunication Union), *Report on the implementation of the Strategic Plan and the activities of the Union for 2018-2019 (ITU Annual Progress Report),* ITU/Concil, Document C19/35-E, Geneva, 18 April 2019. Cf. Also the «Rapporto sulle statistiche digitali globali Q3» published by *Hootsuite* and by *We Are Social,* 2019.

nomic restrictions that cut off the poorest countries.

It has often happened in the history of mankind that the introduction of a new technology has brought about a more or less significant change in people's lives, but none like the advent of the Internet has been able to so profoundly, rapidly and totally change the way of life of a large part of the world's population, so much so that an anthropological change in society itself can be envisaged.

Today, as it has been wisely observed, «we are experiencing not so much an era of change as a change of epochs[3]; a change like the discovery of America or the French Revolution, to name but a few. The effects on individuals, society and democracies of this new world opening up before us cannot yet be determined, although the prodromes do not bode well».

Until a few decades ago renowned scholars believed that television, a domestic tool, was one of the greatest dangers to society: an object capable of influencing people's behaviour and opinions, from an early age[4]. Today, the question does not even seem to arise. The advent of the Internet has completely overturned the social, economic and political conceptions hitherto developed. If television needed a physical place to determine its power over the individual, the *smartphone* simply needs to become a 'prosthesis' of the latter. Today, wherever you turn, you can see people who do not interact with their surroundings because they are bent over sta-

3 Giansoldati Franca, *Papa Francesco: Il comunismo ci ha rubato la bandiera*, in «Il Messaggero», 29th June 2014.

4 Popper R. Karl, *Cattiva maestra televisione*, Marsilio Editori, Venice, 2006. Cf. also Sartori Giovanni, *Homo videns*, Editori Laterza, Bari, 2007.

ring at small light screens. A world, this one, to which everything and everyone is deeply and constantly turned.

Now, as is often the case, when everyone is looking one way, we do not realize what is happening on the other. In this regard, there are many studies and experiments in social psychology that can provide us with useful tools to understand the different aspects of this issue. Contrary to popular belief, we are not observers at all. In fact, we do not pay attention to most of what surrounds us precisely because we are too focused on what catches our attention at a given moment[5]. However, in order to better introduce this aspect, in a dimension that can clarify the basic idea that will underpin this study, we will refer to cinematic fiction.

In 2011, a television series called *Black Mirror* was first aired in the UK and was destined to cause a sensation. Its creator, Charlie Brooker, imagines a world set in the future, but actually inspired by today's world, with the aim of showing how technology, mass media and social networks are changing our lives, overwhelming them and slowly devouring them. In the first episode (*The National Anthem*), the author poses an important question about the limits and dangers of the media with which we are interconnected every day, which lead us to forget or not notice what is really happening in the real world: this will be the focus of the present study, projected in the context of

5 Chabris Christopher, Simons Daniel, The Invisible Gorilla. And other ways in which our intentions deceive us, Gruppo 24 ore, Milan, 2012. It is also useful to mention some cognitive errors, such as: the anchoring effect (the tendency to make decisions by relying excessively on the first piece of information available); the herd effect (the phenomenon whereby people perform certain acts or believe in certain things just because the majority of people do).

National Security and the fight against organized crime.

The film begins with a phone call received by the British Prime Minister in the middle of the night informing him of the kidnapping of the princess, beloved by her people. The ransom demand is shocking: the princess will be killed if the Prime Minister does not have full sexual intercourse with a pig within the following hours on live television and on all terrestrial and satellite networks. The choice is stark: to lose one's dignity as a man and as a politician, live worldwide, or to lose it anyway in the eyes of the world by leaving the princess to her fate? For the man, it is the beginning of a nightmare that will sorely test his morals and those of an entire people. Time is up and the decision is made. And while everyone is turned and concentrated on witnessing an event as extraordinary as it is disturbing, the princess has already been freed by the same jailer in the deserted streets of the city without anyone being able to rescue her or prevent the foul deed, because everyone is turned to watch the event on TV.

Such a scenario is certainly possible, albeit somewhat improbable, even though it concerns television fiction. Of course, there are many events that could be possible. One must always ask oneself whether what is possible is also probable: an exercise, this, that is useful to avoid analysing and making predictions on fanciful, *Hollywood* contexts. Yet on 11th September 2001, four airliners with civilians on board were hijacked by Arab terrorists and used as missiles to hit military and civilian targets. Even film fiction had never before gone so far as to imagine such an event. Television broadcasting, news reporting, state apparatuses and the overwhelming majority of the world's population was turned on its

head to watch those incredible events. In those hours and the following days everyone was looking in one direction.

Today, any event, whether dramatic or not, is captured by the *smartphones* of dozens and hundreds of witnesses, framed from any possible perspective and displayed in real time around the world as it could have never happened in 2001.

It is therefore necessary to ask oneself whether turning one's gaze exclusively in one direction, i.e. to the control and use of *cyberspace* as a field of human actions, might not give terrorist or criminal organizations a free hand in arranging dangerous activities against a nation or population outside the Internet, or allow isolated individuals to move freely outside the cyber world precisely to escape possible controls (cf. the *hawala*[6] economic system used to finance the smuggling of illegal immigrants and terrorist activities).

Of course, no one doubts the importance and necessity of directing the main resources and intelligence to the garrison and control of the cyber space, given its numerous economic, social, political and military repercussions; but nonetheless, it is necessary to reflect on which fronts remain unprotected and poorly defended.

If, therefore, the idea that everything can be foreseen and averted is not viable, and if the bulk of resources and synergies must necessarily be directed towards the *cyber* world, how and where are new resources to be found to acquire information and control what is determined in the real world?

---

6 See, Atti Parlamentari, Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere, Stabilimenti tipografici Carlo Colombo, XVII legislatura, Doc. XXIII - No. 30, 14 Decembre 2017.

The answer could come from a different approach of the Police forces to the conception of their role on the ground, a hypothesis that is also confirmed by statistics.

In 2004, the American journalist Michael Monroe Lewis recounted in his book *Moneyball: The Art of Winning an Unfair Game* the historic feat of the Oakland Athletics baseball team that, during the 2002 season, won twenty consecutive games, setting a new record with a limited budget and a new form of statistical calculation to decide which athletes to buy. *General manager* Billy Beane, after losing his best players, was denied a budget increase by the club in order to compete with richer teams. So, how could big results be achieved with small expenses? The answer was given to him by Peter Brand, a young economics graduate from Yale with radical ideas on how to evaluate a player. Hired as an assistant, Brand convinced the manager to select players based almost exclusively on the percentage that indicates the number of times a player wins a base without penalty help, thus succeeding in creating a competitive team with greater potential than they could have done using traditional selection methods and little money.

Italy is the third State, after Russia and Turkey, with the highest number of Police forces in relation to the population (467.2 officers in service per 100,000 inhabitants, Eurostat 2015 data), and remains the only country in the world to have four national Police forces (Polizia di Stato, Carabinieri, Guardia di Finanza and Polizia Penitenziaria) to which the Fire Brigade and the Corps of the Captaincies must be added. Each corps naturally has its own commands, its own operational centres, its own barracks, its own generals defending its sta-

tus. What is more, in addition to the enormous expense that this entails, the overlapping of subjects and competences, there is also the lack of a system based on the centralization of the analysis of data collected by all the armed forces and Police forces (with the exception of the C.A.S.A.)[7]. Putting aside this aspect, which in any case remains central to any intelligence activity one wishes to carry out, is it possible to use this large Police forces already available and distributed throughout the territory as a 'territory sensor', to monitor, detect, acquire information useful for National Security and the fight against organized crime?

Naturally, it is not a question of reiterating the prerogatives, obligations, duties and *modus operandi* to which the members of the Police forces already refer, an activity distinct and different from those of the institutional Intelligence, but of endowing the former, by means of *ad hoc* training, with that capacity of observation, elicitation and surveillance of the territory and of the people, which often not all police operators possess. More than half of the members of the Police forces, in fact, deal mainly with bureaucratic activities, while only a small percentage regularly carry out investigative and territorial control work, activities which are useful in being able to read the surrounding environment in a different way.

If, therefore, the education of members of the Police for-

7 The Strategic Anti-Terrorism Analysis Committee (C.A.S.A.) is a body of the Ministry of the Interior composed of representatives of the various Italian Police forces and Services with the task of fostering and sharing information on terrorist threats inside and outside the Republic. The C.A.S.A. was established by a Ministerial Decree of 6th May 2004 in the aftermath of the attack on the Italian contingent in Nassiriya.

ces were to be implemented with training aimed at improving those aspects mentioned above (observation, elicitation and surveillance), there would be a huge number of 'human sensors' on the ground, not only active during working hours, but especially when the operators are off duty. Relying, therefore, on the high number of law enforcement personnel, on their diffusion throughout the territory and on the fact that they are already militarily trained men and women (basic training), it could be assumed with good reason that statistically the *Human Sensors* could greatly increase the chances of the Intelligence or *Intelligence-led policing*[8] apparatuses to acquire useful information concerning terrorist and organized crime activities on the national territory.

There are two realities that have experimented and undertaken a similar direction: the 4th battalion of the 27th US Field Artillery Regiment (deployed in Baghdad in 2003); the Israeli army - Israel Defence Forces (IDF), in which the population actively participates in the defence of the nation.

Finally, the study and development of the considered hypotheses will be analysed and compared with the practical aspects arising from police investigative and operational activities, which emerged from the administration of a number of questions submitted to the operators themselves.

---

8 Intelligence-led policy: intelligence-led policing or information policing. It is a policing model that frames all the main police activities (from the fight against organized crime, terrorism, drug trafficking, immigration, to territorial control) in a more efficient way (in terms of optimisation of the resources deployed) and more effective (in terms of results) thanks to adequate preventive analysis of criminal phenomena. An approach, therefore, which postulates close integration between intelligence and police activities in which data analysis is fundamental for a decision-making framework. Cf. Ratcliffe Jerry H., *Intelligence-Led Policing,* Willan Publishing, Cullompton – UK, 2008, p. 6 et seq.

Chapter 1
What is the Human Sensor

1.1
From symmetrical to asymmetrical warfare

Until the Gulf War, the nature of the conflicts between the different antagonists on the world chessboard was *symmetrical* or traditional in nature: two or more clearly recognizable opposing sides competing for resources, territories or commercial advantages by threat or the use of force. The balance between the forces in the field or the victory of one or the other front depended on the superiority in the economic, scientific and technological fields.

Subsequently, the war becomes asymmetrical, in other words, a clash of forces in the field that is enormously unbalanced: where one side, weaker, obeys its own rules, uses unconventional methods and is unrecognisable or incomprehensible in the eyes of the adversary; while the other, although technologically, militarily and economically stronger than the antagonist, suffers its heavy attacks at the most critical and delicate points of its centres of gravity[1].

During the Cold War years, for instance, the logic of nuclear deterrence ensured a certain stability and predictability of the global political-military system. A system in which all the main actors moved within a framework of certain and

1 Cfr. Mini Fabio (edited by), Qiao Liang, Wang Xiangsui, *Guerra senza limiti – L'arte della guerra asimmetrica tra terrorismo e globalizzazione,* LEG Edizioni, Gorizia, 2002, p. 184.

well-defined coordinates: the alignments were well known, the areas of influence defined and geopolitical interests determined. Since the fall of the Berlin Wall, however, the system seems to be slipping into an increasingly uncertain and chaotic world[2]. Alongside the Westphalian state, a whole series of other international actors are powerfully emerging that, like the former, have the capacity to affect political dynamics. Thus, we have moved from the traditional conflicts between one state and another, to conflicts that have the state or states on one side, and on the other a pulp of unrecognizable actors that, while structurally weaker than the former, prove to be much more dangerous.

The nature of contemporary conflicts, therefore, is characterized precisely by the unpredictability and unknowability of the enemy, made possible by two new scenarios that have completely upset the previous power relations: first, the emergence of asymmetric warfare[3]; and second, the attacks on information and communication systems.

The two new aspects have in fact produced an international system of *variable geometry* where, alongside those subjects for which the rules of international politics still apply, a large periphery, or several peripheries, have emerged where relations between subjects are governed by their own rules.

---

2 The last decade of the 20th century was characterized, as never before, by profound upheavals in the world. Of the many causes behind these transformations, one seems to stand out above all others: the Gulf War. *Ibidem*.

3 The concept of asymmetric warfare has changed in meaning over the years. At first, in fact, it was used by the United States to indicate the enormous technological gap that existed between American forces and the adversaries they had to confront (Cf. Jean Carlo, *Manuale di studi strategici*, CSGE, Franco Angeli, Milan, 2017, pp. 250-252.

During the Cold War years, therefore, war efforts were designed to confront an enemy symmetrically and force was deployed using conventional methods. In this context, the army depended on technology exclusively to be able to look behind enemy lines and destroy strategic targets. In asymmetrical warfare, none of this is possible. The enemy can be anywhere, is not identifiable and approaches the conflict with guerrilla or terrorist acts, striking at the centres of gravity of the adversary in such a way as to create great impression and fright in both the regular forces and public opinion. As a result of this new threat[4], states have had to change their strategy and deploy their military and intelligence apparatuses to identify and destroy sensitive targets using their technological capabilities and to gather information on any adversary anywhere in the world.

However, although at the strategic level the constant increase in intelligence gathering has provided a significant advantage in the different phases of conflicts, at the tactical level it has not been sufficient to bring about a complete mastery of information. The only way to meet this need, at least in theatres of war, has been a different deployment of military forces in the field.

4 The expression Global War on Terrorism (G.W.O.T.) was used by the media and the US government to refer to a series of military operations undertaken after 11 September 2001. Cf. Eric Schmitt, Thom Shanker, *Bombings in London: Hearts and Minds - U.S. Officials Retool Slogan for Terror War*, in «The New York Time». 26, July, 2005, p. 7

1.2
Counter-terrorism and asymmetric warfare: the Israeli experience

Israel, more than any other state, has since its birth found itself operating in a highly asymmetrical strategic scenario, regularly having to deal with non-state combatant organizations such as the PLO, *Hamas* and *Fatah*[1].

The Israeli military apparatus has, to its cost, gained enormous experience in irregular warfare and counter-terrorism, although the results, as you can well understand, have not always been positive.

Particularly in recent years, the IDF (*Israel Defence Forces*) has encountered considerable difficulties in responding to threats due to the increase of the asymmetric component of conflicts. The traditional efficiency and effectiveness of the Israel Defence Forces have been challenged by the asymmetric element exalted by the adversary - the Palestinian or Lebanese organizations, the weak party in question - because of the greater advantages this could bring on the ground.

Although the Israeli approach to *Counter-Terrorism* (CT) remains the most advanced and effective system that we

1 PLO (Palestine Liberation Organization); Hamas (Islamic Resistance Movement); Fatah (or *al-fatah*, is a Palestinian political and paramilitary organization).

know of, precisely because terrorism has always been a reality in the life of the country, there is no official doctrine within which to encapsulate it, and the reason lies in the very nature of the threat (terrorism is always different and unpredictable) which effectively prevents its codification. Israel has thus adopted a more organic and holistic approach to CT that relies on innovation and creativity to deter and create divisions within terrorist groups and their supporters through coercion and persuasion[2].

However, in order to cope with the continuous threats to the security of the state and its citizens, the architecture of Israeli counterterrorism relies in a variety of ways on the involvement of the entire nation: the Israel Defence Forces (the IDF); the specialized units of the security apparatus; the police; the private sector; the whole of society.

In this regard, it should be borne in mind that the entire Israeli population participates in the defence of the state not only by serving compulsory military service for several years[3], but also by remaining in the army as reservists until they reach a ripe old age. Moreover, there is an obligation, even if on leave, to serve in the army for one month a year.

This ensures that the entire Israeli population constantly participates in the security of the state, not only when they return to their military uniform, but also when they return to civilian life, while, for example, walking around Jerusalem or

---

2 Isaac Kfir, *Israel's Approach to Counterterrorism*, in «The Strategist (ASPI - The Australian Strategic Policy Institute)», 27 September, 2018.

3 Conscription is compulsory for both women (24 months) and men (36 months). Each recruit undergoes basic training (*Tironut* - the Hebrew term for the training of recruits in the Israel Defence Forces, divided into levels) lasting six months. Once they have completed their military service, they remain at the army's disposal as reservists (men up to the age of 50, women up to the age of 46).

in any other city in the country.

Their military training and the context in which they live naturally predisposes them to observe and detect everything that goes on around them just as if they were many *sensors* on the ground.

1.3
HUMAN SENSOR AND THE 4TH BATTALION

On 5 November 2003, an interview with a high-ranking US Army[1] officer appeared in a major American newspaper, emphasizing the importance of adopting a new military strategy in the Iraqi conflict, which was essential to cope with the increasing difficulties of fighting an asymmetric war. It was necessary to extend 'intelligence' to all soldiers:

> Everyone is an intelligence officer—that's sort of our theme. If you're talking about a paradigm shift, this is it: You have to see everyone you come in contact with as having intelligence value[2].

On 1st May 2003, a few months after the start of the second Gulf War[3], the US President hastened to proclaim American military superiority and the conclusion of military opera-

---

1 Vernon Loeb, *Instead of Force, Friendly Persuasion*, in «The Washington Post», 5 Novembre 2003, p. 24.

2 Cf. Michael S. Patton (Major of the 4th Battalion of the 27th Field Artillery Regiment), *ES2: Every Soldier is a Sensor*, in «Association of the United States Army, voice for army – support for the soldier», August 2004.

3 The second Gulf War dubbed Iraqi Freedom (March 2003-December 2011) was a war conflict undertaken as part of a larger "counter-terrorism" project led by the Americans and a coalition of other states (an array of 49 countries dubbed "the coalition of the willing," 15 of which reportedly requested anonymity) against Saddam Hussein's Iraq, which was guilty of wanting to use weapons of mass destruction (an information later proven to be unfounded) and allegedly giving support to Islamist terrorism.

tions in Iraq[4], adding: 'we will leave a free and democratic and reconstructed Iraq'[5]. Shortly afterwards, the conflict turned into a war of liberation from the US army, considered an invader by many Sunni and Shiite Arab armed groups, and finally resulted in a civil war between the various factions, caused by an unbalanced management of power that favoured the Shiite majority component.

The US military was thus faced with an unconventional war fought outside the traditional battlefields. Western technological warfare, based on the use of air power, but especially on the use of drones, had been decisive in the change of conflict. Unable to face the antagonist in the open field, given the absolute disparity of forces, the weaker side changed its war strategies and tactics, responding to the economic and technological superiority of the adversary with guerrilla and terrorist techniques[6].

All the information and technological capacity the US military had at its disposal was not able to prevent or avoid attacks from an unpredictable and 'invisible' enemy, of which nothing was known.

In order to cope with this new scenario, it was necessary

---

4 Landing on the aircraft carrier Lincoln, U.S. President George Bush declared, on live television, the end of the war in Iraq (behind him a banner read, Mission Accomplished).

5 Cfr. Redazione, *Bush: finiti i combattimenti in Iraq*, in «Corriere della Sera», 2 maggio, 2003.

6 The weaker side rather fights its opponent using guerrilla warfare (mainly urban), terrorist warfare, holy war, prolonged warfare, network warfare and other forms of combat. In most cases, the weak side chooses as the main axis of battle those lines of operation where its opponent does not expect to be hit and the centre of gravity of the assault is always a point that will cause a deep psychological shock in the opponent." See in, Qiao Liang, Wang Xiangsui, Limitless Warfare. The art of asymmetric warfare between terrorism and globalization, *op. cit*., p. 47

to train, integrate and maximize the most effective resource available, necessary to detect and report information directly from the battlefield and useful above all at a tactical level: the Soldier.

The first attempts were pioneered by the 4th Battalion of the 27th Field Artillery Regiment of the United States of America as described in the newspaper interview in the *Washington Post*:

> Lt. Chris Kane's patrol crossed Haifa Street and headed quickly for the back alleys of Sheik Maruf after hearing the first grenade explode. Another group of American soldiers was under attack in the sewage-clogged labyrinth.
>
> Soon, as they headed down a dark alley looking for a young man in a black shirt who threw the homemade grenade, another went off with a deafening crack, followed by staccato bursts of automatic rifle fire. In the chaos that followed, another soldier shouted that he saw someone firing from the rooftop of a house. His squad mates burst inside and found five men. They ordered the Iraqis outside. Their frightened wives and whimpering children followed. None of the men was wearing black. No shell casings were found on the roof.
>
> Kane, 24, a tall, fair, bespectacled officer from Fairfax County, two years out of West Point, approached an elder among the men and said, through his Iraqi interpreter, "Tell him we need his help." The interpreter took aside the old man, dressed in a white dishdasha, a traditional robe, and visibly shaking. The two spoke at length.
>
> At first, the old man said he knew nothing. But after more prodding and cajoling by Kane, the man relented. "I need time to relax," he said, "and then I will give you all their names."

> This is the kind of war that the U.S. Army's 1st Armored Division, "Old Ironsides," is fighting in Baghdad -- not with tank rounds and artillery shells but with persuasion and cultivated trust that produce far more powerful ammunition in the fight against a burgeoning Iraqi insurgency.
>
> "The way to win this is intelligence-based operations," said Lt. Col. Brian J. McKiernan, who commands the 4th Battalion, 27th Field Artillery Regiment, "and in this environment, it's all driven by human intelligence."
>
> With its armored vehicles sitting in parking lots, the 1st Armored Division is reinventing itself on the fly, grooming neighborhood informants and sending paid sources deep into Baghdad's teeming neighborhoods, CIA style, to collect information on Islamic militants and Iraqis loyal to former president Saddam Hussein and his Baath Party[7].

So, it has been realized that the individual soldier is the most effective collector of information, more skilful and sophisticated than all available technological systems. In the theatres of asymmetric warfare, soldiers are immersed in extremely dynamic and unpredictable operational environments: in cities, in the countryside or wherever they may be, soldiers monitor, observe and talk to the local population on a daily basis, directly acquiring information much more relevant to the context in which they operate than any technological sensor will ever be able to detect. But more importantly, humans differ from artificial information-gathering systems in that they interact with each other and their environment in unpredictable and surprising ways, more so than an artificial

---

7 Vernon Loeb, *Instead of Force, Friendly Persuasion*, in «The Washington Post», 5 November 2003, p. 24.

sensor ever could.

Of course, in order to take full advantage of this important human skill, it is necessary that soldiers are trained for such tasks by also making use of that natural predisposition to adaptation and improvisation of which humans are capable, 'thus turning every combatant into a sensor on the ground'.

The basic idea is simple: every soldier must not only be combat-ready, but in a highly changeable and unpredictable environment he/she must also be able to serve as an information collector. Hence the concept that 'every soldier is a sensor' (Human Sensor)[8].

Clearly, the value of news acquired in the field only becomes significant if it is collected, processed and integrated into a broader operational framework. If there is no analysis activity which processes the collected news and data, there is no useful information for decision-making.

8 FM 2-91.6, Soldier Surveillance and Reconnaissance: FUNDAMENTALS OF TACTICAL INFORMATION COLLECTION, Regular Army, Army National Guard, and Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 115979, requirements for FM 2-91.6., 10 October 2007.

1.4
FUNDAMENTALS OF THE HUMAN SENSOR ACTIVITY

In 2007, an important field manual (Field Manual No. 2-91.6)[1] was issued by the US Army Headquarters, which launched a new doctrine on a large scale in support of *Every Soldier is a Sensor* (ES2) initiative.

That famous paradigm shift, that had been so much advocated following the experience of the 4th Battalion a few years earlier, became a structured program adopted by the entire army. An operational decalogue that brought together a set of modus operandi to provide all soldiers with the necessary tools for gathering information during operational activities in the field such as surveillance, reconnaissance, patrolling, interaction with the local population, and tactical site exploitation[2].

Therefore, as well as providing a kind of vademecum on how to do 'information' activity and replacing a whole series of previous outdated manuals on the tactical employment of soldiers, FM No. 2-91.6:

---

1 Headquarters Department of the Army, *Field Manual No. 2-91.6 – Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*, General Dennis J. Reimer Training and Doctrine Digital Library, Washington, 2007.

2 Tactical site exploitation refers to actions taken to ensure that documents, materials and personnel are identified, collected, protected and evaluated in order to facilitate further action.

• Provides the doctrinal framework for Soldiers and leaders at all echelons and forms the foundation for ES2 curricula within the Army Education System. Its audience is broad, from military Soldiers and leaders to civilians. It is essential that all Soldiers and civilians understand how their daily observations feed into the bigger intelligence process and help create a more favorable environment for US success in a region.

• Is a compilation of tools to help all Soldiers collect information through tactical questioning, detainee handling, and document and equipment handling in offensive, defensive, stability operations, and civil support operations.

• Is not intended to make the Soldier an expert on intelligence collection. It is not intended to train Soldiers as intelligence collectors nor authorize Soldiers to conduct interrogation and source operations.

• Introduces the basics of questioning and reporting and provides some tools for patrols and S-2s.

• Applies to the Full Spectrum Operations. Principles outlined are valid under conditions involving use of chemical, biological, radiological, nuclear, and high yield explosives (CBRNE)[3].

In order to overcome the *impasse* caused by a highly asymmetrical warfare scenario, the Americans realized that they had to embark on another way of warring, one that

3 Headquarters Department of the Army, *Field Manual No. 2-91.6 – Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection,* op. cit. p. iii.

necessarily entailed a tactical knowledge of the territory in which they were operating and the people who inhabited it. It was essential, that is, to implement in all soldiers the awareness that their daily observations played an essential role in providing the 'contextual information' that the most advanced intelligence systems were unable to provide.

Among the main activities to which soldiers must pay most attention are interactions with the local population. The handbook emphasizes how building and improving these relationships allows them to obtain 'information of immediate value' that is important for understanding the environment[4]. Equipping oneself with a guide, which is useful for interacting with locals and moving around the territory, is also strongly recommended. Of course, there are restrictions to which soldiers must adhere. For instance, although it is useful and necessary to ask questions of the natives to acquire news and establish contacts, soldiers are not allowed to pay or reward for information received, nor are they allowed to ask or instruct someone to seek specific information. This would be equivalent to undertaking operations that fall within the realm of intelligence (*source operations)*[5]*,* activities denied to anyone without training in source management.

Despite the existence in each soldier of a different level of awareness and skills in information gathering activities

---

4 To this end, all soldiers are provided with both some notions of psychology and verbal and non-verbal communication, as well as practical elements, for example, on how to ask questions, what questions to ask or not to ask, and so on. Cf. Field Manual No. 2-91.6, op. cit., p. 3-1 et seq.

5 Headquarters Department of the Army, *Field Manual 2-22.3 (FM 34-52) Human Intelligence Collector Operation*, General Dennis J. Reimer Training and Doctrine Digital Library, Washington, 2006, pp. 1-4; 5-1; 8-7.

(due to a number of variables including experience gained in the field), the adoption of this program has undoubtedly demonstrated the importance and centrality of the role played by each soldier as a *Human Sensor* in highly asymmetrical contexts. A different use of military activity that favoured the acquisition of those information that were useful for understanding the surrounding environment, determining an informational success where sophisticated and technologically advanced systems had failed.

Indeed, soldiers are often the first to notice changes in their theatre of operations precisely because they are aware of them. Ultimately, immediately identifying possible danger indicators means avoiding disastrous situations for the safety of soldiers and civilians.

On the basis of the American experience (ES2), it would be interesting to elaborate and test a training model (and an operational manual) aimed at training all Police forces, in order to implement 'observation, elicitation, and surveillance'[6] capabilities, useful for gathering environmental information for the protection of National Security and the fight against organized crime, finally verifying whether and how significant they are.

6 See paragraph 2.2

Chapter 2
A different vision of the Police forces

2.1
Information Services and Police Forces Intelligence

When we refer to the intelligence activities (i.e., the processes of acquiring, organizing, and managing information)[1] carried out by the Intelligence Services and the Police forces, it should be kept well in mind that the purposes of these two entities pertain to different areas[2]. A distinction that is present in all countries with some nuances that may relate to both organizational[3] and functional arrangements.

While *Institutional Intelligence* is the tool by which the state collects, analyses, stores and disseminates (to stakeholders) information and data useful for government decision-making in matters of National Security and National Interest, *Police Intelligence* is the activity by which, law enforcement forces collect, analyse and disseminate information to higher levels or judicial or government authority. It is the information process declined through the three main phases according to a threefold direction,

1 Mosca Carlo, Gambacurta Stefano, Scandone Giuseppe, Valentini Marco, *I Servizi di Informazione e il Segreto di Stato : (Legge 3 August 2007, n.124) – presentation by Giovanni Conso,* Giuffrè Editore, Milan, 2008, p. 193 ss.

2 See table 2.1 – A.

3 The organizational structure of the Security Services in different countries can be *unitary* (as in Spain, where there is a single intelligence service with espionage and counterintelligence tasks both inside and outside the state), *binary* (as in many NATO countries including Italy where there is a distinction between internal and external intelligence activities) or *communitarian* (a system divided into several agencies, as in the US).

depending on the nature of the information processed or requested (internal higher bodies, judicial authority, political authority)[4].

With regard to our legal system, the Intelligence Services are the exclusive holders of the intelligence functions for the internal and external security of the Republic and report to the Prime Minister. The police forces are primarily concerned with the prevention and suppression of crimes and are functionally subordinate to the Judicial Authority. In this regard, it is possible to say that while for the Police forces the intelligence is an instrumental activity for the protection of public safety and public order, for the Intelligence Services, on the other hand, it constitutes its raison d'être, necessary to ensure national security from internal and external dangers.

However, the Security Services Reform Act of 2007[5], while maintaining the clear separation of the functions of the two entities, took care to establish closer cooperation between the Intelligence Services, Armed forces and Police forces:

> Within the scope of their respective attributions, the Armed forces, Police forces, officers and agents of the judicial and public security police provide all possible cooperation, including technical-operational cooperation,

4 Cit. by Caligiuri Mario in: *Predictive Policing. Il futuro della sicurezza è nei modelli di prevenzione*, regional convention, Napoli, 24 May 2019.

5 See, Law 3rd August 2007, n. 124, "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto".

to the personnel assigned to the security information services, in carrying out the tasks entrusted to them[6].

The information interchange is the main *leitmotif* of the collaboration between the different organs of the State, coordinated and directed by the DIS (Department of Information for Security), the beating heart of this exchange[7]. In particular, it seemed essential to implement the collaborative relations between Information Services and Police forces within the scope of the fight against the mafia and terrorism, establishing in both cases ad hoc bodies with which to improve the information exchange: the General Council for the fight against organized crime[8] and the Committee for strategic counter-terrorism analysis (C.A.S.A.).

Intelligence, therefore, given all due and necessary premises, is not an exclusive activity of the Information Services, but rather a method that finds its natural use in some specific offices of the Police forces, which are increasingly aimed at the analysis of criminal phenomena, investigations and the search for sources of evidence for the suppression of crimes.

---

6 Ivi, Art. 12 com.1.

7 Izzi S., *Intelligence e gestione delle informazioni – Attività preventiva contro i traffici illeciti*, Ed. Franco Angeli, Milan, 2011, pp. 61 – 64.

8 Art. 1, D.L. 29 October 1991, No. 345, converted by Law No. 410 of December 30, 1991.

Table 2.1 – A

Comparative table			
Institutional Subject	Institutional Function	Functional Dependence	Intelligence Activity
Safety Information Services	*To ensure the external and internal security of the Republic against the threats and to protect national interests.*	*President of the Council*	*Information activity aimed at obtaining all kinds of useful information to ensure the protection of the Republic and national interests.*
Police Forces[9]	*Protection of public safety and order*	*Judicial Authority*	*Information activity aimed at the prevention and suppression of crimes to protect public safety and public order.*

9 It should be borne in mind that within the Intelligence functions and activities of the four Police forces, two have general competencies (Polizia di Stato and Carabinieri) and the other two have specific and distinct competencies (Guardia di Finanza and Polizia Penitenziaria). The latter, however, are also assigned a function of contributing to public order and security activities.

2.2
The OES Activity
(Observation, elicitation and surveillance)

Since the earliest times in the history of human organization, the most powerful weapon at the beck and call of kings or powerful lords to know the plans, secrets or innermost thoughts of allies and enemies in the military, economic and political spheres has certainly been the use of spies. Not surprisingly, one of the most recurrent expressions in the world of espionage calls the spy the second oldest profession in the world.

The need to learn and practice "this dark art"[1], so important to the destiny of any kingdom or the fate of any mighty[2],

1 Depending on the historical periods and on the country under consideration, opinion toward spies does not vary much, generally deeming them a reprehensible but necessary figure. In the second half of the nineteenth century, for example, Lord FitzRoy Somerset Reglan, a British general in the Crimean War declared that "the acquisition of news by clandestine means abhors gentlemen." Indeed, he lost the Battle of Balaklava in 1854 to the Russians.

2 Since its origin, espionage has been predominantly located in the military side. It is necessary to wait until the late 16th century to see the emergence of a new concept of the organization of spies. The originator and founder of modern intelligence was the English politician and diplomat Walshingam. Alain Charbonnier writes that "the legend about the espionage skills of the English originated during the reign of Elizabeth I, when Sir Francis Walsingham organized the first political-military espionage network in the modern sense. Since then British intelligence agents, except for a few interludes that are not very honorable, but certainly very 'ideological,' to put it mildly (see the Cambridge Circle), have always worked at all latitudes 'in defence of the Kingdom.'" See Charbonnier Alain *L'Intelligence Service apre gli archivi del MI5*, in «Gnosis – Rivista italiana di Intelligence», aprile 2009.

over time has led fine intellects to codify its principles, beginning with the two oldest and most authoritative treatises on espionage that we know: the *Art of War* by Sun Tze (a Chinese general who lived between the 6th and 5th centuries B.C.); and the less widespread but equally important *Arthaśāstra* by Kautilya[3] (an Indian political scientist who lived in the 4th century B.C.).

However, whatever espionage or counter-espionage activity one wishes to consider, be it military, economic, political, technological, and so on, one must keep in mind (yesterday as well as today) the importance of the human factor as a central element of Intelligence activity and organization, especially in the interactions between individuals and in the understanding of the surrounding environment.

Throughout texts on espionage and investigative techniques, it is often reiterated what skills are needed in gathering information from human sources, including: knowing how to observe (looking carefully at people and the environment to identify possible indicators of danger); knowing how to stimulate a conversation to obtain information (elicitation); and

---

3 *Arthaśāstra* whose meaning in Sanskrit is "code of power," is a work of balance, wisdom and political and military strategy on how to gain power and how to maintain it. Written more than twenty-four centuries ago, the document was unearthed only in the early 20th century A.D. Kautilya, the author of this important work, is considered the Aristotle and the Hindū Macchiavelli: "At the time of the strategic confrontation between the United States and the Soviet Union, someone said that Macchiavelli and Metternich would not have served Henry Kissinger well if the stainless dean of the Soviet Foreign Ministry Andrej Gromyko had read *The Code of Power*. Max Weber and Indian Prime Minister Jawaharlal Nehru, for whom Machiavelli's *The Prince* is inoffensive compared to this jewel of pure rationality, would certainly have agreed. " See Magi Gianluca (a cura), Kautilya, *Il codice del potere. L'arte della guerra e della strategia indiana*, Edizione Il Punto d'Incontro, Vicenza, 2011, p. 8.

knowing how to keep watch (keeping an eye on someone or something).

In this regard, however, it is necessary to make a brief distinction between the human intelligence information activity of institutional intelligence (Humint) and that of police intelligence (Police Humint), precisely to avoid uncertainty regarding their functions and purposes.

The *Institutional Humint* consists of the research, collection and processing of news regarding security and national interest from physical persons[4]. NATO defines Humint as "a category of intelligence derived from information collected and provided by human sources."

The *Police Humint,* on the other hand, is primarily concerned with finding all possible information and sources of evidence on criminally relevant facts. It consists of that information flow that includes reports from confidants, informants and the police officers themselves, spontaneous statements on facts and people of ordinary people, surveillance activities, reports and minutes of security activities.

Although some sectors of the Police forces are particularly versed and experienced in OES practice (just think of those who carry out investigative work, territorial control, street patrols, surveillance, and escorts), potentially being

4 In Intelligence management, information research involves different systems with reference to the source including: Humint (Human Intelligence, for news from physical persons); Masint (Measurement and Signature Intelligence, for metric, angular, spatial, wavelength, etc. data of events and targets of information interest); Osint (Open Source Intelligence, for information drawn from open sources); Sigint (Signals Intelligence, for signals and/or electromagnetic emissions from abroad); Geoint (Geospatial Intelligence, for georeferenced data and images). See Table 2.2 - A.

able to have more law enforcement personnel with similar skills, thanks to specific training that provides all the necessary elements for this purpose, would greatly increase the likelihood of gathering useful intelligence to maximize the tactical efficiency of an operation or even improve the strategic one, as the American experience has shown.

When we refer to elicitation, on the other hand, the matter is somewhat more complex, precisely because the agent's personal skills no longer operate in two distinct and distant spheres, where on the one hand there is the one who acts as a spectator/detector (the passive party), and on the other who or what is part of the event (the active party), but they operate in a context where the two spheres of action overlap. In this case, therefore, in order to establish contact with the subject from whom information is to be gathered, it will be necessary for the agent to be equipped not only with good interpersonal and communication skills but also with basic notions of psychology.

In fact, the term eliciting is used particularly in the field of psychology in reference to the behaviours or conduct that are useful in discreetly obtaining information through questions or other stimuli. This is a technique of such importance that it is being used not only in the world of intelligence, but increasingly in the private sector as well. A medium, then, for gathering news or data without declaring one's intentions with the aim of extracting sensitive information from an interlocutor who is reluctant to reveal it, by exploiting a seemingly normal conversation.

In contrast to the first two techniques (observation and surveillance), elicitation remains a difficult activity to practice,

so much so that it is not recommended for those who do not have those characteristics mentioned above, particularly if it involves approaching individuals about whom one has no knowledge[5].

Therefore, the member of the Police forces remains an indispensable and qualified source in acquiring environment news sourced from the local people (e.g., merchants, professionals, acquaintances, friends, etc.).

5 In this regard, it will be useful to refer to practical investigative experience, addressed in the next chapter.

Tabella 2.2 – A

<table>
<tr><th colspan="4">INTELLIGENCE MANAGEMENT</th></tr>
<tr><td rowspan="5">Collection</td><td rowspan="3">Human Intelligence HUMINT</td><td colspan="2">Special reconnaissance (organizations)</td></tr>
<tr><td>Clandestine</td><td>Asset recruiting • Cell system • Covert action • Direct action • Operational techniques</td></tr>
<tr><td>Espionage</td><td>Agents (field • handlingAsset) • Black operation (black bag) • Concealment device • Cryptography • Cutout • Dead drop • Denial and deception • Eavesdropping • False flag • Industrial espionage • Interrogation • Numbers station • Official cover (Non-official) • One-way voice link • Resident spy • Steganography • Surveillance</td></tr>
<tr><td>Signals (SIGINT)</td><td colspan="2">By alliances, nations and industries • In modern history • Operational platforms by nation • Direction finding • Traffic analysis • TEMPEST</td></tr>
<tr><td>Measurement and signature (MASINT)</td><td colspan="2">Electro-optical • Geophysical • Nuclear • Radar • Radiofrequency • Materials • Casualty estimation (earthquake)</td></tr>
<tr><td>Other</td><td colspan="2">Cultural (CULTINT) • Financial (FININT) • Geospatial (GEOINT) • Imagery (IMINT) • Market (MARKINT) • Open-source (OSINT) • Technical (TECHINT)</td></tr>
<tr><td>Analysis</td><td colspan="3">Cognitive traps • Competing hypotheses • Target-centric • Words of estimative probability • All-source intelligence • Basic intelligence • Intelligence assessment • Medical intelligence • Military geography • Scientific & Technical intelligence</td></tr>
<tr><td>Dissemination</td><td colspan="3">Intelligence cycle security • Counterintelligence (organizations) • Counterintelligence and counter-terrorism organizations</td></tr>
</table>

2.3
The Police forces in Italy

Italy is the third-largest state in the world, after Russia and Turkey, in terms of the number of Police forces in relation to population[1] (467.2 officers on duty per 100,000 inhabitants) and it remains the only country to have four nationwide law enforcement agencies (Polizia di Stato, Carabinieri, Guardia di Finanza and Polizia Penitenziaria), of which two with general competencies and two with specific competencies.

Each corps naturally has its own commands, its own operational centres, its own barracks, its own generals defending its power status. This entails, in addition to the enormous expense and overlapping of subjects and competencies among the different forces, a greater obstacle to the adoption of an *Intelligence-led policy* system based on information centralization, which would be necessary for a more effective analysis of the data collected by all armed and Police forces (except for the C.A.S.A.).

1 According to the UNODC (United Nations Office on Drugs and Crime) 2013 annual report, (data taken from other organizations such as Eurostat) Russia is the most militarized country in the world with 564.6 officers per 100,000 population, while Turkey ranks second with 474.8 police officers (the statistic refers to nations with a population over 50 million). Although the number of police officers in the European Union has been slowly decreasing in recent years, (between 2009 and 2016 the EU experienced a continuous decrease in the number of officers on the ground, with a reduction of 3.4 percent), Italy remains by far the most militarized country in the EU even in 2015 with 453 officers per 100,000 inhabitants (however, the Eurostat statistical analysis does not take into account the difference in population between the different states placing it in sixth place after countries that do not have a population over 11 million). Cf. Statistics published by the European Commission, *1.6 million police officers in the EU*, in "Eurostat," Eurostat News, Product code: ddn-20190104-1, published on 04 - Jan-2019.

Putting aside this aspect, which in any case remains central to any Intelligence activity one wishes to carry out (here intended as a method of acquiring information)[2], would it perhaps be possible to use the numerous agents of the Police forces, already available and well distributed throughout the territory, to monitor, detect, and acquire information useful for National Security (terrorist activities, activities that are subversive to the democratic order) and for countering organized crime (with reference to indirect issues concerning National Security) as if they were many sensors?

This is not, of course, a matter of reiterating prerogatives, obligations, duties and *modus operandi* to which members of the Police forces already refer (activities which are distinct and different from those of Institutional Intelligence), but of better equipping the former, by means of *ad hoc* training, with the ability to observe, elicit and watch the territory and people, which often not all police officers possess[3].

In fact, more than half of the members of the Police forces are mainly involved in bureaucratic or functional activities within their organization, while only a small percentage regularly carries out investigative work or territorial control, which are activities that can prepare and train the police officer to pick up and decipher those signals coming from the surrounding environment.

> "Sixty percent of the men in uniform, from Cuneo to Caltanissetta, work in the technical-logistics apparatus. An army of white-collar, secretaries and clerks: [each Police

2 See Table 2.3 – A.

3 "Sixty percent of uniforms are not assigned to the security of citizens, but work in offices and guard stations and commands scattered throughout our regions." Statements by the Sap (Autonomous Police Union) in 2015, later echoed by several news outlets.

> forces] in fact has its own operations centres, its own barracks, its offices for uniforms, the one for salaries, its fleet of vehicles, its apparatus and its training schools. A plethoric duplication that reaches, in Florence, its apex: the 7,000 operators in the city refer to 11 different headquarters, while around the Arno there are four canteens named after the police, two in which only Carabinieri can eat, one assigned to the firefighters and another reserved for the municipal police. In Florence some commands are only a few meters apart, but even in Rome and Milan the overlaps are resounding: near the Duomo there are about thirty police stations, barracks of the Arma, [...], public security departments and police headquarters offices. [...]. A waste of resources that matches the waste of men engaged in the surveillance of too many rented properties: if all the offices were merged into single police headquarters we would have as many as 150 more policemen available for security activities in the Catanese territory. At present in Italy there are 1,850 command centres of the Polizia di Stato, 6,140 of the Carabinieri (including more than 4,000 stations), as well as some 20 central directorates, to which must be added the Finance detachments. An enormity [...]"[4].

Of course, one can hardly think of eliminating bureaucratic activity to send more Police forces on the road as repeatedly stated by improvised politicians. And the reasons why this is impossible to do are essentially two: the first lies in the fact that most of the bureaucratic activities, being related to police activities, contain by their nature professional or office secrets, or classified information[5] that prevents their know-

4 In the weekly journalistic investigation of Espresso (2015), it is revealed, in addition to some aspects related to the waste of economic resources and overlapping activities of the Police Forces, how personnel are employed. Cf. Fittipaldi Emiliano, *Troppo Divise*, in "L'Espresso," No. 2, year LXI, Jan. 15, 2015, pp. 30 - 37.

5 Every public employee is obliged by law not to disclose secrets concer-

ledge to anyone other than those belonging to that Police forces. Thus, the possibility that some of the bureaucratic activity may be carried out by civilian employees, useful in relieving the military of such duties, may concern only those administrative and accounting areas for which such employment is possible; the second reason, however, lies in the fact that contrary to what one might think it is precisely the bureaucratic activity that represents the real backbone of the state and the one that really holds the power (the so-called *Deep State*)[6] and which, despite some attempts at rationalization, is impossible even to reduce. In fact, as it has been proven by a keen scholar of human organizational systems, Northcote Parkinson: any bureaucratic organization, by the mere fact of its existence, tends to grow annually at a rate of no less than 5 percent, and will continue to expand even in the event that it has nothing to do[7].

Taking into account what has been said, it is possible to consider that if one were to supplement the training of members of the Police forces (every year there is a professional refresher training activity for the Police forces., both in the legal-administrative and in the technical-operational spheres)[8]

---

ning his or her profession (Disclosure of Professional Secrets, Art. 622 P.C.) or office (Disclosure and Use of Official Secrets, Art. 326 P.C.), and to ensure the protection of personal data and privacy. In addition, access to classified police documents is allowed only to those who by function or office have the authority or right to know it.

6 Under the term *Deep State* we mean that set of organizations of the state (military, economic, bureaucratic apparatuses, etc.), which are capable of influencing or weighing their will in political decisions; "in front of every room of direct power there forms a kind of antechamber of indirect influences and controls, an entrance towards the ear of the powerful, a corridor towards his soul. There is no power without this antechamber and without this corridor." Cf. Schmitt, Carl, *Dialogo sul potere*, Il Melangolo, Genova, 1990.

7 Cf. Parkinson Cyril North, *Parkinson's Law*, Monti & Ambrosini, Pescara, 2011. Cf. also, Aprile Pino, *Elogio dell'imbecille. Gli intelligenti hanno fatto il mondo, gli stupidi ci vivono alla grande*, Ed. Piemme, Milan, 2012. pp. 106-109.

8 For example, for the Polizia di Stato, six days of professional refresher trai-

with activities aimed at improving those aspects of OES that are useful for intercepting the so-called weak signals[9], one would possess a huge amount of "human sensors on the ground"; the Human Sensors precisely who would be active not only during working hours, but especially when off duty[10]. The implementation of such a system, aimed at predicting as far in advance as possible the development of dangerous situations on the ground, would significantly decrease the effectiveness of any threats to Public Order and Public Safety, and would, above all, allow for an increase in the ability of decision-making systems to provide immediate and effective responses.

In this regard, some initiatives that were taken by the ministers of the Interior (who succeeded each other between 2016 and 2018) and by the chief of police himself following the tragic terrorist events that struck several European cities should be considered interesting.

A few days after the 2016 terrorist attack in Nice, for example, a circular from the head of the Viminal that was sent to prefects and quaestors called on "all officers to carry their service weapon even outside specific assignments and service hours, urging vigilance at all times." A similar initiative

---

ning (in which interdisciplinary lectures are given by Polizia di Stato officers or experts from within or outside the administration), three of operational techniques and three of shooting training, are scheduled annually. In some regions, for example, the Sisfor system (law enforcement online training system) is being piloted to train personnel in theoretical activities.

9 Surveillance is not simply about peering at a radar screen, but about taking a proactive view of the evolving environment. Embedded in this conception is the idea of relative Intelligence - understanding and acting before the other - and the central importance of communication - weak signals are primarily a pretext for building a common vision and being collectively alert. Cf. Ansoff Igor H., *Le risposte strategiche ai "segnali deboli"*, in «Sviluppo e organizzazione», fasc. 33, 1976.

10 It is useful to recall that numerous and of all kinds are the examples that have seen various members of the Police forces intervene in dangerous situations off duty.

was taken the following year following the extraordinary summit of the Strategic Counterterrorism Analysis Committee convened by Home Department Marco Minniti, to decide what measures to put in place after the 2017 Barcelona attack. From the meeting, which was attended by the national leadership of the Police forces and Intelligence Services, it was reiterated the need for all police officers to carry their service weapon at all times, even when not on duty.

The 2016 Berlin bombing, on the other hand, had already laid the groundwork for a new counterterrorism doctrine, dubbed by then newly appointed Minister Minniti as "collaborative prevention," which somehow extended to non-police personnel, such as local administrators, mayors, and municipal police corps of cities, joined by quaestors and prefects, certain terrorism prevention tasks, so as to "make effective and widespread those forms of active vigilance and passive defence of urban areas in the face of the lone wolf threat"[11].

Thus, relying on the large number of members of the Police forces, on their widespread distribution throughout the territory, and on them being already militarily trained men and women (basic training), it could be assumed with good reason that statistically these *Human Sensors* could greatly increase the *chances* of both Institutional Intelligence and Police Intelligence in acquiring useful information concerning Homeland Security and organized crime.

11 Bonini Carlo, *Terrorismo, il nuovo schema di Minniti: "Sindaci e polizia locale ci aiuteranno a fermare i lupi solitari"*, in «Repubblica», 22 dicembre 2016.

Table 2.3 A

PLANNING E DIRECTION
COLLECTION
PROCESSING
ANALYSIS
DISSEMINATION
EVALUATION
INTELLIGENCE
CYCLE

2.4
Off-duty Police activity

Although the idea of being able to have a huge "army" of *Human Sensors* scattered all over the territory for the acquisition of environmental information may raise some doubts about its actual implementation and effectiveness (how to implement such a training program, in what system to collect the information activity coming from Police forces operators, who and how should manage the data analysis, how much such a program would cost), there is one question that stands out above all others: why should a member of the Police forces have any interest in performing his or her work even off duty?

First of all, it is worth mentioning that in the history of the Police forces and in the chronicles, there are plenty of examples of off-duty officers (in the performance of their duties) who have intervened in extremely dangerous situations, risking their own safety to save that of other people[1]. Fortunately, not all activities performed outside working hours occur in such dramatic ways. However, most of these situations, precisely because of the innumerable scenarios that could occur, are handled predominantly in two ways: either by im-

1 If all the data regarding the profile of Police forces members who have operated off-duty (police background, training, knowledge, experience, etc.) could be available, it would be possible to analyse the common and repetitive characteristics that become crucial in such contexts.

mediate action, aimed at preventing the commission of a crime, in providing public relief, and so on; or by deferred action, by giving information to one's command centres regarding places, people, and facts concerning criminal or potentially criminal activities.

While acknowledging the de facto existence of off-duty policing, albeit mainly limited to dangerous situations, the question remains whether all police officers do so or whether they show up, as alleged here, doing OES activities.

In order to better address the question just posed, it is necessary to evaluate two additional aspects concerning the activity of law enforcement officers in such a context: the legal obligation to intervene when there is a criminal offense (particularly when there is ex officio prosecution) and financial compensation for the activity performed. The former concerns certain legal provisions that in fact oblige members of the Police forces to observe the duties inherent to their function even when off duty[2]. The latter, on the other hand, relates to some purely economic-administrative issues involving the recognition of police officers working off-duty with remunerative compensation in overtime, which by custom the personnel never request[3].

---

2 Officers and agents of the judicial police (c.p.p. art. 57), or as in the case of members of the Polizia di Stato, having contracted a legal obligation with the State, in the present case with reference to the public security system, are required to observe the duties inherent in their function even outside working hours (art. 68 of Law No. 121 of 01.04.81) and are therefore to be considered on permanent duty even during periods of leave and furlough. See also art. 55, 330 and 347 of the Code of Criminal Procedure.

3 The overtime allowance for police officers is divided by bands with reference to rank, but it does not represent a particularly attractive amount.

Just in reference to the last of these aspects, one might wonder whether different choices (e.g., greater reward incentives) might incentivize out-of-service OES activity[4].

In any case, this is not the central argument as to why a police officer should carry out off-duty OES activities: rather, it is the psychological aspects (with reference to altruistic and prosocial human conduct) and the statistical aspects (with reference to a significant number of Police forces in the country that if properly trained could implement such an activity) that determine the success of such a project (Human Sensors).

4 A given human behaviour occurs the more often a reward is associated with it. In this regard see the basic principle of Thorndike's learning theory: *the law of effect* (a response that defines a pleasant effect tends to repeat itself, conversely an unpleasant effect causes the response not to be repeated); And *the law of exercise* (learning is gradual and improves with repetition of trials, and the more often a response is repeated, the more likely it becomes).

2.5
IMPLEMENTATION OF THE *OES* MODEL IN THE ACTIVITY OF *HUMAN SENSORS*: A MATTER OF SOCIAL PSYCHOLOGY AND STATISTICS

What are the reasons why a subject, in our case a member of the Police forces, is inclined to behave altruistically off duty?

To be able to answer this question, we need to look beyond the "mechanistic" aspects related to the existence of a legal norm that imposes a certain behaviour on the subject and look to social psychology and sociobiology for the deeper elements for understanding this human characteristic.

According to authoritative scholars, it is *motivations* that drive a person to behave in a *prosocial* or *altruistic* manner.

The prosocial conduct, i.e., those behaviours that aim to bring relief or help to others, cannot necessarily be called altruistic, precisely because the motivations that drive a person to engage in such behaviours could be determined by the expectation of gaining an advantage.

Even when it comes to altruism, things are not very different from what is commonly thought. If we consider altruism in the light of some aspects of Charles Darwin's evolutionary theory, such as natural selection and the individual's struggle for survival, there seems to be complete contradiction with that principle. The British scientist was never able to explain this contradiction, so much so that he himself doubted the soundness of his theory, simply because he started from an erroneous postulate that did not distinguish between species that

have elaborated social structures and species that have not.

> In social species, the competitive advantage for the transmission of one's chromosome set does not depend solely on the individual but is related to the survival of the family unit, group, or entire herd[1].

Looking at the issue from another perspective, then, we see how selection no longer occurs with reference to the individual, but to the social system, and that most sympathetic attitudes are not generated by love of neighbour, but rather, as sociobiology explains, by some form of self-interest.

In Scottish ecologist Vero Copner Wynne-Edwards's theory of group selection, for example, it is argued that individuals who are willing to sacrifice themselves for the survival of the species are less likely to go extinct than a rival group whose members put their own self-interest first[2].

A more convincing perspective was later provided by William Hamilton with the concept of *parental selection*[3] [1964], which was later supplemented by the *selfish gene* theory of evolutionary biologist Richard Dawkins[4] [1976], who explai-

---

1 Cfr. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, Il Mulino, Bologna, 2010, p. 249.

2 Wynne-Edwards V. C., *Animal dispersion in relation to social behaviour*, Oliver and Boyd, Edinburgh, 1962.

3 For both humans and animals, altruistic behaviour toward offspring, grandchildren, cousins occurs because doing so increases the probability of survival of one's genes or a genetic set that contains much of one's DNA anyway. In this way, evolution does not promote the reproductive success of the individual but that of the gene. See Boca S., Bocchiaro P., Scaffidi Abbate C., I*ntroduzione alla psicologia sociale,* op. cit. p. 250.

4 In his famous book, the scholar reduces all evolutionary dynamics to a competition between genes, dismissing the question of altruistic and cooperati-

ned that altruistic behaviours, even those that appear to perform a pure act of love, are determined by one's genes to perpetuate oneself[5].

However, it is down to biologist Robert Trivers' [1971] theory of *reciprocal altruism* to explain why individuals behave altruistically even toward nonconsanguineous members. This theory is based on the concept of exchange (I do a favour for you because I expect you to do one for me): ultimately, an individual enacts an altruistic behaviour toward a stranger if the potential benefits of the action outweigh the cost[6].

From an evolutionary perspective, then, altruism represents a mechanism by which individuals and social groups increase the likelihood that their genes will survive and they cooperate to maximize the individual benefits that can be derived in the future.

Some researchers conducted experiments to define the neural area of reciprocal altruism by recording the strongest signals in the presence of alliances and mutual cooperation in the same brain areas that respond positively to an indefini-

---

ve behaviours existing in nature by arguing how they are nothing more than a subtle form of disguised selfishness, in which those who behave altruistically actually do so to favour their closest relatives (who share a good percentage of the same genes) or with a view to some other advantage or benefit for themselves. Cf. Dawkins Richard, *Il gene egoista. La parte immortale di ogni essere vivente*, Arnoldo Mondadori Editore, Milano, 2011.

5 A mother who jumps into the fire to save a child in danger does so imagining that she is performing a genuine act of love but, in reality, in her this type of behaviour is programmed at the genetic level and a categorical imperative is encoded in her DNA: do whatever it takes, even at the cost of your own life, to ensure and safeguard the transmission of your chromosomes. S. Boca, P. Bocchiaro, C. Scaffidi Abbate, *Introduzione alla psicologia sociale*, *op. cit*., p. 250.

6 Cf. Hauser Marc D., *Menti Morali. Le origini naturali del bene e del male*, Il Saggiatore, Milan, 2007, pp. 252 – 253.

te number of pleasures[7]. Thus, the instinct for cooperation, leading to a pleasant feeling of well-being, further reinforces altruistic behaviours.

Although the various sociobiological hypotheses consider altruism from the perspective of genetics, it is also necessary to examine those studies that consider the issue in relation to *cultural selection*, reading altruism as a social value and norm to be internalized through learning.

The main assumption of a theoretical model referring to cultural selection highlights how individuals, by living within a society and developing a sense of belonging to social groups that are meaningful to them, are influenced by the values and norms they share with other members of the group.

Often, simplistically, one is led to believe that a person is altruistic or selfish, courageous or fearful, depending on his or her attitude in relation to the same action, but this judgment does not help to explain the deeper aspects of such behaviours. For social psychologists, however, the question must be put in other terms in order to be understood. And to do so, one must start with a question: when do people help?

In the 1970s, a *staged model of intervention*[8] was developed that could answer this question. Before an individual engages in helping behaviours in an emergency situation, five distinct conditions must occur:

---

7 Rilling J., Gutman D., Zeh T., Pagnoni G., Berns G., Kilts C., *A neural basis for social cooperation,* in «National Center for Biotechnology Information, U.S. National Library of Medicine», Atlanta, 2002.

8 Cf. Boca S., Bocchiaro P., Scaffidi Abbate C., I*ntroduzione alla psicologia sociale, op. cit.,* pp. 255 – 257.

1. noticing the event
2. interpreting the event as an emergency
3. taking responsibility
4. knowing what to do
5. deciding to intervene

Of course, it is essential for the subject to notice what is happening. Often trivial circumstances such as being in a hurry can prevent the perception of alarm[9]. In addition to noticing the emergency condition, it is necessary for the subject to interpret it as such. In some contexts, for example, the individual may not immediately notice the emergency situation, and to overcome this condition of uncertainty and confusion he or she tends to rely on what other people present are doing.

However, realizing that one is in an emergency situation is not enough to make the individual decide to intervene, but an additional step is needed: taking responsibility.

Studies undertaken in this regard have disturbingly shown how willingness to help decreases in dangerous situations as the number of people present increases[10], ascertaining that the number of witnesses generates a split-responsibility effect in the participants, where each one thinks and hopes that it will be the other who will intervene[11].

Finally, a condition of fundamental importance in order to

---

9 Compare in this regard a famous study from 1973 called the "Good Samaritan," by Darley and Batson.

10 We refer to the 1964 Kitty Genovese tragedy. The young American woman was attacked and killed in the street in front of about 40 people who despite the screams and violence did not intervene to help. Cf. Bocchiaro Pietro, *Psicologia del male*, Editori Laterza, Bari, 2010, pp. 47 – 67.

11 This social behaviour is known as "diffusion of responsibility." Ivi, p. 55.

intervene in dangerous or emergency situations, is to know what to do. Lack of knowledge, skills, and experience puts the subject in a condition of blindness, inadequacy and fear in the face of danger, precisely because he or she is unable to foresee what possible scenarios might unfold. Having knowledge of the situation and knowing how to handle it are crucial in making a person decide to intervene or not, prerequisites without which adequate help cannot be offered.

While the above stadial model may be considered valid, it does not exhaustively represent all the different situations that may arise. For example, there are circumstances in which subjects, despite being aware of the victim's need for help and being called to their responsibilities, prefer not to meddle so as not to risk it. To clarify these situations, another theoretical model, experimentally verified, has been developed that explains in cost-benefit terms what factors come into play.

In the theory of *social exchange*, human interactions are guided by a kind of social economy whereby individuals exchange not only material goods, but also social goods such as love, assistance, information, status, aiming, as is the case in economics (according to the "minimax" theory of Hungarian mathematician John von Neumann), for maximum pleasure with minimum cost. According to this principle, individuals act rationally and in their own interest by evaluating in terms of advantage and disadvantage the decision to help or not to help.

Even in the case of altruism, therefore, humans think in terms of costs and benefits. Reasoning in terms of reciprocity, for example, it may be cost-effective to lend one's help because the favour is expected to be returned in the future. So-

cial approval, and consequently the elevation of self-esteem, which in this way generates a feeling of well-being, is also a condition that promotes altruistic behaviour.

Ultimately, it is possible to say that benefit maximization, as mentioned above, is not only concerned with the sphere of material goods, but also, and perhaps especially, with that of social goods such as self-esteem, esteem, love, approval or gratitude[12].

While the considerations made so far are valid and important in helping us understand the breadth of psychological mechanisms and motivations that can lead a subject to behave altruistically, it is also necessary to highlight those conditions that do not take into account the cost-benefit decision-making model. One of these is the *perception of similarity*[13].

In fact, it has been shown that people are all the more willing to help others the more they are perceived as being similar to themselves. The main reason lies precisely in the perception of similarity, which increases the attraction between individuals, thus increasing the willingness to help.

This short path that has been taken in the field of social psychology and sociobiology explains what are the behavioural mechanisms by which an individual can decide to engage in an activity seemingly without benefits, thus clarifying those aspects that have led to doubts about the possibility that a member of the Police forces could in a deliberate and participatory way (if put in the condition of knowing what to do and

12 In this regard, it would also be useful to investigate those aspects concerning the guilt generated by non-intervention in emergency situations and its effects on the psyche on the human behaviour necessary to restore one's self-image. Cf. Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale, op. cit*., p. 254.

13 Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale, op. cit.*, p. 259.

how to perform the role of Human Sensor) start such an activity off duty regardless of his legal obligations.

Equipping members of the Police forces with an OES model that is useful in the activity of Human Sensor simply means having, or arranging for, personnel who are already qualified and scattered throughout the territory and ready to act autonomously when circumstances require it for the purpose of gathering contextual information.

The idea of using all Police forces indiscriminately to implement a broader information collection is based primarily on the likelihood with which a police officer, if trained in OES activity, can help to significantly increase the *chances* of gathering information useful for Intelligence activity or preventing emergency situations from becoming a danger to National Security or Public Safety.

For this purpose, we will use a small example to refer to those statistical aspects mentioned above, starting, however, with a question: How much would the administration of a training or instructional course for OES capacity building to all Police forces personnel affect information gathering?

In order to answer this question, it is necessary to start with some premises.

Let us consider, as the target population for this analysis (see Table 2.5 - A), the set of Police forces "Pf", of which 40 percent practice mainly investigative and preventive activities (preparatory to information activity) which we will call "If", while the remaining 60 percent practice exclusively technical

- bureaucratic activities (with a modest information gathering capacity) which we will call "Tf"[14].

Table 2.5 - A

Police forces →	*Pf*	40 %	Police officers who mainly carry out investigative, preventive and territorial control activities	→	*If*
		60 %	Police officers who mainly carry out technical - bureaucratic activities	→	*Tf*

We introduce the parameter ICI (Investigative Capability Index) to express the ability to collect useful information in Intelligence activity with a range between 0 and 1, where 0 is the null value and 1 is the maximum value (so all intermediate values will be considered: 0.1; 0.2; ..., 0.5; etc.).

Let us assume (see Tab. 2.5 - B) that Investigative Forces (*If*) have an ICI of 0.6 - 0.7, while Technical - Bureaucratic Forces (*Tf*) have one of 0.2 - 0.25[15].

Table 2.5 – B

Pf	Capacity to collect information from 0 → 1	
If	0,6	0,7
Tf	0,2	0,25

14 This indication refers to statements by the police union Sap (see § 2.3) regarding the percentages of Polizia di Stato personnel employed in investigative and technical-bureaucratic activities. It is possible to assume with good reason that the other law enforcement. also tend to have lower numbers of personnel employed in investigative activities.

15 The hypothesis refers to average percentage data collected from questionnaires administered to Police forces investigators (see § 3.2).

At this point, it is necessary to assess how much a formation or training course can have an impact in improving those skills needed by each police officer (in OES activities), in order to implement information gathering capabilities.

A number of studies by John Barron (1987) and John Bishop (1994) have examined a close correlation between training and productivity, establishing what impact professional upgrading of human capital determines on increases in labour productivity[1]. Barron, for example, points out that the productivity index following training leads to substantial productivity growth: "a 10 percent increase in training increases productivity by 2 percent during the first three months of employment."[2]. According to Bishop, however, the magnitude of the spillover benefit[3] in the first three months is estimated to be around 16 percent of productivity net of training costs[4].

Several Italian and European economic reports also point to the positive effect of vocational training in business productivity[5].

---

1 Black Sandra E., Lynch Lisa M., *Human - Capital Investments and Productivity,* in «The American Economic Review», Vol. 86, No. 2, Papers and Proceedings of the Hundredth and Eighth Annual Meeting of the American Economic Association San Francisco, CA, January 5-7, 1996 (May, 1996), pp. 263-267

2 Barron John M., Berger Mark C., Black Dan A., *On-the-Job Training*, W.E. Upjohn Institute for Employment Research, Kalamazoo, Michigan, 1997, p. 185.

3 In Italian "overflow," the "situation in which a public expenditure, incurred to produce benefits for the residents of a territorial or administrative sphere, also generates benefits outside that sphere. See VV.AA., *Enciclopedia dell'Economia Garzanti,* Garzanti Editori, Cernusco, 1997, p. 1120.

4 Lynch Lisa M., *Training and the Private Sector,* University of Chicago Press, 1994. Cf. Chapter 6 by John Bishop, *The Impact of Previous Training on Productivity and Wages,* pp. 161 – 200.

5 «In fact, it is estimated that for every hour of training per employee, the corresponding revenues increase by more than one euro». See Isfol (Istituto per lo sviluppo della formazione professionale dei lavoratori), *XVI Rapporto sulla*

However, like other intangible activities, the possibility of establishing a value of the impact of a training course on productivity in an unambiguous way is not easy to determine because it is dependent on many variables, such as the manner in which refresher courses are administered, the quality of the training, whether the training activity is carried out with internal or external[6] resources to the company, the per capita hours of training, the background and education of each worker, and so on.

Let us assume that a well-structured training course, for the purpose of improving the OES capabilities of each operator in high-value information collection, would affect the ICI by only 10% more than the previous value, a much lower percentage than those found in the various studies[7]. In this case, the 60 percent of Police forces that do not conduct preparatory activities for information collection would increase their total information collection capacity by 0.275 percent, leading to a total increase in Information Capabilities (IC) of 1 percent more.

Formazione continua Annualità 2014 – 2015, commissionato dal Ministero del Lavoro e delle politiche sociali (Direzione generale per le politiche attive, i servizi per il lavoro e la formazione), dicembre 2015, pp. 27 – 28.

6 Some studies have shown a different impact of training courses on productivity depending on whether the training is carried out in-house with its own experienced staff or outside. In the second case, there is a significant increase.

7 Bartel, for example, points out that those companies that implemented new training programs for specific groups of employees experience significant productivity gains (by an average of 19 percent). Cf. Bartel, P. Ann, *Productivity gains from the implementation of employee training programs*. Industrial Relations, Vol. 33(4), 1994, pp. 411-425. Cf. also, de Kok Jan M.P., *The Impact of Firm - provided training on production: testing for firm - size effects, Tinbergen Institute Discussion Paper,* Netherlands, 2000, p. 5.

Table 2.5 - C

Police forces Pf numerical %	(ICI) Index of Collection Capacity of information 0 to 1 (mean value)	Total value of (IC) Information Capacity before a training course %	Hypothetical % increase in ICI after a training course	Partial increase in ICI	Overall value of ICI after training course	Total value of (IC) Information Capacity after a training course %
If 40%	0,7	28	10%	0,07	0,77	31
			15%	0,105	0,80	32
			20%	0,14	0,84	34
Tf 60%	0,25	15	10%	0,025	0,275	16
			15%	0,0375	0,288	17
			20%	0,05	0,30	18

In this regard, it has been evaluated a different impact of training courses whether aimed at skilled or unskilled personnel. In fact, in 2008, a study was conducted that analysed the effects of training on labour productivity using a homogeneous and representative group of companies and showing that within professional groups the effect of training on productivity is larger and more significant for "blue collars" than for "white collars"[8]. This evidence could be useful in assessing more carefully the usefulness that a refresher course would have on members of the Police forces who do not normally carry out informational activities.

So, by assessing a greater impact for those police officers who do not regularly carry out investigative or preventive work, it is possible to consider a greater impact on the increase in IC (see Table 2.5 - D).

8 Colombo Emilio, *Stanca Luca, The Impact of Training on Productivity: Evidence from a Large Panel of Firms,* Working Papers from University of Milano – Bicocca, No 134, Department of Economics, Milano, 2008, p. 1

Table 2.5 - D

Police forces Pf numerical %	(ICI) Index of Collection Capacity of information 0 to 1 (mean value)	Total value of (IC) Information Capacity before a training course %	Hypothetical % increase in ICI after a training course		Partial increase in ICI		Overall value of ICI after training course		Total value of (IC) Information capacity after a training course %	
If 40%	0,7	28	10%		0,07		0,77		31	
			15%		0,105		0,80		32	
			20%		0,14		0,84		34	
Tf 60%	0,25	15	10%	20%	0,025	0,05	0,275	0,30	16	18
			15%	25%	0,0375	0,063	0,288	0,54	17	32,4
			20%	30%	0,05	0,075	0,30	0,55	18	33

In view of the considerations above, it is possible to believe that widespread training or upgrading of the Police forces would appreciably improve environmental information gathering by increasing the Intelligence's *chances* of intercepting those notorious weak signals that are increasingly difficult to pick up.

But how much would it cost the state to activate such a program? According to some estimates, the cost of a refresher course for a corporate employee averages around 50 euros. However, it should be considered, as mentioned above, that the Police forces already have in their budgets the cost for the refresher training they are required to attend annually. Therefore, it would mainly be a matter of setting up a training/educational program and a teaching staff experien-

ced in OES activities.

If we consider the dramatic terrorist events that have hit different cities around the world since 2001 and the interconnections that increasingly see terrorism, organized crime and corruption acting together[9], then perhaps we need to ask ourselves whether Human Sensor in police Intelligence should not be considered a useful tool for contextual information gathering.

9 Maronta Fabrizio, Caracciolo Lucio, *Criminalità e terrorismo sono due facce della stessa medaglia. Conversazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa),* in *«Limes», n° 11*, dicembre 2015.

Chapter 3
The Human Sensor in the activity of Police Intelligence

3.1
Police intelligence and National Security

As mentioned, the *police Intelligence* is the activity by which law enforcement agencies, collect, analyse and disseminate information, directing it to different levels of expertise according to its nature.

This is an information process in which Intelligence activity can both relate to the prevention and suppression of crime (increasingly this is being done through the use of powerful software and technologically advanced devices that can catalogue, aggregate and process an infinity of data and information)[1], and both bring into being and sustain an investigative process. To this end, there are two main pillars on which the effectiveness of any Intelligence activity rests: good information gathering and excellent analytical skills[2]. The lack

1 Being able to have powerful, technologically advanced systems, such as the one in use at the Carabinieri General Command (SI.CO.TE. - *Territorial Control System,* a program included among those of specific relevance to defence and National Security) to elaborate and process structured and unstructured, internal and external data with heterogeneous formats, makes it possible to ensure a higher level of support for general prevention and territorial control activities. This system has made it possible to expand the analytical and operational capabilities of departments dedicated to intelligence activities and countering terrorism and organized crime.

2 Needless to say, the other elements of the Intelligence cycle are also indispensable in order to obtain information that is useful to the decision maker: setting an unnecessary information goal leads to distracting resources and valuable time from activities that would be more important instead; the lack of a system capable of processing the enormous amount of data available would have definite consequences for the timeliness and accuracy of the analysis; and the absence of properly organized archives would limit research capabilities.

or weakness of either of these two moments greatly affects the intended knowledge and prediction results.

Although the Police forces have tasks and functions that are distinct from those of the Security Information Services, the geopolitical, social, technological, economic, and military upheavals of recent decades have brought - are bringing - these two worlds to an increasing convergence.

Until 1991, collaboration between Police forces and Intelligence agencies in Italy was, at least officially, predominantly concerned with crimes against the state (subversive propaganda, terrorist activities and subversion of the democratic order, and so on) of a political or criminal matrix (right-wing extremists, left-wing extremists and organized crime). Just think of the terrorist activity and massacres that have bloodied the country since World War II, beginning with the massacre at Portella della Ginestra in 1947.

As a consequence of the "Years of Lead," which were characterized by an extremization of political dialectics and an upsurge of street clashes to the point of armed and terrorist struggle, Italy was provided with innovative and cutting-edge legislation[3] in the fight against terrorism In this context it was necessary both to give the Police forces greater powers and to clarify what the position of the Intelligence Services was in the constitutional and democratic framework of the State, legally regulating its activities for the first time[4].

3 A series of repressive measures were introduced that strengthened police powers. Special corps (GIS, NOCS) were established for counterterrorism purposes and harsher penalties were enacted. Cf. Legge n. 15 del 6 febbraio 1980.

4 The offensive launched at the heart of the state by domestic terrorism brought united political forces to legislate on security matters as never before.

The long history of fighting organized crime and domestic terrorism has forged a culture of counterterrorism that is absent in other states around the world which have not experienced subversive seasons comparable to Italy's.

If we look at the data regarding terrorist attacks that hit Europe from the second half of the 20th century until the 1990s, it becomes clear that this phenomenon is mainly related to nationalist and separatist movements or right-wing and left-wing political extremism. Since 2001, instead, there has been a significant increase in attacks of a pseudo-religious nature[5] (phenomenon of religious radicalization; membership in jihadist extremist groups)[6] or related to social unrest.

In particular, the latter phenomenon is perhaps scarcely considered today as a real and ongoing threat to National Security. In Mario Caligiuri's interesting analysis[7], social unrest

---

The Law of Oct. 24, 1977, No. 801, introduced Law into the field of Security Intelligence Services for the first time. Precise political responsibility is given for the activities that are carried out in the world of Intelligence with the President of the Council at the head, and by competence the Minister of the Interior (heading the operational structure SISDe - Civil Service) and the Minister of Defence (heading the operational structure SISMi - Military Service). In addition, COPACO (Parliamentary Committee for the Control of Intelligence Services) is created to monitor the activities of the two security bodies.

5 Since 2006, Europol has published an annual statistical report on terrorist attacks and related arrests. Cf. EUROPOL - European Union Agency for Law Enforcement Cooperation, EU Terrorism situation & trend report (TE - SAT).

6 In the West, the word *Jihad is* often given a negative connotation of its meaning by translating it as "holy war." In reality, the term means "effort, commitment" and can cover a plurality of meanings.

7 Cf. Caligiuri Mario, *Il disagio sociale digitale: da problema di Ordine Pubblico a questione di Sicurezza Nazionale*, in "Formiche," no. 154, December 2019 :" The cyber space is increasingly central to social life, representing, to a certain extent, the prevailing economic sphere, as well as the political, communicative, informational and even educational sphere. It has thus become the decisive area of conflicts, which are increasingly economic and cultural in nature, fought through information warfare on the web."

is placed at the centre of an articulate analysis of its danger to society and the democratic institutions of a country[8]. And while on the one hand the increase in social inequalities, the crisis of democracy, job insecurity, low schooling, and poverty are just some of the conditions that generate and nurture this malaise, on the other hand the use of the Internet propagates and disproportionately amplifies its most nefarious and disastrous effects. All too soon, in fact, it has been magnified the greatness of the new world - *the cyber space* - where everything is unfettered, everything is free, everything is democratic. Today we know that things are not so simple and that there is a price to be paid[9]. The noticeable increase in cases of threats to the National Security related to social distress[10] shows how the problem needs to be addressed in a comprehensive and organic way, not only by monitoring *cyberspace*, where terrorist activities often find fertile ground, but also by identifying the elements of dangerousness in individuals who

---

8 Cf. Caligiuri Mario, *L'avanzata del disagio sociale (e quali rimedi)*, in «Formiche», n. 146, aprile 2019, pp. 38-39.

9 Caligiuri Mario, *Il disagio sociale digitale: da problema di Ordine Pubblico a questione di Sicurezza Nazionale, op. cit*.

10 The analyses conducted by the Council of Europe (2016) particularly focus on those "individuals who feel marginalized, mistreated, socially excluded, and desperately seek a sense of life and a sense of belonging (that) are at high risk of being radicalized, indoctrinated by extremist propaganda, including through the Internet and social networks, and recruited by terrorist groups" and draw a rather defined profile of the radicalized individual: young males (although the female share is growing) with low levels of education and little knowledge of the Islamic religion, unemployed or with unskilled jobs, often from poor families. Cf. Parliamentary Assembly, - Assembly debate on January 27, 2016 (6th Sitting) (see Doc. 13937, report of the Committee on Political Affairs and Democracy, rapporteur: Mr. Dirk Van der Maelen; Doc. 13959, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr. Pieter Omtzigt). Text adopted by the Assembly on January 27, 2016 (6th Sitting). See also Recommendation 2084 (2016).

may be considered dangerous in the abstract (the socially disadvantaged, by lifestyle or personality traits)[11] and in the environments that foster their criminal tendency (the so-called "deviant places")[12].

Since the events of September 11, 2001, terrorist attacks have gradually become more and more media-driven and sensational. The motivations, targets, and antagonists of the clashes change. Bomber cells are getting smaller and smaller, carrying out attacks with low technological capability, using *Improvised Explosive Devices* (IEDs) vehicles thrown at high speed into the crowd, aggressions made with small arms or edged weapons, terrorist activities that are sometimes even carried out by deranged individuals[13].

---

11 In this regard we can refer to the classification made by Law No. 1423 of Dec. 27, 1956 regarding preventive measures, which identifies certain types of people who are dangerous to security and public morality: "vagabonds and idlers; subjects engaged in illicit trafficking; subjects proclivious to crime; suspected exploiters of prostitutes, smugglers or drug traffickers; subjects habitually engaged in activities contrary to morality or public morality." Legislation was later introduced regarding the dangerousness of criminal subjects linked to the Mafia and terrorism. In the 1980s, new legislation (Art. 2 of L. 327/1988) intervened on the evaluation criteria inherent to the profile of subjects to be considered dangerous: "those habitually engaged in criminal trafficking; those who habitually live, even in part, with the proceeds of criminal activities; those who endanger the physical or moral integrity of minors, society, security or public tranquillity." Further classification covered categories related to sports violence and racially motivated violence.

12 According to the theory of *Ecology Crime* by Rodney Stark there are five factors that affect criminal deviance: population density, poverty, mixed use (urban areas where residential areas are adjacent to commercial spaces in cities), transience of residents, and social disintegration. Cf. Stark R., *A Theory of the Ecology of Crime*, in «Criminology», 25 (1987), pp. 891 - 907. See as well, Saitta Pietro – Rinaldi Cirus, *Devianze e crimine: antologia ragionata di teorie classiche e contemporanee,* PM Edizioni, Varrazze (SV), 2017, pp. 145 – 152.

13 See for example: the Oslo bomber Anders Behring Breivik who in July 2011 staged two terrorist attacks aimed at targeting the Norwegian government, or the October 2017 Marseille attack in which an illegal Tunisian fatally stabbed two young female students at Saint-Charles station.

The realization by each state of its vulnerability to such attacks has led each country to implement various security and protection measures for its territory, fostering the creation of centres for coordination and information exchange between different police and security agencies. The focus of cooperation between Intelligence agencies and the Police forces will increasingly be on the pseudo-religious terrorist threat.

In the aftermath of the *Twin Towers* attacks, Italy, too, adopted a series of urgent measures aimed at ensuring greater security of the state and its citizens[14]. But it was only in 2003 (after the terrorist attack on the Italian contingent in Nassirya) that a unified counter-terrorism structure was born, which provides for closer information collaboration between Police forces and Intelligence services, the C.A.S.A. precisely.

Recent studies of the terrorist phenomenon have shown how its branches and interconnections are not confined to specific individuals and specific activities, but find broader and more dangerous links in the world of corruption and crime[15].

By analysing terrorist attacks in recent years, it emerges how the world of terrorism is strongly connected to the world of crime[16]. Not only to the most vicious organized crime,

---

14 One of the first acts taken by the Italian state against terrorism was the approval of Law 438/2001, aimed at adapting Italian legislation (revision of Article 270 bis c.p.), until then oriented toward the threat of domestic terrorism, to the serious emergency of international terrorism.

15 Cf. Shelley L. I., *Dirty Entanglements Corruption*, Crime, and Terrorism, Cambridge University Press, 2014, p.5.

16 While in the past terrorism was mainly financed by states or powerful political organizations, in recent years this source of funding seems to be gradually eroding raising the need to find alternative sources of livelihood. Financing occurs through various channels, including trafficking in drugs, arms, archaeological finds, kidnapping for ransom, and human trafficking. Cf. Maronta F., Caracciolo L., *Criminalità e terrorismo sono due facce della stessa medaglia. Conver-*

made up of large-scale drug and arms trafficking, but also-and increasingly-to small-scale urban crime (which feeds on drug dealing, smuggling, counterfeiting), to which Western security apparatuses pay little attention.

Generally, the link between terrorism and organized crime is approached erroneously, as if they were two distinct criminal offenses independent of each other. From the post-war period to the present, however, there has been a growing realization that the boundary between them is increasingly blurred, resulting in a dangerous intermingling of economic activities and political objectives in order to destabilize states, giving rise to what some scholars have called *hybrid threats*[17].

This increasingly promiscuous and dangerous nature between criminal and terrorist organizations was highlighted as early as 2009 by the executive director of the *United Nations Office on Drugs and Crime* (UNODC):

> Today, drug trafficking has become the main cause of another problem: the financing of terrorism. It has become increasingly difficult to clearly distinguish terrorist groups from ordinary criminal organizations because their strategies increasingly tend to overlap. If we do not sever the link between crime, drugs and terrorism, the world will witness the emergence of a hybrid and that means organized crime terrorist organizations[18].

---

sazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa), op. cit., 2015.

17 Raufer Xavier., *New World Disorder, New Terrorism: New Threats for Europe and Western World, in «*Terrorism and Political Violence» 11, n° 4, 1999, p. 35.

18 Cf. Innocenti Piero, Caradonna Mirna, *Il narcotraffico internazionale è il "bancomat" privilegiato dai terroristi: Dalle Farc a Hezbollah, da al Qaida a Boko*

Just as the advent of asymmetrical warfare changed the scenario of confrontation, requiring a new awareness in order not to succumb to the new reality before us, so these new hybrid threats, due to a mixture of relationships between corruption, terrorism and crime[19], require a pragmatic approach in order to be limited. In addition to the new crime scenario, there is, as it was mentioned, the equally insidious and dangerous threat to National Security arising from social unrest, which may become uncontainable in the near future.

In such an environment, one cannot think of focusing only on single targets. Threats are increasingly numerous and unpredictable. That is why more extensive information gathering in the field of human sources by the Police forces could prove decisive in intercepting those famous "weak signals" that are often not recognizable by the, however powerful, technological systems.

Haram: dove c'è una lotta armata, c'è il commercio di droga a finanziare il conflitto, in «Limes», No. 6, July, 2015.

19 Cf. OCSE Report: Terrorism, corruption and the criminal exploitation of natural resources, Parigi, 2016. Vedi pure Shelley L., *Dirty entanglements: Corruption, crime and terrorism*, op. cit. 2014.

3.2
The investigative and informational model in the practical activity of the Police forces

In order to understand whether the construction of the hypothesized theoretical model can work, i.e., transform every law enforcement practitioner into a Human Sensor in police Intelligence activity, it is necessary to identify a frame of reference that takes into account practice and observation of reality as guidelines on which to structure a training program essential for implementing OES capabilities.

To this end, a reconnaissance[1] survey was carried out to identify what are the repetitive and significant elements that can identify a good Police forces investigator, and to research what is the most effective training path to obtain them. The results of the survey not only provided news that was useful for the purpose, but also revealed some important nuances regarding both investigative experience and practice, as well as intelligence activity.

The study model involved a *reasoned-choice* statistical sample concerning some members of the Police forces who regularly carry out long-time investigative activities. The administration of the questions included some open-ended questions designed to gather data and information from each

1 The sample that was used pertained to a number of Police forces members divided by geographic area (south, central and northern Italy) that was not particularly significant, but was enough to be able to determine a trend.

person's personal experience.

The analysis of the reports has described around which characteristics (with reference to those that police officers themselves consider essential to being a good investigator) the frequency distribution of the so-called *markers* observed was most concentrated, regardless of each officer's geographical origin and experience. The elements that emerged thus allow us to identify what are the key aspects that should be fostered and looked for in each individual operator.

According to statements by most investigators, everyone could perform OES duties if properly trained, even individuals who have no experience or notion of investigative and informational work. Indeed, the possibility of being able to acquire these kinds of technical skills would even lead to encouraging a good portion of police officers to perform their jobs with more enthusiasm.

Of course, to say that everyone can implement OES capabilities in the Human Sensor activity of Police Intelligence certainly does not mean that everyone wants to do it (especially if it is to be done off-duty) or that everyone is able to do it in the same way (and certainly not by relying solely on a training course). There are, in fact, many variables that contribute to determining the effectiveness of such an intervention, repeatedly reiterated by the interviewees themselves: the validity of the training course, personal cultural background, professional background, aptitude for similar activities, motivations, curiosity, and the system's ability to stimulate and organically incorporate new figures.

However, relying on the theory of large numbers, precisely because of the significant number of members of the Poli-

ce forces, it can be argued that widespread training in this regard would greatly increase the likelihood of being able to acquire useful information not otherwise acquired.

However, if we move on to consider the ways in which investigators have been trained, and which of these has contributed most to shaping their investigative skills, the question becomes really interesting.

The training is based on classical methods of learning: one theoretical (training courses; seminars; handouts, codification of laws, specific texts; study of previous investigative activities); the other empirical (direct experience; confrontation with others in the investigative/informative field and law enforcement; sharing of experiences).

But it is the second modality that is considered crucial for acquiring skills and professionalism in the field. While there is an extensive literature regarding the *modus operandi* of police investigative and informational techniques, it is the practical knowledge imparted by the most experienced practitioners themselves that provides the most important tools. A practical knowledge that cannot be transferred in any other way than by listening, observing and understanding how the most skilled investigators think, act and resolve different situations.

And, as is the case in *industry clusters*[2], the more this

2 In economics, the term *industry cluster* refers to a concentration of closely interconnected firms, suppliers and institutions in a given geographic area. The main innovation cluster known today is Silicon Valley. According to economist Michael E. Porter the cluster is «a geographic agglomeration of interconnected firms, specialized suppliers, service firms, firms in related industries, and associated organizations all operating in a particular field, and characterized by the simultaneous presence of competition and cooperation among firms». See Por-

knowledge is broad (extending to different fields and disciplines), deep (the child of a great deal of experience gained over time) and concentrated (enclosed in a small place and among many parties that greatly increase the opportunities), the more training and innovation will ensure a competitive advantage.

In fact, *clusters* tend to take place through agglomerations of different entities in a given physical location and allow access to the maximum flow of information and ideas, opportunities for collaboration, availability of specialists and knowledge. In addition, they allow for maximum efficiency in work activity, development of specialized *teams*, reduced risk exposure of Police forces members themselves, and more options for choice.

In this regard, one can refer to the economist Harmaakorpi Vesa's[3] study to understand why some working entities

ter Michael E., *Il vantaggio competitivo delle nazioni*, Einaudi, Torino, 2011.

3 By adapting Harmaakorpi's model in the context of the Police forces, it is possible to understand why some working environments, under equal resources, have greater informational, investigative, preventive, operational, etc. capacity. The economist's study is aimed at the development and innovation of regional systems starting from the analysis of the techno-economic and socio-institutional aspects of which the territory is made. "A region's competitiveness is based on regional resource configurations. In a turbulent world, these resource configurations must be renewed over time, imposing demands on regional dynamic capabilities. This study highlights five regional dynamic capabilities: leadership capacity, visionary capacity, learning capacity, networking capacity and innovative capacity. The study takes a holistic viewpoint in assessing the regional innovation environment. This environment is seen as a system of innovation networks and institutions located within a region, with regular and strong internal interactions that promote innovativeness and is characterized by integration. Innovations are increasingly seen as the result of nonlinear processes deeply embedded in normal social and economic activities. The nonlinear and interactive nature of innovation processes places new demands on social cohesion in the regional innovation system." See Harmaakorpi Vesa, *Building a competitive regional innovation environment : the regional development platform me-*

are more efficient, effective and innovative than others. Just as industrial *clusters* derive their strength from collective efficiency, that is, the "competitive advantage that comes from the presence of local external economies and joint actions"[4], so the *cultural* clusters[5] in the area of police investigative and informational work derive their strength from the collective efficiency brought about by the existence *in loco* of an investigative *background* and joint actions of the various players.

In the framework of empirical knowledge, for example, one of the most relevant aspects in the transfer of knowledge to individuals new to information activities concerns recommendations on how to acquire information from human sources (see Table 3.2 - A).

However, if to understand the importance of practical knowledge transfer we look to the field of study of ethology and gnoseology, we will notice how animals not only behave

---

thod as a tool for regional innovation policy, Doctoral dissertations series 2004/1, Helsinki University of Technology, Lahti Center, 2004.

4 Schmitz J. Hubert, Collective efficiency and increasing returns, in "Cambridge Journal Economic," Oxford University Press, vol. 23(4), July 1999, pages 465-483. By "external economies" we refer to those advantages outside the individual firm but internal to the *cluster*, such as: the on-site presence of skilled labour and suppliers and the rapid diffusion of knowledge; by "joint actions," on the other hand, we refer to those forms of collaboration both between individual firms or groups of competing firms and with suppliers or customers. In transliteration from the economic model to the investigative model, external economies can be understood to mean the combination of investigators from a particular office and other sectors and operators in the system; joint actions can be understood to mean the collaborative interaction between operators in the same office, between several offices, and between them and other institutions of the state.

5 Here understood as the concentration of men, resources, professional skills and cultural endowments that, individually or systemically, can be directed in the process of enhancing police investigative and informational activity.

by innate instincts and behaviours, but also by environmental conditioning and learning processes. The Austrian ethologist Konrad Lorenz, in fact, believed that the performance of human cognition is determined in the same way as the evolutionary process for the preservation of the species, that is, both by reference to "a real system, formed as a result of a natural process" that is evolutionary, and "in an interactive relationship with an equally real surrounding world"[6]. Similarly, the close interaction between police officers in the transfer of practical knowledge can serve to understand how individuals and environments are able to influence each other.

Nonetheless, it should be kept in mind that the lack of structured and specific pathways on the subject, due to the shortage of sufficient technical, logistical and economic resources, may have paradoxically benefitted the training of investigative personnel beyond measure, offsetting the need to acquire knowledge and skills with the simplest, cheapest and most effective modality available: shadowing experienced operators and gaining experience in the field.

The analysis of the reconnaissance survey revealed another fundamental aspect, regarding the Humint activity of Police in acquiring information: compared to the various information gathering activities of the Police forces[7], news from human sources turns out to be decisive. In fact, according to the interviewees, *human sources* are the main and most im-

---

6 Cfr. Konrad Lorenz, *L'altra faccia dello specchio: per una storia naturale della conoscenza,* Adelphi, Milano,2007.

7 Reference is made to the main information sources of the Police forces. See Table 3.2 - B.

portant *sources of information*. Indeed, often, breakthroughs in investigations or new investigative hypotheses come from informants, confidants, witnesses and collaborators. Of course, when referring to this type of information source, it is necessary to assess its reliability and veracity[8].

Although the use of modern technologies has enabled increasingly elaborate analysis of available data, greatly increasing the ability to search, aggregate and catalogue information to the point of becoming a formidable tool for understanding, preventing, planning and suppressing various criminal phenomena and possible connections with other social actors, the Humint activity of the Police remains irreplaceable and fundamental in information gathering.

8 The evaluation, grading and dissemination of information, is carried out through various *cross evaluation* systems. In this regard, both the Police forces and the Intelligence Services use certain models for evaluating and understanding the reliability of the information source and the veracity of the news collected. See Table 3.2 - C / 3.2 - D on the information evaluation method: *4x4 Europol system; 6x6 DEA system.*

Table 3.2 – A

SOME INDICATIONS ON HOW TO ACQUIRE INFORMATION FROM HUMAN SOURCES AND MANAGE THE RESOURCE REPEATEDLY REITERATED BY THE POLICE INVESTIGATORS THEMSELVES	
1	*Put the source at ease so as to instil trust*
2	*Reliability of the source*
3	*Information feedback*
4	*Do not trust the first information*
5	*Assess what the source's benefit is and why it reveals a particular piece of information*
6	*Annotation of information in a notebook*
7	*Meeting with the resource in pairs*
8	*Talk little and let the source speak*
9	*To say less than you know*
10	*Leading the conversation*
11	*Do not make yourself blackmailable*
12	*Do not get emotionally involved*
13	*Do not try to achieve a goal at all costs*
14	*Do not influence the source by giving him information*
15	*Ensure confidentiality of the source by not revealing the identity to third parties*
16	*Giving formal feedback (reporting) to one's superiors*

Table 3.2 – B

INFORMATIVE SOURCES of the Police Forces	
SOURCES	TYPOLOGY
Open	OSINT – open source intelligence
Technological	SIGINT – signals Intelligence IMINT – imagery Intelligence COMINT – communications Intelligence ELINT – electronic Intelligence CYBINT – cyber Intelligence
Human	HUMINT – human source intelligence: informant; confidants; witnesses; collaborators; undercover agent; interposed person.
Documental	- DATA BANKS - POLICE FORCES ACTS - PROCEDURAL ACTS
Closed	Documentary sources subject to constraints of confidentiality

EVALUATION OF INFORMATION
System 4x4 (Europol)

Table 3.2 – C

SOURCE RELIABILITY	A	Always reliable
	B	Almost always reliable
	C	Almost never reliable
	D	Reliability not verified
VERACITY OF INFORMATION	1	Unquestionable accuracy
	2	Information known only to the source
	3	Not known at source but found by external
	4	Unverifiable information

SOURCE

A Source for which there is no doubt about authenticity, reliability, or competence, or information provided by a source that, in the past, has proven to be reliable in all cases.

B Source from which the information received proved reliable in most cases.

C Source from which the information received proved unreliable in most cases.

D Source whose reliability cannot be assessed.

INFORMATION

1 The information is considered secure without reservation.

2 The information is personally known to the source, but not personally known to the agent providing it.

3 The information is not personally known to the source, but is endorsed by other information already on record.

4 The information is not personally known to the source and cannot be endorsed in any way.

EVALUATION OF INFORMATION
System 6x6 (DEA – *Drug Enforcement Administration*)

Table 3.2 – D

SOURCE RELIABILITY	A	Completely reliable.
	B	Normally reliable.
	C	Fairly reliable.
	D	Usually unreliable.
	E	Unreliable.
	F	Unclassifiable.
VERACITY OF INFORMATION	1	Confirmed.
	2	Probably true.
	3	Possible.
	4	Not very reliable.
	5	Unlikely.
	6	Unclassifiable.

SOURCE

A Absolute lack of doubt about the authenticity of the source. Proven to be completely reliable.

B There is some doubt about the authenticity, reliability and competence of the source although, in the past it has proven to be reliable in most cases.

C It usually gives rise to doubts about the authenticity, reliability, and competence of the source. In the past, some information has proven to be reliable.

D There are doubts about the authenticity, reliability and competence of the source. Occasionally reliable in the past.

E There are major doubts about the authenticity, reliability and competen-

ce of the source. It has provided unreliable information in the past.

F No judgment can be made because the source is not known.

INFORMATION

1 Confirmed by other sources. Logical in itself. Concordant with other qualified information on the same topic.

2 Unconfirmed. Logical in itself. Concordant with other qualified information on the same topic.

3 Unconfirmed. Logical in reasoning. Concurs in some places, with other information on the topic.

4 Unconfirmed. Not illogical. Not believed at the time of evaluation although possible.

5 The opposite is confirmed. Illogical. Contradicted by other information on the subject.

6 It is not possible to judge the information.

Explanatory note

While the evaluation and grading of information is used to establish the level of its trustworthiness (e.g., in the 4x4 system, level A1 indicates a very high reliability of the news), for the dissemination of information, on the other hand, we use a system that assigns a code depending on the recipient starting from the least confidential 1 up to the most confidential 6 (e.g., information with code 1 might be available to all Police operators, while information rated 6, only to operators dealing with a particular type of investigation).
A reliability level *A2 - 1* means that the source is always reliable, the information tested and known by the source but not the operator, and can be disseminated to all Police agencies.

3.3
The importance of the Human Sensor in the new demographic and technological scenarios

In the coming decades, two factors will act most forcefully in the social, economic and political changes on the planet: the increase in world population; the pervasiveness of technology in all areas of human life.

The latest 2019 United Nations report confirmed estimates of world population growth from the current 7.7 billion to 8.5 billion in 2030 and 9.7 billion in 2050, rising to nearly 11 billion by the end of the century (10.9 billion in 2100)[1].

And while Western countries will have an increasingly marked and steady decline, with a substantial increase in the over-65s[2], continents such as Asia, partly Latin America and particularly Africa will see a significant increase in their populations with a far lower average age. Nigeria alone, for example, will have a population of about 411 million in 2050 (more than double its current population), where the whole of Europe will not exceed 716 million[3] (a number even lower than

1 United Nations, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019: Highlights (ST/ESA/SER.A/423), New York, 2019.

2 The population of the globe is aging rapidly. While in 2019 the percentage of those over 65 is 9 percent, by 2050 it will be 16 percent. See Morgan Steve, *Come sarà la Terra quando saremo 10 miliardi,* in «Limes », n° 10, agosto, 2019.

3 United Nations, Department of Economic and Social Affairs, Population Division (2017). World Population Prospects: The 2017 Revision, Key Findings

that surveyed today). The demography of the 21st century, then, will mark the gradual decline of the Old Continent. A scenario, this one, that will bring about an upheaval in the economic, political and social arrangements of many countries.

World population growth, climate change, wars and famines will inevitably lead to increasing masses of human beings moving from the countryside to the cities and from one country to another in search of better living conditions. What's more, the idea of being able to reach the coveted "promised land" is further fuelled by the increasingly widespread use in third- and fourth-world countries[4], of the Internet, which, by bouncing images and footage of big-city opulence into every computer and *smartphone*, increases its reach.

Suffice it to recall the effect that commercials broadcast on Italian television had on the Albanian population in the aftermath of the collapse of the communist regime. On August 8, 1991, the cargo ship *Vlorë*, with 20,000 refugees on board piled up like ants, entered Italian territorial waters, docking at the port of Bari[5]. The country's economic collapse, severe food shortages and widespread political and social uncertain-

---

and Advance Tables. Working Paper No. ESA/P/WP/248, New York, 2017, pp. 23; 26. (for growth estimates see table 3.3 – A1/A2/A3).

4 Simoncelli Lorenzo, *Internet in Africa: i giganti del web alla guerra dei cavi,* in "la Repubblica - Affari e Finanza," 3 agosto 2019: «From 2000 to the present, Africa is the Continent that has grown the most in the number of Internet connections. In 20 years, it has grown from 4.5 million users to 525 million, almost all of them young people under 35 who connect to the Net more with smartphones than with PCs. Despite the growth, Africa still has the lowest population Internet penetration rate in the world».

5 Cf. Cfr. Redazione, *Invasione – Senza speranze: ponte aeronavale per rimpatriarli*, in «Gazzetta del Mezzogiorno», anno CIV – n. 198, 9 agosto 1991.

ty led many Albanians, hitherto isolated from the rest of the world, to flee and try their luck in other countries, some to escape starvation others chasing freedom.

Most of them had Italy as their destination not only because it was not far away, but also because of the many expectations it created, fuelled by those commercials that induced people to believe, erroneously, that they could arrive in a rich and happy country, where people even bought food for their pets, while on the other side of the Adriatic Sea they had nothing to feed themselves. If a simple television broadcast could instil these perspectives, one has to imagine what access to the Internet can bring about in the many developing countries.

The study of migration phenomena in recent decades has shown a substantial relocation of populations from the countryside to the cities. And it is precisely the latter that are having to undergo a radical change in their own appearance and identity, becoming more and more a huge suburb, a *non-city*. According to some scholars,

> «*megacities* are destined to succeed States as major geopolitical players. Megacities that hold a decisive share of national GDP and loom as global *hubs* due to their economic clout, ability to attract investment, and connection to counterpart centers [...] There are many more functional cities in the world today than there are actual states. Such cities are often islands of *governance* and order in much weaker states. Megacities are indifferent to the fragile states that surround them»[6].

6 Barile Alessandro, *Indagine sulle periferie,* in «Limes» n°4, maggio, 2016.

Traditional cities seem to be slowly sinking into a boundless and messy suburbia generated by its squatter nature (on the one hand, it is being built illegally; on the other hand, land-use plans now serve only to ratify what has already been built) thus becoming a boundless urban settlement that separates the "legitimate city" (the historic one) and the "functional city" (the one where the most important economic activities are concentrated, where people meet, study and work) from the immense suburbs, which, marginalized by the processes of public enhancement, turn into social ghettos, increasingly mestizo and less and less politically integrated and representable.

> «In Italy, the urban metamorphosis of the city of Rome serves well as a negative role model. Indeed, the capital is an abnormal city, disproportionate to its needs and population: 1287 square kilometres, compared to the 105 square kilometres of Paris or the 785 square kilometres of New York. A city where less than three million people live, making it one of the least densely populated large cities in the world. A contradiction generated by the squatter nature of its expansion: a third of the city's territory was born illegally, a territory larger than the entire municipality of Naples is in fact squatted, but it is also that portion of the territory where most of Rome's population resides today. So, can Rome still call itself a city? Rather, the facts correlate two cities, antithetical and hostile to each other: a historic centre quantitatively tiny compared to the rest of the territory administered by the municipality, but where all the city's economic flows are concentrated, from global tourism revenues to municipal economic and administrative representative functions, to which must be added the first (semi)peri-

> pheral belt meanwhile integrated into the legitimate city; and an immense periphery that begins at the edge of the Grande Raccordo Anulare (once a true city *limes*) and continues for miles beyond, in the middle of the former Roman agro now completely cemented and (sub)urbanized. A periphery, however, that holds no compactness or unity, except sociologically derived from its economic, cultural and political marginalization. We should speak then of suburbs, in the plural, because these urban settlements do not communicate with each other, they are as distant from the centre as they are from each other»[7].

Suburbs without ethnic borders, incorporating mixes of spurious identities, where it is the native residents who approach the living conditions of migrants and not vice versa. The difficulty of integrating millions of suburban dwellers will produce autonomous forms of integration, prompting a portion of these marginalized or socially maladjusted to find a sense of belonging and redemption in religious radicalism or criminal organizations.

In recent years, in addition to the migration issue, another important phenomenon has occurred: the advent of the Internet, which, with its innumerable repercussions in many spheres of human life, has produced a profound and radical change in society, disrupting every concept hitherto known concerning man's interactions with himself and the world around him.

---

7 Barile Alessandro, *Indagine sulle periferie, Op. Cit*.

A consistent and pervasive increase in technologies (particularly information and digital technologies) that increasingly invest not only the military, economic and political spheres of many countries, but also the private sphere of people. Just think, for example, of the IoT (*Internet of Things*)[8], where everything is networked and interconnected, ready to send and receive data useful for analysing, managing and controlling entire cities, companies, transportation, utility administrations, buildings or anything you want to connect[9]. An enormous amount of data (the *Big Data*)[10] that dematerializes the physical world by bringing it back into computable forms from which all kinds of information can be extrapolated and known. A volume of data that increases year by year exponentially[11] thus raising numerous questions about who materially has this data and how they decide to use it or make it available to others. This is a matter of no small importance[12].

---

8 The term "*Internet of Things*" (IoT) was proposed in 1999 by British engineer Kevin Ashton to describe a system in which objects in the physical world can be connected to the Internet through sensors.

9 IoT is just one part of the IoE (*Internet of Everything*). Indeed, the latter connects people, processes, data, and things in ways that make networked connections more relevant and valuable than ever before, turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunities for companies, individuals, and countries (Cisco, 2013).

10 «Big Data is the information asset characterized by such a high volume, velocity and variety that it requires specific analytical and technological methods for its transformation into value». De Mauro A., Greco M., Grimaldi M., *A formal definition of Big Data based on its essential features*, in "Library Review," Vol. 65 No. 3, 2016, pp. 122 - 135.

11 See table 3.3 – B

12 «An investigation by The New York Times and The Guardian, after months of fact-checking and negotiations with sources, has found that Cambridge Analytica-a data analytics firm that has worked with Donald Trump's election team and other controversial campaigns such as the pro-Brexit campaign-has collected the personal data of more than 50 million Facebook users (mostly Americans) in one of the tech giant's biggest *policy* violations. This data was allegedly

The possible applications of the evolution of IoT are truly countless and of great importance, particularly when relating them to National Security and the fight against organized crime. For example, the possibility of being able to acquire a huge amount and variety of data from so-called *smart cities* (starting from public transportation control and management, pet and people identification, authentication, traffic monitoring, etc.) allows both Security Services and Police Forces to be able to prepare contextual information useful for an increasingly detailed, broad and effective analysis of issues.

An extreme example of such systems is the use of artificial intelligence adopted by China. Indeed, all kinds of data end up in Chinese government databases: images and footage from cameras scattered around the city and equipped with facial recognition systems, payment card transactions, car movements, phone records, supermarket loyalty cards, cadastral data on homes, all the way to patient records. One of the biggest investments has been precisely in the use of artificial intelligence for facial recognition. Already in 2016 there were 176 million surveillance cameras on the ground and by 2020 it is estimated that 450 million more will be installed[13]. A system so effective that it can reconstruct with remarkable accuracy the movements and activities performed by anyone over the past seven days and locate a man among

---

used to build powerful software that would be able to predict and influence choices at the ballot box. While not entirely surprising (social networks have long been talked about as a potential risk to democracies) the case has raised a great deal of debate». Cf. *Cos'è il caso Cambridge Analytica?,* in «Il Foglio»19 Marzo 2018.

13 Cf. Tremolada L., *Cina, quando la sorveglianza è globale: sotto controllo 1,3 miliardi di persone,* in «Ilsole24ore», 15 aprile 2018.

a crowd of sixty thousand people[14].

Needless to say, one can well understand the capacity of these new technologies in the area of surveillance and territorial control and, at the same time, the need for human intelligences capable of preparing these powerful softwares to process and analyse the collected data and information.

However, it should be considered that although the prospect of an increasingly technological and artificial society even tends to determine human behaviour in a predictive way, humans will always be able to evade and circumvent the various control systems, as repeatedly demonstrated. Indeed, the very extreme pervasiveness of the technology with which we are wrapping the real world may eventually prove to be a boomerang from which we need to find shelter. A technological world dominated by an incredibly large data collection that is impossible to manage except with powerful microprocessors and complex software, where historical memory is increasingly Orwellian[15], information manipulable, data unverifiable, human relationships surrogate, where everything is image, and "written culture" is a brief and ephemeral quotation.

Information overload, for example, remains one of the no

---

14 News story reported in article: *Chinese man caught by facial recognition at pop concert*, in "BBC News," April 13, 2018.

15 In George Orwell's short story, *1984,* an Outer Party employee working in the offices of the Ministry of Truth is in charge of "correcting" books and newspaper articles already published, editing them so as to make the predictions made by the Party itself verifiable and true. He is also in charge of editing written history, thus helping to fuel the Party's own reputation for infallibility, apply *damnatio memoriae* toward dissidents who "never existed." "He who controls the past controls the future. He who controls the present controls the past." Orwell G., *1984*, Mondadori, Milano, 2004, p. 38.

small problems that could lead to intelligence failure, as happened to the U.S. agencies in 2001: although they had several elements to prevent the plot, they were unable to "connect the different dots" that would create the overall picture of the terrorist attack.

Robert David Steel, one of the world's leading experts on the U.S. Information and Security system, predicted the failure of international strategic intelligence years before the events of 9/11, listing and justifying the reasons that would lead to this outcome: over-technology in data collection is the first point[16].

In such a landscape then, placing blind faith in technological systems to ensure National Security and fight organized crime could mean once again[17] disregarding the extremely complex nature of man and his ability to adapt to the changes around him, ready to put in place measures and countermeasures to be beyond the reach and control of an increasingly technological society.

---

16 The six weaknesses of international intelligence pointed out by Steel are, "1) over-technology in data collection; 2) inadequate clandestine collection, basically limited to open sources; 3) serious inadequacies in resource management; 4) mental inertia compounded by organizational inertia; 5) lack of credibility of the director of acquisition if he or she appears to be inadequately informed about technologies and countermeasures; and 6) no involvement with the public." Cf. Steel Robert David, I*ntelligence – Spie e segreti in un mondo aperto*, Rubbettino Editore, Soveria Mannelli, 2002, p. 81.

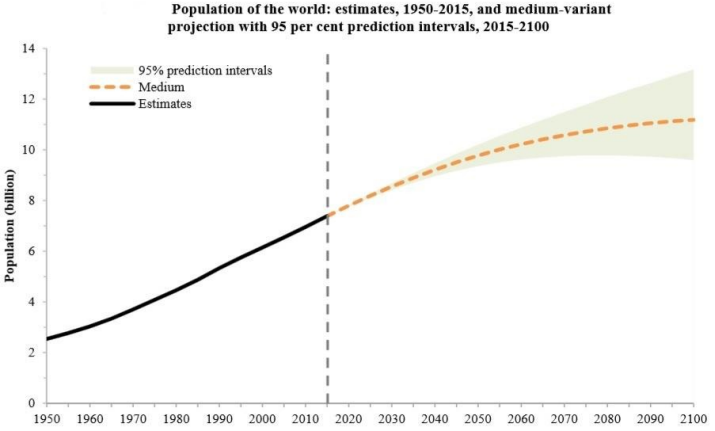
17 Prior to the attack on the Twin Towers, intelligence agencies halfway around the world, particularly those in the U.S., had devoted their greatest efforts and resources to implementing SIGINT technology systems (see the development of the AUSCANNZUKUS program known to the general public as "Echelon" developed by a cordate of 5 countries: Australia, Canada, New Zealand, the U.K. and the U.S., focused on the interception and collection of private and public communications).

It is in this context that the work of Human Sensor, aimed at safeguarding the National Security and combating organized crime, finds its raison d'être. An army of human sensors scattered throughout the territory and capable of autonomously activating, moving, seeing and listening in increasingly large and overpopulated cities, where the most sophisticated technologies will not be able to interpret the many complex nuances of human behaviour.

Table 3.3 - A1				
POPULATION OF THE WORLD AND REGIONS, 2017, 2030, 2050 AND 2100 ACCORDING TO THE MEDIUM-VARIANT PROJECTION				
	Population (millions)			
Region	*2017*	*2030*	*2050*	*2100*
World	7 550	8 551	9 772	11 184
Africa	1 256	1 704	2 528	4 468
Asia	4 504	4 947	5 257	4 780
Europe	742	739	716	653
Latin America and the Caribbean	646	718	780	712
Northern America	361	395	435	499
Oceania	41	48	57	72

Source: United Nations, Department of Economic and Social Affairs, Population Division (2017). *World Population Prospects: The 2017 Revision.* New York: United Nations

Table 3.3 – A2

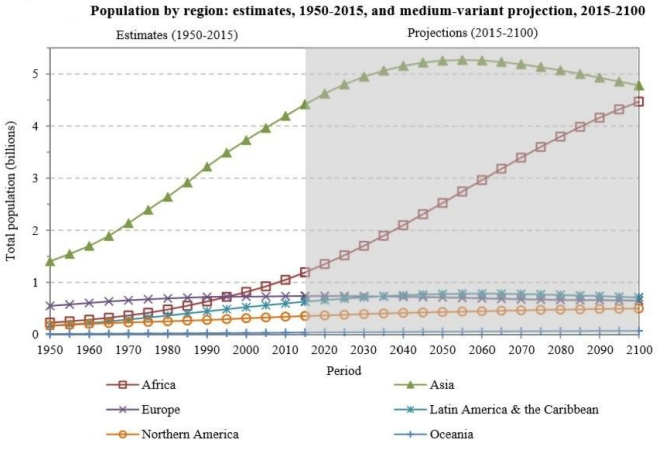


Source: United Nations, Department of Economic and Social Affairs, Population Division (2017). *World Population Prospects: The 2017 Revision*. New York: United Nations.

United Nations Department of Economic and Social Affairs/Population Division
World Population Prospects: The 2017 Revision, Key Findings and Advance Tables

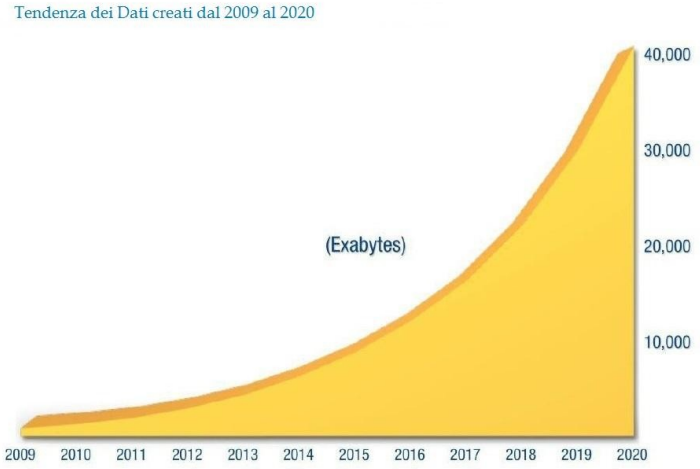
Table 3.3 – A3

2050 than in 2017. Beyond 2050, Africa will be the main contributor to global population growth.



Source: United Nations, Department of Economic and Social Affairs, Population Division (2017). *World Population Prospects: The 2017 Revision*. New York: United Nations.

Table 3.3 – B



This graph shows the exponential growth of *global data* starting from about 3 zettabytes in 2013 to about 40 zettabytes expected by the end of 2020. One exabyte equals 1,000,000,000,000,000,000 bytes, and 1,000 exabytes equals 1 zettabyte.
Source: Digital Universe Study - IDC.

Conclusions

The political, economic and social changes of the last thirty years have produced profound and rapid changes in the lives of people and states. The end of the division of the world into two blocs, the Gulf War, 11 September 2001, globalisation, the advent of the internet and of new communication technologies, the political destabilisation of many countries, the crisis of democracies, the economic and commercial rise of China, the Russian military resurgence, climate change, famine, the increase in world population, mass migratory phenomena, the boundless city suburbs alien to all possible integration: a world, ours, that seems to escape all possible governability and control.

Today, we seem to be repeating the same mistakes that in the recent past have led international intelligence apparatuses to fail in their predictions due to overconfidence in technological systems.

According to some in the field, the main flaw of the International Intelligence Services in recent years consists in their poor ability to interpret and decipher the so-called 'weak signals', caused by the lack of good analysts capable of connecting the famous dots. This may be partly true. In modern society, in fact, culture seems to be increasingly oriented towards hyper-specialisation, in which everyone knows everything about a particular sector or subject, but nothing about everything else: thus, the task of deciphering the complexity

of the world, of being able to look far and wide, has become arduous, precisely because we are used to seeing things in one place and close up.

The main problem, however, may lie elsewhere. The ability to catalogue, aggregate and analyse the available data (by now an impressive amount to manage) is not always sufficient to be able to determine a correct prevision or prediction of the scenarios one wants to understand, if one does not have a good collection of information. Often, in fact, there is a lack of precisely that contextual information that eludes sophisticated technological systems, as repeatedly demonstrated, making it necessary to acquire it through *Humint* activity directly in the field, as Robert David Steel had already pointed out.

If, on the one hand, Intelligence activity is - and will be - aimed at implementing the use of powerful software that collects and analyses the enormous mass of data sent by an increasingly networked world, on the other, there will be a need to guard those peripheries, those shadowy areas, those environments or those individuals who tend to exclude technology from their criminal and terrorist activities. These are the places where dangers to National Security or Public Safety are most likely to lurk.

Of course, it is not possible to monitor, control or supervise such an extensive and messy area, both because of the scarce financial resources and the large number of targets. A possible solution, on the other hand, could come precisely from a different vision of the employment of the Police forces, training them as human sensors to gather contextual in-

formation from the multiple local scenarios in which each operator is daily and naturally immersed.

This would provide a formidable force in intelligence work. An army already trained, numerous, scattered throughout the territory and without costs to be sustained, ready to be activated autonomously. This is an activity which would greatly increase the chances of the Police Intelligence and Institutional Intelligence to be able to acquire useful information to fight organized crime and safeguard National Security.

GLOSSARY

Glossary

Humint (Institutional)	Human Intelligence - This is the Intelligence discipline consisting of the search and processing of information that is of interest to national security and that is coming from individuals. Its specificities are linked to the typicality of the source and are mainly substantiated by particular handling methods.
Human Sensor (ES2)	It is a method of information gathering adopted in extremely changeable and unpredictable operational contexts by soldiers not particularly trained in Intelligence activities but ready to serve, not only as combatants, but also as 'human sensors' to detect any useful information from the tactical context in which they operate.
Intelligence led policy	Intelligence-led policing or information policing. It is a policing model that frames all the main police activities (combating organized crime, terrorism, drug trafficking, immigration, territorial control) in a more efficient (in terms of optimisation of the resources employed) and more effective way (in terms of results) thanks to adequate preventive analysis of criminal phenomena. Therefore, an approach that postulates a close integration between Intelligence and police activities in which the analysis of data is fundamental for a decision-making framework.
Intelligence (Institutional)	It is the instrument by which the state, through its Security Intelligence Services, collects, analyses, stores and disseminates (to interested parties) information and data useful for government decision-making in matters of National Security and National Interest.
OES (Observation, Elicitation, Surveillance)	It is that human activity that is preliminary to the collection of news and information that are useful for Intelligence, investigative and territorial control activities.
Police Humint	It is that activity carried out by the Police Forces that is mainly concerned with finding all possible information and sources of evidence on criminally relevant facts. It consists of that flow of information that includes news from confidants, informants and the police officers themselves, spontaneous statements on facts and persons of ordinary people, surveillance activities, reports and minutes of security activities.
Police Intelligence	This is the activity by which law enforcement agencies collect, analyse and disseminate information to higher levels or judicial or government authorities. It is the information process declined through the three main phases in function of a threefold direction, depending on the nature of the information processed or requested (internal superior bodies, judicial authority, political authority).

Preface Sources

Azzolini G., *Dopo le classi dirigenti. La metamorfosi delle oligarchie nell'età globale*, Laterza, Roma- Bari 2017.

Bauman Z., Lyon D., *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma-Bari 2014.

Beck U., *La società del rischio*, Carocci, Roma 2000.

Buchanan L., *Il settimo senso. I segreti delle spie psichiche dell'esercito americano*, Edizioni Il Punto di Incontro, Vicenza 2010.

Caligiuri M., *Intelligence e guerre dell'informazione nel XXI secolo: come respingere più efficacemente le minacce cyber*, in U. GORI (a cura), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Angeli, Milano 2019.

Caligiuri M., *Potere e sicurezza nelle smart cities*, in "Limes", 5, maggio 2019.

Caligiuri M. (a cura), Post Covid-19, Analisi di Intelligence e proposte di policy 2020-2021(2020), allegato a "Formiche", n. 5, maggio 2020.

Caligiuri M. (a cura), *Studi di intelligence 3. Avvicinarsi alla realtà*, Rubbettino, Soveria Mannelli 2021 (in corso di pubblicazione)

Dick P.K., *Rapporto di minoranza e altri racconti*, Fanucci, Roma 2002.

Faverzani C., Lanfranca D. (a cura), *La storia, le storie. Camilleri, la mafia e la questione siciliana*, Quaderni Camilleriani 2. Oltre il poliziesco: letteratura/multilinguismo/traduzioni nell'area mediterranea, Grafiche Ghiani, Monastir 2016.

Gagliano G., *Guerra psicologica. Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco, Roma 2013.

Galli G., *Il golpe invisibile. Come la borghesia finanziario-speculativa e i ceti burocratico-parassitari hanno saccheggiato l'Italia repubblicana fino a vanificare lo stato di diritto*, Kaos, Milano 2015.

Gori U., Germani L.S. (a cura), *INFORMATION WARFARE 2011, La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Angeli, Milano 2012.

Harari Y.N., *Homo Deus. Breve storia del futuro*, Bompiani, Milano 2017.

Lawrence W., *Le altissime torri. Come al-Qaeda giunse all'11 settembre*, Adelphi, Milano 2007.

Lissoni A., *Psicospie. Viaggio negli archivi segreti del paranormale in America, Russia e Medioriente*, Editoriale Olimpia, Sesto Fiorentino 2003.

Lombardo E., *Sicurezza 4 P. Lo studio alla base del software XLAW per prevedere e prevenire crimini*, Mazzanti, Venezia 2019.

Naim M., *Illecito. Come trafficanti, falsari e contrabbandieri stanno controllando l'economia mondiale*, Mondadori, Milano 2006.

Ostrander S., Schroeder L., Scoperte psichiche dietro la cortina di ferro. *URSS/BULGARIA/CECOSLOVACCHIA*, MEB, Torino 1975.

Rosling H., *Factfulness. Dieci ragioni per cui non capiamo il mondo. E perchè le cose vanno meglio di come pensiamo*, Rizzoli, Milano 2018.

Teti A., PsychoTech. Il punto di non ritorno. La tecnologia che controlla la mente, Springer Verlag, Milano 2011.

Wertherbach E., *Organisierte Kriminalität*, in "Zeitschrift für Rechtspolitik", 1994, n. 2.

Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Roma 2019.

Sitography

http://foreignpolicy.com.
https://formiche.net.
https://www.agi.it.
https://www.nonsprecare.it.
https://www.repubblica.it.
https://www.treccani.it.

Filmography

The Men who stare at Goats, by Grant Heslov (2009).
Minority Report, by Steven Spielberg (2002).

Bibliography

Aprile Pino, *Elogio dell'imbecille. Gli intelligenti hanno fatto il mondo, gli stupidi ci vivono alla grande*, Ed. Piemme, Milano, 2012.

Barron John M., Berger Mark C., Black Dan A., *On-the-Job Training*, W.E. Upjohn Institute for Employment Research, Kalamazoo, Michigan, 1997.

Bartel, A.P. *Productivity gains from the implementation of employee training programs*. Industrial Relations, Vol. 33(4), 1994.

Bauman Zygmunt, *La solitudine del cittadino globale*, Feltrinelli Editore, Milano, 2004.

Bertaccini Davide, *Polizia professionale – Polizia di comunità – Polizia dei problemi – Polizia dell'ordine – Polizia di prossimità*, Maggioli Editore, Santarcangelo di Romagna, 2011.

Boca S., Bocchiaro P., Scaffidi Abbate C., *Introduzione alla psicologia sociale*, Il Mulino, Bologna, 2010.

Bocchiaro Pietro, *Psicologia del male*, Editori Laterza, Bari, 2010.

Chabris Christopher, Simons Daniel, *Il gorilla invisibile. E altri modi in cui le nostre intenzioni ci ingannano,* Gruppo 24 ore, Milano, 2012.

Chomsky Noam, *Capire il potere*, Marco Tropea Editore, Milano, 2002.

Chomsky Noam, *Egemonia americana e "Stati fuorilegge"*, Edizioni Dedalo, Bari, 2001.

Chomsky Noam, Herman Edward S., *La fabbrica del consenso, ovvero la politica dei mass media*, Marco Tropea Editore, Milano, 1998.

Clausewitz Karl von, *Della Guerra*, Arnoldo Mondadori, Milano, 2000.

Colombo Emilio, *Stanca Luca, The Impact of Training on Productivity: Evidence from a Large Panel of Firms,* Working Papers from University of Milano – Bicocca, No 134, Department of Economics, Milano, 2008.

Cossiga Francesco, *Abecedario per principianti, politici e militari, civili e gente comune*, Rubettino Editore, Soveria Mannelli, 2002.

Dawkins Richard, *Il gene egoista. La parte immortale di ogni essere vivente*, Arnoldo Mondadori Editore, Milano, 2011.

De Kok Jan M.P., *The Impact of Firm - provided training on production: testing for firm - size ef fects, Tinbergen Institute Discussion Paper, Netherlands, 2000.*

Gagliano Giuseppe, *Guerra psicologica – Saggio sulle moderne tecniche militari cognitive e di disinformazione*, Fuoco Edizioni, Rende, 2013.

Giannulli Aldo, *Come funzionano i servizi segreti,* Ponte alle Grazie , Milano , 2013.

Giupponi T. F., *Servizi di informazione e forze di polizia dopo la legge n. 124/2007* – contributo per il Gruppo di lavoro di Astrid, 20 maggio 2009.

Harmaakorpi Vesa, *Building a competitive regional innovation environment: the regional development platform method as a tool for regional innovation policy*, Doctoral dissertations series 2004/1, Helsinki University of Technology, Lahti Center, 2004.

Hauser Marc D., *Menti Morali. Le origini naturali del bene e del male*, Il Saggiatore, Milano, 2007.

Hobsbawm Eric J, *Il secolo breve,* 1914-1991: l'era dei grandi cataclismi, Rizzoli Editore, Milano, 2000.

Illuminati G., *Nuovi profili del segreto di Stato e dell'attività di Intelligence,* G. Giampichelli Editore, Torino, 2010.

Izzi S., *Intelligence e gestione delle informazioni – Attività preventiva contro i traffici illeciti*, Ed. Franco Angeli, Milano, 2011.

Jean Carlo, *Manuale di studi strategici*, CSGE, Ed. Franco Angeli, Milano, 2017.

Kautilya, *Il codice del potere. L'arte della guerra e della strategia indiana* , Ed. Il Punto d'Incontro, Vicenza, 2011.

Konings Jozef, Vanormelingen Stijn, *The Impact of Training on Productivity and Wages: Firm Level Evidence,* The Institute for the Study of Labor, Discussion Paper No. 4731, Bonn, 2010.

Konrad Lorenz, *L'altra faccia dello specchio: per una storia naturale della conoscenza*, Adelphi, Milano, 2007.

Lynch Lisa M., *Training and the Private Sector,* University of Chicago Press, 1994.

Macchiavelli Niccolò, *Il Principe*, Biblioteca Universale Rizzoli, Milano, 1995.

Major Jeffrey C. Schrick, *Effective Intelligence In Urban Environments, Edit.* Tannenberg Pickle Partners Publishing, 2015.

Montanelli Indro, Cervi Mario, *L'Italia degli anni di piombo*, 1965 – 1978, Rizzoli - Corriere della Sera, Milano, 2011.

Mosca C., Gambacurta S., Scandone G., Valentini M., *I Servizi di Informazione e il Segreto di Stato (Legge 3 agosto 2007, n.124),* Giuffrè Editore, Milano, 2008.

Orwell G., *1984*, Mondadori, Cles, 2004

Parkinson Cyril North, *La legge di Parkinson*, Monti & Ambrosini, Pescara, 2011.

Pisani Vittorio, *Informatori, notizie confidenziali e segreto di polizia*, Giuffrè Editore, Milano, 2007.

Popper R. Karl, *Cattiva maestra televisione*, Marsilio Editori, Venezia, 2006. Cfr. pure Sartori Giovanni, *Homo videns*, Editori Laterza, Bari, 2007.

Qiao Liang, Wang Xiangsui, *Guerra senza limiti – L'arte della guerra asimmetrica tra terrorismo e globalizzazione,* LEG Edizioni, Gorizia, 2002.

Ratcliffe Jerry H., *Intelligence-Led Policing,*Willan Publishing, Cullompton – UK, 2008

Saitta Pietro – Rinaldi Cirus, *Devianze e crimine: antologia ragionata di teorie classiche e contemporanee,* PM Edizioni, Varrazze (SV), 2017.

Sawyer Ralph D. (a cura di), *Cento strategie non ortodosse*, Neri Pozza Editore, Vicenza, 2000.

Schmitt, Carl, *Dialogo sul potere*, Il Melangolo, Genova, 1990.

Singh Simon, *Codici & Segreti – La storia affascinante dei messaggi segreti dall'antico Egitto a Internet*, RCS Bur saggi, Milano, 2015.

Steel Robert David, I*ntelligence – Spie e segreti in un mondo aperto*, Rubbettino Editore, Soveria Mannelli, 2002.

Sun Tzu, *L'arte della Guerra,* Oscar Mondadori, Milano, 2008.

Wynne-Edwards V. C., *Animal dispersion in relation to social behavior*, Oliver and Boyd, Edinburgh 1962.

Altre Fonti

Ansoff I.H., Le risposte strategiche ai "segnali deboli", in «Sviluppo e organizzazione», fasc. 33, 1976.

Barile A., Indagine sulle periferie, in «Limes» n. 4, maggio 2016.

Black S. E., Lynch L. M., Human. Capital Investments and Productivity, in «The American Economic Review», vol. 86, n. 2, Papers and Proceedings of the Hundredth and Eighth Annual Meeting of the American Economic Association San Francisco, CA, January 5-7, 1996 (May, 1996).

Bonini C., Terrorismo, il nuovo schema di Minniti: "Sindaci e polizia locale ci aiuteranno a fermare i lupi solitari", in «la Repubblica», 22 dicembre 2016.

Caligiuri M., L'avanzata del disagio sociale (e quali rimedi), in «Formiche», n. 146, aprile 2019.

Caligiuri M., Predictive Policing. Il futuro della sicurezza è nei modelli di prevenzione, convegno regionale, Napoli, 24 maggio 2019.

Caligiuri M., La rivoluzione che verrà. Come il disagio sociale digitale minaccia la sicurezza nazionale, allegato, in «Formiche», n. 153, dicembre 2019.

Charbonnier A., L'Intelligence Service apre gli archivi del MI5, in «GNOSIS. Rivista italiana di Intelligence», aprile 2009.

De Mauro A., Greco M., Grimaldi M., A formal definition of Big Data based on its essential features, in «Library Review», Vol. 65 n. 3, 2016.

Fittipaldi E., Troppo Divise, in «L'Espresso», n° 2, anno LXI, 15 gennaio 2015.

Giansoldati F., Papa Francesco: Il comunismo ci ha rubato la bandiera, in «Il Messaggero», 29 giugno 2014.

Innocenti P., Caradonna M., Il narcotraffico internazionale è il "bancomat" privilegiato dai terroristi: Dalle Farc a Hezbollah, da al Qaida a Boko Haram: dove c'è una lotta armata, c'è il commercio di droga a finanziare il conflitto, in «Limes», n° 6, luglio, 2015.

Kfir I., Israel's Approach to Counterterrorism, in «The Strategist (ASPI - The Australian Strategic Policy Institute)», 27 settember, 2018.

Loeb V., Instead of Force, Friendly Persuasion, in «The Washington Post», 5 Novembre 2003.

Maronta F., Caracciolo L., Criminalità e terrorismo sono due facce della stessa medaglia, Conversazione con Louise Shelley, professoressa e direttrice del Terrorism, Transnational Crime and Corruption Center alla George Mason University (Virginia, Usa), in «Limes», n. 11, dicembre 2015.

Morgan S., Come sarà la Terra quando saremo 10 miliardi, in «Limes», n. 10, agosto, 2019.

Raufer X., New World Disorder, New Terrorism: New Threats for Europe and Western World, in «Terrorism and Political Violence» 11, n° 4, 1999.

Redazione, Bush: finiti i combattimenti in Iraq, in «Corriere della Sera», 2 maggio, 2003.

Redazione, Cos'è il caso Cambridge Analytica?, in «Il Foglio»19 Marzo 2018.

Redazione, Invasione. Senza speranze: ponte aeronavale per rimpatriarli, in «Gazzetta del Mezzogiorno», anno CIV, n. 198, 9 agosto 1991.

Rilling J., Gutman D., Zeh T., Pagnoni G., Berns G., Kilts C., A neural basis for social cooperation, in «National Center for Biotechnology Information, U.S. National Library of Medicine», Atlanta 2002.

Schmitt E., Shanker T., Bombings in London: Hearts and Minds. U.S. Officials Retool Slogan for Terror War, in «The New York Time». 26, July, 2005.

Schmitz J.H., Collective efficiency and increasing returns, in «Cambridge Journal Economic», Oxford University Press, vol. 23(4), July 1999.

Shelley L.I., Dirty Entanglements Corruption, Crime, and Terrorism, in «Cambridge University Press», 2014.

Simoncelli L., Internet in Africa: i giganti del web alla guerra dei cavi, in «la Repubblica. Affari e Finanza», 3 agosto 2019.

Stark R., A Theory of the Ecology of Crime, in «Criminology», 25 (1987).

Tremolada L., Cina, quando la sorveglianza è globale: sotto controllo 1,3 miliardi di persone, in «la Repubblica», 15 aprile 2018.

NAME INDEX

Africa, 98, 99, 108, 109
America, 13, 19, 35, 108 109
Ansoff H. Igor, 57
Aprile Pino, 56
Aristotle, 48
Ashton Kevin, 103
Asia, 98, 108, 109
Australia, 106
Azzolini Giulio, 12
Baghdad, 25, 36
Balaklava, 47
Barcelona, 58
Bari, 99
Bartel P. Ann, 73
Batson Daniel, 67
Barile Alessandro, 100, 102
Barron John, 72
Bauman Zygmunt, 11
Beane Billy, 23
Beck Ulrich, 9
Berger Mark C., 72
Berlin, 28, 58
Berns Gregory S., 66
Bishop John, 72
Black Dan A., 72
Black Sandra, 72
Boca Stefano, 64, 65, 66, 69
Bocchiaro Piero, 68, 69, 71, 72, 74
Bonini Carlo, 58
Brand Peter, 23
Breivik Anders Behring, 82
Brooker Charlie, 20

Buchanan Lyn, 13
Bush George, 34
Caligiuri Mario, 9, 10, 11, 12, 13, 44, 80
81,
Caltanisetta, 54
Camilleri Andrea, 16
Canada, 106
Caracciolo Lucio, 76, 83
Caradonna Mirna, 84
Caribbean, 108, 109
Chabris Christopher, 20
Chicago, 12
China, 104
Colombo Emilio, 74
Crimea, 47
Cuneo, 54
Darley John, 67
Darwin Charles, 63
Dawkins Richard, 64, 65
De Mauro Andrea, 103
Dick Philip K., 12
Europe, 80, 98, 108, 109
European Union, 53
Faverzani Camillo, 16
Fiore Paolo, 11
Florence, 55
Fittipaldi Emiliano, 55
Gagliano Giuseppe, 11
Galli Giorgio, 11
Gambacurta Stefano, 43
Genovese Kitty, 67
Germani Luigi Sergio, 10
Germany, 9, 12

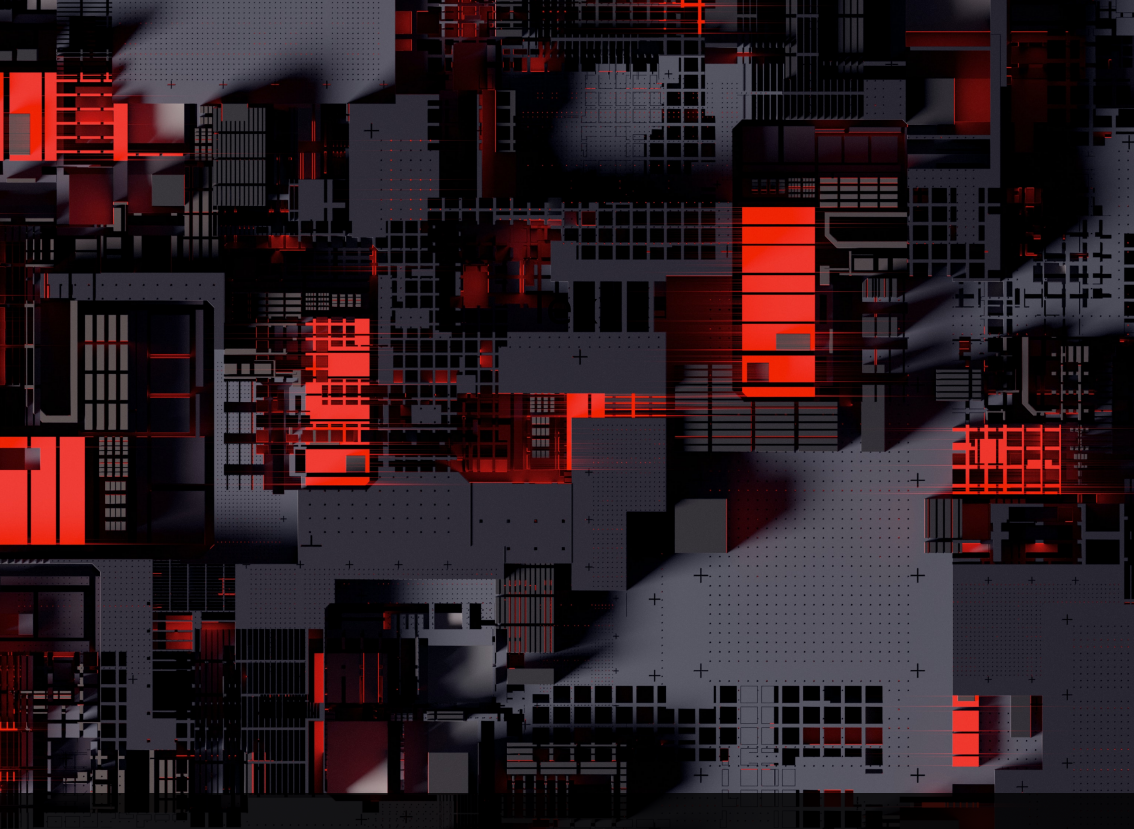
Giansoldati Franca, 19
Gori Umberto, 10
Greco Marco, 103
Grimaldi Michele, 103
Gromyko Andrej, 48
Gutman David A., 66
Hamilton William, 64
Harari Yuval Noah, 16
Harmaakorpi Vesa, 89
Hauser Marc D., 65
Heslov Grant, 13
Innocenti Piero, 84
Iraq, 33, 34
Israel, 30, 31
Italy, 7, 9, 10, 12, 23, 43, 53, 55
79, 83, 86, 100, 101
Izzi S, 45
Jean Carlo, 28
Jerusalem, 31
Kane Chris, 35
Kautilya, 48
Keith Alexander, 10
Kfir Isaac, 31
Kilts Clinton D. , 66
Kissinger Henry, 48
Lanfranca Dario, 16
Latin America, 98, 108, 109
Lawrence Wright, 9
Lewis Monroe Michael, 23
Lissoni Alfredo, 13
Lombardo Elia, 12
London, 12
Lorenz Konrad, 91

Los Angeles, 12
Lynch Lisa M., 72
Lyon David, 11
Macchiavelli, 48
Magi Gianluca, 48
Maronta Fabrizio, 76, 83
Marseille, 82
McKiernan J. Brian, 36
Metternich W. N. L. Klemens, 48
Milan, 12, 55
Mini Fabio, 27
Minniti Marco, 58
Monti Mario, 11
Morgan Steve, 98
Mosca Carlo, 43
Naim Moisés, 15
Naples, 12, 101
Nassiriya, 24, 83
Nehru Jawaharlal, 48
Neumann John von, 68
New York, 101
Nigeria, 98
Nice, 57
New Zealand, 106
Oceania, 108, 109
Omtzigt Pietre, 81
Orwell George, 105
Oslo, 82
Ostrander Sheila, 13
Pagnoni Giuseppe, 66
Papa Francesco, 19
Paris, 101

Parkinson Northcot, 56
Patton Michael S., 33
Popper Karl R., 19
Porter Michael E., 88
Qiao Liang, 27, 34
Ratcliffe Jerry H, 25
Reglan Fitzroy Somerset, 47
Reimer Dennis J., 38, 40
Rilling James K., 66
Rinaldi Cirus, 87
Rome, 55, 101
Rosling Hans, 15
Russia, 13, 23, 53
Saddam Hussein, 33, 36
Saitta Pietro, 82
Sartori Giovanni, 19
Scaffidi-Abbate Costanza, 64, 65, 66, 69
Scandone Giuseppe, 43
Schmitt Carl, 56
Schmitt Eric, 29
Schmitz J. Hubert, 90
Schroeder Lynn, 13
Shanker Thom, 29
Shelley Louise I., 76, 83, 84, 85
Simoncelli Lorenzo, 99
Simons Daniel, 20
Soviet Union, 48
Spain, 43
Spielberg Steven, 12
Stanca Luca, 74
Stark Rodney, 82
Steel Robert David, 106, 112

Sun Tze, 48
Terzi di Sant'Agata Giulio, 11
Teti Antonio, 13
Thorndike Edward Lee, 62
Tremolada Luca, 104
Trento, 12
Trisolini Marcello, 13, 16
Trump Donald, 103
Turkey, 23, 53
United Kingdom, 106
United States of America, 28, 33, 35, 48
Valentini Marco, 13, 43
Van der Maelen Dirk Leo, 81
Venice, 12
Vernon Loeb, 33, 36
Vlorë, 99
Walsingham Francis, 47
Wang Xiangsui, 27, 34
Wertherbach Eckart, 15
West Poit, 35
Wynne-Edwarda Vero Copner, 64
Xavier Raufer, 84
Zeh Thorsten R., 66
Zuboff Shoshana, 11

Pubblicato nel mese di settembre 2023
SOCINT *Press*
c/o Università della Calabria, Cubo 18-b, 7° piano via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia



Intelligence needs human skills, because it involves logic, rationality, thinking. In this original and well-argued publication, the figure of the Human Sensor in Police Intelligence is outlined. The proposal of this profession can be considered as the new frontier in intelligence gathering, as successfully experimented by the American army in the Second Gulf War. In fact, it is a matter of intercepting *weak signals*; that can then become overwhelming not only for public order but also for national security. Therefore, specific training that develops observation and surveillance techniques for Police Forces could be decisive. With these human tools, both old problems, such as organized crime, and new ones, such as social unease, can be tackled.

(from the preface by Mario Caligiuri)

ISBN: 978-1-28011-140-1

9 791280 111401