Scientific Research Publishing

Open Journal of Political Science, 2018, 8, 35-46
http://www.scirp.org/journal/ojps
ISSN Online: 2164-0513
ISSN Print: 2164-0505

The Intelligence Cycle*

Antonella Colonna Vilasi

Centro studi Uni, Rome, Italy
Email: mavil@tiscali.it

How to cite this paper: Colonna Vilasi, A. (2018). The Intelligence Cycle. *Open Journal of Political Science, 8,* 35-46.
https://doi.org/10.4236/ojps.2018.81003

Received: November 9, 2017
Accepted: December 26, 2017
Published: December 29, 2017

Copyright © 2018 by author and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution-NonCommercial International License (CC BY-NC 4.0).
http://creativecommons.org/licenses/by-nc/4.0/

Open Access

Abstract

Focusing on the Information Cycle, reference is made to the distribution architectures and the pathways that the various Intelligence products (journals, reports, alerts, forecasts) produce to the Administration (Intelligence Cycle). An introduction to any study on the Information loop needs a brief digression to clarify concepts such as data, news, and information. *Events* mean any event or action that has been established to be true and/or has occurred and whose knowledge is assigned an information value; the information is the unclear cognition of a fact and/or a significant event related to topics of interest; information, in turn, is the product resulting from data following a frame of processing, analysis, interpretation, comparison, reasoned integration and evaluation.

Keywords

Intelligence, Security, Intelligence Cycle, Politics, Society

1. Introduction

According to the U.S. Marine Corps handbook: *Counterintelligence* (U.S. MARINE CORPS, 2007), "The Intelligence Cycle is a procedure frame work for the development of mission-focused Intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the Intelligence officer must consider each IR (Intelligence Requirement) individually and apply the Intelligence Cycle in a manner that develops the required Intelligence in the most effective way".

*Pioneer in Intelligence Studies in Italy, during the last 20 years the author's research interests focused on Intelligence, the relation with the Political Science and the Intelligence Cycle. With more than 70 books published on the topics; among them: *The Intelligence Cycle*, *The History of M16*, *The History of the CIA*, *The History of the Italian Secret Services*, *The History of the Entity*, *The History of Mossad*, *and The History of the STASI.*

An introduction to any study on the Information loop needs a brief digression to clarify concepts such as data, news, and information.

Events mean any event or action that has been established to be true and/or has occurred and whose knowledge is assigned an information value; the information is the unclear cognition of a fact and/or a significant event related to topics of interest; information, in turn, is the product resulting from data following a frame of processing, analysis, interpretation, comparison, reasoned integration and evaluation (Castelvecchi, Lo Re, & Zardo, 2002).

2. Research Questions and Research Methods

2.1. Research Questions

With reference to this research, the first question posed is: how can Intelligence address the new challenges that we live every day, in computerized, multiethnic and multicultural societies, and above all in a globalized world?

Second question: what are the new capabilities and know-how and analysis tools that contemporary Intelligence needs in such a complex, turbulent and "chaotic" international system so as to require a new holistic and less systemic approach?

2.2. Research Methods

This study uses a three-step methodological approach: data collection, coding and analysis, using qualitative techniques.

The article offers a number of original contributions to the scientific literature. First, it re-examines the sources and the theory-building and proposes alternatives to the referable scientific literature accepted and proposed by the majority of scholars.

It strengthens the holistic interrelations in terms of consistency between disciplines such as Intelligence studies, history, sociology, political geography, and political science.

Thirdly, the proposed mixed methods generate an agenda for possible future studies and researchs.

The documents used refer to Open Source documents, archives, publications, and reliable secondary sources.

The limitation of this research id due to the fact that the Intelligence Cycle should be treated with an entire volume, and not only with a brief article.

3. Literature Review

Academic studies, apart from the bibliography proposed in the article, refer mainly to Intelligence agencies' manuals for internal use, in particular to CIA manuals.

As far as the Information collection is concerned, it can derive from covert sources (from the Defense or other Intelligence agencies), or from Open Source documents like: archives, publications, radio, TV, newspapers, scientific disser-

tations, and secondary sources as well.

The Information gathered is generically related to any element capable of gaining value, it may be a single section of an Information or a standalone element, whose reliability is established or easily verifiable (Izzi, 2011). Mainly, the focus is on the research and analysis units.

The data resulting from the Information process are often of great importance to National Security.

Simple, even trivial news, appropriately "worked" and embedded in a partly sketched scenario can complete a picture, sometimes very relevant (Eftimiades, 1994).

The Information must therefore be characterized by:

- certainty, that is, to be objective;
- completeness, as far as possible every useful element should be overlooked;
- organicity, the individual elements must be traced back to the general structure, with reference to concrete and proven connection frames;
- compatibility in a complete picture of a certain situation, with no discordant issues, and if some reveal a divergence, they must be re-evaluated;
- interpretation, every piece of Information must be analyzed in its entirety and, if more than one person evaluates, these should be differentiated;
- attribution and news, where possible, must be linked to an identified source or certainly identifiable;
- timing, the Information elements must be dated and, if their value extend over time, it must be delimited;
- localization, the acquired data must be placed accurately in the geographical area to which they relate;
- new data, the final data produced by the Information process must not relate to obvious or previously acquired things.

In order to clarify these points we can try to understand how these different "Information" modes come right into the Information loop.

Let's start by saying that Intelligence can be compared to a company that receives an input following a request from the decision maker; at the end of a long procedure, both the Information note, and the news collected as final output, end-up in a piece of Information that is further screened, processed, analyzed and inserted in a scenario context (Steele, 2002).

Information gathering is realized through what is called the Intelligence or Information Cycle, which is composed of several stages.

The term "Process" or "Information Cycle" can be used indiscriminately since the nature of the Information activity is that of a cyclical process; which means that Intelligence management is a permanent and systematic process that does not have a definite term, due to the fact that the Information produced is the basis for further research activities.

The Cycle is set up for real-time management of any data and news, as the activities conducted are interconnected and aimed at acquiring, collating, processing, evaluating and disseminating Information useful to the final security

of the Nation.

For operational aims, it is irrelevant whether the purposes are precautionary, just a mere expression of a need to know, or repressive, with a set of counterintelligence measures.

In its evolution the process re-emerges, therefore, systematically, since the elements that are not in-depth or carried out in the previous activities can, of course, constitute the prerequisite for further investigations.

The Information Cycle can be subdivided into a series of phases:

- conceptual phase or "directive";
- planning phase;
- data acquisition;
- data collection and analysis;
- final evaluation.

The first phase is of utmost importance, as you must start from the situation analysis in order to find the useful data for defining the "Information objectives" (Johnson, 2006).

If the collected data prove to be inadequate, the "clues", or provisional elements, as a work hypothesis, can be transformed into the research activity's "objectives" (Kock, 2011).

The following step focusing on "planning" aims to assign "objective" Information, with particular regard to capabilities and efficiency; the planning phase should indicate the most suitable sources to activate and use, as it can provide relevant data.

In the distribution of goals, it is appropriate to allocate, as far as possible, the same goal to multiple structures and sources, in order that the result can be compared and verified with cross-references.

Once the Cycle is completed, orders and requests are sent to sources and research bodies; from now on the Information network is activated.

The research consists in identifying the essential Information (such as the enemy's environment), and any factor that may influence the choice regarding the line of action (core competencies of the Research Unit).

Also external factors that may compromise a successful outcome should be stressed. At this stage, the analyst is fundamental; the image of a lonely analyst, the jealous master of a number of sources, who, with his conceptual tools, elaborates an ingenious outlook is almost obsolete.

Today, we can only think of "analysis groups" that work in teams on the same sources and give a specialized interpretation merging into an organic analysis.

Once the research phase has ended, it is transferred to the "data collection", which consists in the "transmission" of the Information by the search bodies to the Information body responsible for its "backup".

Once the organizational phase and the Information process have been concluded, the proper analysis step begins, the real production phase. If the collection and Information searching is done in a precise and exhaustive way, it is

possible to develop an effective and complete analysis.

The Information "analysis" enables to "sweep" the data in all the components, in order to analyze the possible applications and usefulness for the set-up objectives. The analysis phase consists of the following steps (Colonna Vilasi, 2011):

- preliminary examination;
- information evaluation;
- integration-interpretation;
- transcription and archiving.

"Preliminary examination" consists in a first screening of the Information: whether it is complete in all its parts, if the data are urgent, so as to recommend its immediate dissemination, without evaluation and interpretation (if they are to be prioritized for distribution, if they are of an informative interest, and even if they are of no interest).

This phase, therefore, gives the possibility to identify the Information potentialities and develop a comprehensive reconnaissance of practicable deepening hypotheses.

In the Information evaluation, both civil and military, an alpha-numerical cataloging system is used, which takes into account both the "source reliability" or the search tools and the Information "truthfulness". Sources verification, in fact, is one of the most delicate steps.

When talking about sources we must refer to different types of Information: traditional, open, confidential, free, internal and external (Rapetto & Di Nunzio, 2002).

Nevertheless, we can add an additional level of classification, as the sources can be relevant and irrelevant, have a fair relationship between costs and benefits.

In short, as regards the Information system in general, the issue of sources is a juniper of Information, possibilities and alternatives.

The sources and their retrieval methods are so complex that it has become necessary to identify for each moment of the "collection" a precise phase.

As regards sources, we can name the following steps: "discovery", "distinction", "distillation" and "distribution".

In Intelligence studies, the term "Information sources" defines a person or thing (documents and/or materials) from which Information is obtained.

A source can be controlled and activated to provide answers to specific questions:

-not controlled when it provides Information;

-Open (in this case it is an untrusted source that provides background Information or Basic Intelligence) and Current Intelligence Information;

-random, when an individual spontaneously provides Information without being required.

Information sources, open or covert, are important in the research context.

The first, in particular, can be made up of archives and computer files; the Open Source can also come from newspapers, magazines, scientific publications,

official reports of government-run public debates.

In democratic countries, where the press and publication of political and scientific news are open, open Information is very useful because it provides a complete, up-to-date and reliable picture of the situation in the various sectors.

The covert sources, on the other hand, are those whose accessibility is forbidden, and therefore subject to specific espionage or interception activities, conducted either by people or through technical means; in this case, to have access to such sources, it is necessary to rely on a dense and effective Information network made up of sophisticated specialists and equipment capable of detecting events and transforming them into interpretable signals.

Scholars use to categorize Information in two major categories:

- Human Intelligence (HUMINT), Information from Human Sources, and
- Signals Intelligence (SIGINT), which refers to technological aspects and tools.

The so-called Open Source Intelligence (OSINT) is also used.

Open Source Intelligence (OSINT) is not just Open Source Information, nor a substitute for "all source analysis". OSINT is a distinct analytical process that integrates human expertise with an integrated human-technical process to produce just enough, just in time Intelligence-Information tailored to support a specific decision (NATO, 2001).

The application of each system depends on the Information priorities; the most predictable threat to our security is, in the opinion of many experts, the proliferation of mass destruction weapons, which can also be used by small terrorist groups.

For this kind of threat, Governments need more HUMINT and OSINT sources.

HUMINT is the Information obtained through human sources, that is by informants or interrogators and monitors who, for institutional or professional reasons, are aware of the Information they want to find; this is undoubtedly the oldest and most risky Information gathering system, able to provide Information coverage even in impenetrable areas from other systems.

In vogue in the Cold War period, this technique has for some time been shadowed by the technology collection tools, but recently, in a multipolar world, it has proven to be an extremely effective and versatile tool.

As for any other human activity, however, such data acquisition has negative aspects as well.

The time interval between detection, verification, and relationship may be so long as to frustrate the utility of the same Intelligence Cycle.

Another serious problem can be the bias of both the agent and the informer with obvious repercussions on the credibility of the Information which, on the other hand, can hardly be verified.

The alternative is represented by Signals Intelligence, which is a ductile instrument dictated by both the specific Intelligence requirements and the type of detectors available.

In war time, battlefield decisions are subject to satellite surveys, photographic surveys of different light, ultraviolet or infrared bands, radar or sonar signals in the marine environment.

Intercepting and decoding enemy's communications is of utmost importance, via the Communication Intelligence (COMINT).

The scenario changes, and the enemy of my enemy is no longer necessarily my friend, especially in the economic sector.

Experts classify SIGINT (Signal Intelligence) according to the detected Information.

Measurement and Signature Intelligence (MASINT) include measurements collected from sensors, except for communications and photographic surveys (COMINT and Imagery respectively) (Asker, 1994).

The Imagery was of paramount importance during the Cold War for Arms Control and the Deployment of the Atomic and Conventional Arsenals; on a tactical level, Imagery has proved to be an indispensable tool for limiting losses between both military and civilian opponents.

A study carried out at the end of the First Gulf War by the United States Congress highlighted the high quality of the contribution offered to the operation by three new tactical gathering tools: JSTARS, ASARS and UAV.

The Air Force Army, equipped with the Joint Surveillance and Target Attack Radar System, has been able to provide Information on targets to be hit, regardless of weather conditions (Carapezza, Law, & Stalker, 1999).

The Advanced Synthetic Aperture Radar System has been able to locate moving vehicles and deliver high-resolution images of fixed targets, both at night and day.

The Unmanned Aerial Vehicle, used on such occasion for the first time, has been able to produce precious ground maps for the Navy, Army and Amphibious units without risking the loss of just one pilot.

In order to map for tactical purposes (1:50,000) it is necessary to use images taken at low altitude. On the other hand, flight operations in such situations expose the aircraft and the pilot to a high risk of being hit.

However, Imagery is no longer an exclusive monopoly of superpowers. In fact, on the market there are companies that can provide cheap price images with a resolution of one meter.

The sensors for detection are classified in two types:

- Presidia, manned and unmanned (abandoned on the ground or in the oceans and communicating via radio signals).
- Unattended Ground Sensors (UGS), definitely the most popular.

They are classified into: acoustic, seismic, magnetic, radiological and electro-optical, and have the advantage of having instant Intelligence capabilities, detect movements that cannot be discovered otherwise and do not endanger any human life.

On the other hand, disturbances from nearby installations have to be camouf-

laged to avoid detection, and require a sophisticated analysis system for data interpretation. Even if nowadays the fiber optic communication systems detect an increasing amount of Information with satellites or the Comint earth stations, in the near future SIGINT will undoubtedly continue to be one of the leading activities. At the same time, decoders will become increasingly obsolete due to the sophisticated and cheaper encrypted systems.

The first step in Intelligence is then linked to the "Open Source" area. Open Source Intelligence is a process for collecting, selecting, distilling and disseminating unclassified data to a small community of operators and in relation to specific topics.

Open Sources are no longer of primary Intelligence relevance since they have become a key tool for many other areas including private and business sectors.

Intelligence scholars distinguish three categories of Open Source:

- Open Source Data, OSD, simple and immediate, such as photographs, commercial satellite's imagery, personal letters, interrogations;
- Open Source Information, OSIF, generally assembled by an editorial selection, forming a unit of possibly verified newspapers, books, and scientific publications;
- Open Source Intelligence, OSINT, deliberately sought after, discriminated, analyzed and disseminated to a selected audience.

The overall belief that Open Sources are just a collection of newspaper clippings or more or less careful navigation on Internet, deceive many people, especially Intelligence operatives.

Nevertheless, the idea of finding useful Information in the press is certainly valid.

Also ethically, no one will be able to recruit an agent for stealing news readable in a newspaper, or using satellite's images provided by licensed companies, as Google Earth.

Among the advantages of Open Sources we can cite their immediate availability when a crisis occurs.

Most emergency situations happen in countries of "secondary" importance, which are not covered by classified collection capacity.

Often emergency situations involve excessive trust in international organizations and the need of having to share with allies of dubious reliability.

All this, if not impossible, is at least very difficult in the case of classified sources.

It should not be forgotten that, via OSINT, results do not necessarily have to relate secret ratings. OSINT can also be a key instrument for military operations.

Nowadays the ability of an analyst consists of putting the politician who has a burning question quickly in touch with a world-wide expert, generally in the private sector, and offer the requested right away and within a few minutes.

Another advantage of relying on external expertise is that the training of such experts is a cost to others, which does not affect the budget.

Governmental agencies will not have to keep staff constantly updated and,

above all, targeted at a specific field, which even in the advantage of specialization, limits the field of interest.

Universities are also useful sources with their continued scientific research as for a huge source of accurate and, above all, reliable data.

Indeed, some universities are specializing in the construction of archives that in the present state are far superior to the quality, quantity and expertise of those kept by Government agencies and in many countries.

Just to make a few examples:

- The Monterey International Institute of International Studies, has the most comprehensive global database on the proliferation of nuclear, chemical and biological weapons;
- The Marcy Hurst College, is specialized in drug trafficking;
- The Oxford University, has created a Department called Oxford Analytica that uses teachers as a real "Intelligence council" capable of providing world-class consultations.

4. Conclusion

In conclusion, each Nation needs spies and satellites, useful in a National Intelligence Community capable of using Open Sources, quickly and at low cost, capable of tracing back to political, parliamentary and extra-parliamentary groups, or organized protesters, such as the Black Blocs.

Commonly spread through Internet, such as Indymedia: brochures, leaflets and all sorts of media, ideas, and action plans cannot and should not escape the consideration of Intelligence analysts.

Cinema can also be a very interesting Open Source for the 007.

Cinema does not just reflect the director's mentality, but also the producer's ideology and culture, tensions, problems and hopes. Cinema is above all a social phenomenon. And as such, it describes the world better than many books and dossiers.

In addition, many films have been written in collaboration with the CIA and other agencies, which, in exchange for tools, media, and their approval, inculcate in the viewer's minds a self-evident image.

Another Open Source is Internet. However, the myth of Internet as the source through which Intelligence finds the majority of Information, is not true. Ninety percent of useful Information is not even digitized or published, but is owned by private companies or institutions.

It is true, however, that the gradual growth in network users, the ever-increasing pervasiveness in business, institutions, groups and individuals, does not allow this tool to be omitted as it is still an important source for professional Intelligence, with reference to the technical-logistic aspects.

A 1994 study by the US Open Source Program Office (Cospo) of the US-NSC stated that Internet contains only four hundred and fifty sites that are really useful and in any case full of "rough" data, and that ninety-nine percent of the

content of the network is made of pornography, opinions and advertising. In fact, two hundred and fifty thousand potentially useful Intelligence files are now available in the "deep web".

Further evidence of what has been said is a development program carried out by the United States. It provides investments aimed at spreading the computer usage in Third World countries and to allow access to the network, and thus facilitating the ability to capture Information from US Intelligence.

In fact, the network freely runs ideas, information and even criminals.

It is undoubtedly a media tool capable of undoing distances and breaking cultural and linguistic barriers between religious, political, social and criminal organizations that can use the network to implement different strategies of attack and defense, lawful and illicit.

In addition, new technologies allow including software into almost every electrical appliance, from refrigerators and dishwashers to automobiles and mobile phones, communicating with the net-citizen of the civilized world, knowing his tastes and habits.

Technologies that help us to live better, on the other, make us more "detectable".

This is undoubtedly useful to economic Intelligence.

A refrigerator that finds that milk is about to end and orders it directly to the trusted minimarket reveals what your tastes and habits are like, transforming yourself into a human market research. On Internet you can find technologically advanced companies that offer various types of services accessible by millions of users.

There are services for business and consumer users, or social services; but cyberspace involves also negative implications, such as terrorist propaganda, pedophilia and pornography, weapons and organs traffic, satanism, and money laundering towards tax havens.

Also technological espionage has come to the fore at the expense of many companies and research institutes.

Internet, however, is always a sufficiently reliable mirror of reality with positive and negative aspects. Internet, distributed and interlinked, reflects human social patterns and constitutes therefore a series of aggregations in which it is possible to conduct a reliable analysis according to the sociometric disciplines.

Search engine technology is also very useful.

The Intelligence analyst out of academic schemes can find useful tools such as search engines or data mining. These tools can optimize data in a semantic discrimination and interrelation of apparently disconnected information, with subsequent source listing.

Another example of Open Source is the "gray literature".

A term that indicates, in the jargon of librarians and documentaries, a vast area of "unconventional documents" that are not disseminated through the normal commercial channels and are therefore often difficult to locate and

access.

The reference to gray color was born in the mid-1970s and refers to something intermediate between the normal "white" literature of commercial circuits and the "black", completely inaccessible.

This category includes, inter alia, doctoral dissertations, business and technical reports, reports submitted at conferences, essays awaiting acceptance by academic journals, catalogues, hardware and software manuals, university notes related to training courses, audiovisuals, bulletins and newsletters, theater scripts, press releases, exhibitions and translations catalogues.

Given the amplitude of the category, there are no comprehensive repertoires for identifying the references of any existing "gray literature", even at National level.

Some private institutions and companies are creating sectoral databases, available on Internet, computerizing many documents, or more often by providing bibliographical indications.

For example, a European community project has created in 1985 a database called the European Literature (European Association for Gray Literature exploitation).

In November 2002, it was made of 780,000 documents.

Important sectors of gray literature are the pre-prints, that is, research publications, studies and theories, long before their appearance in official scientific journals, which, before publishing an article, subject the content to a peer review by international experts.

Finally, it is necessary the presence of particularly motivated staff with a broad and multidisciplinary culture, capable of focusing on the purpose and the function of the information processed.

Intelligence production, to be truly effective, must be available to the widest possible audience without compromising either the users' political position or the Intelligence leaders.

Nowadays with an increasing level of privacy, the usefulness of Information decreases.

Knowing the hidden secrets of your enemy continues to be of paramount importance for the National Security, but it is useless to take risks and face high costs for collecting data that could easily be taken from a student as well (Quigging, 2007).

References

Asker, J. R. (1994). *High-Resolution Imagery Seen as a Threat Opportunity* (pp. 51-53). Aviation Week and Space Technology.

Carapezza, E., Law, D. B., & Stalker, K. T. (1999). *Unanttended Ground Sensor Technologies and Applications*. Michigan: SPIE.

Castelvecchi, A., Lo Re, C. C., & Zardo, F. (2002). *L'intelligence americana. Uomini, strutture e politiche dei servizi Usa* (p. 33). Roma: Castelvecchi.

Colonna Vilasi, A. (2011). *Manuale d'Intelligence* (pp. 15-55). Reggio Calabria: Città del Sole edizioni.

Eftimiades, N. (1994). C*hinese Intelligence Operations.* Annapolis: Naval Institute Press.

Izzi, S. (2011). *Intelligence e gestione delle informazioni. ttività preventiva contro i traffici illeciti* (p. 22). Milano: Franco Angeli.

Johnson, L. K. (2006). *Strategic Intelligence* (p. 61). Westport: Greenwood Publishing Group.

Kock, W. U. (2011). *Counterterrorism and Open Source Intelligence.* Odense: Springer.

NATO (2001). *Osint Handbook.* Norfolk, VA: Saclant.

Quigging, T. (2007). *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (p. 157). London: Qorld Scientific. https://doi.org/10.1142/6357

Rapetto, U., & Di Nunzio, R. (2002). L'Atlante delle spie: Dall'Antichità al grande gioco a oggi. Milano: Rizzoli.

Steele, R. D. (2002). *Intelligence. Spie e segreti in un mondo aperto* (p. 242). Soveria Mannelli: Rubettino.

U.S. MARINE CORPS (2007). *Counterintelligence* (p. 6). New York: Cosimo.