American Journal of Multidisciplinary Research & Development (AJMRD)
Volume 2, Issue 11 (November- 2020), PP 27-33
ISSN: 2360-821X
www.ajmrd.com

Research Paper **Open Access**

Cyber Humint. A Behavioral Analysis Perspective.

Paola Giannetakis[1] – Lucia Iannilli[1] - Federica Caravelli[1]
[1]*(Link Campus University, Italy)*

ABSTRACT: Cyber HUMINT is an important tool of contemporary Intelligence, interacts, exclusively on-line with sources and targets, in a similar way to what is performed traditionally. The rise of social media allowed a new development of human intelligence. Paradigms in this direction enlighten the necessity to identify specific characteristics of such professionals.

Keywords - Humint, intelligence gathering, cyber Humint, hybrid threats, terrorism

ASYMMETRIC THREATS

In a complex operational scenario, characterized by fluid and asymmetric threats in continuous transmutation and more unpredictable then before, one rule is still fundamental: gathering the right information at the right time makes the difference.

The processes of economic globalization, geopolitical transformations, rapid changes and pervasive use of new techs characterize our era and contribute to the creation of an increasingly diversified plethora of threats to be handled by intelligence agencies. Asymmetric challenges and asymmetric means are central component of future threats, Hughes, [9] described asymmetric warfare as attacking an adversary's weaknesses with unexpected or innovative means while avoiding his strengths as in a traditional warfare would be. In the modern era, many forms of asymmetric attack are possible: terrorism, guerilla, WMD, propaganda, cyberattacks, settled to destabilize countries' societies and institutions.

Technological development has changed the way we search and analyze news, and therefore the way we do intelligence has changed. Methodologies, information models and tools have undergone a real revolution. Doctrines, organizational models, procedures, consolidated tools in recent decades have opened to new intelligence paradigms, indeed majority of Intelligence Services launched programs to reorganize technical, research and information analysis procedures. With this huge – infinite – amount of data success depends mainly on two critical issues: one is to be able to ask the right questions, the other is to be able to see the meaningful and leave the rest behind, this is the main difference to produce a reliable intelligence product; in simple terms removing the noise and isolating what matters for the specific necessity.

TERRORISM AND TECHNOLOGIES

New technologies, encryption, anonymization, drag and drop devices, data calls, brought in instruments of communication and coordination without the need for command centers, making possible to organize attacks, easily and quickly, all over the world.

With Jihad 2.0 we experienced a media war that has its ideological connotation, an identifiable model, precise functioning and dedicated professional resources, all oriented to the concept of networking through the network. Social media became a mirror of the reality in which terrorist or criminal organizations are reflected. In 2013, we started to see the success of the media strategies carried out with Social Media: thousands of young people recruited online by ISIS to sacrifice themselves in Syria or Iraq.

Technologies have introduced new opportunities for terrorist groups by enhancing the capabilities of Communications, Command, and Control which have reduced the time and risks of transmitting information. IT has given the possibility to communicate, coordinate and conduct activities in a manner often isolated by a central command becoming faster and more secret.

The recent evolution of the jihadist threat towards forms of "widespread" terrorism, often characterized by the action of radicalized subjects on the web and not always linked to well-organized groups, requires a relaunch and strengthening of HUMINT capabilities. Information research, to develop an effective understanding and prevention of new and constantly evolving threats, must consider the new forms of relationships that are also implemented on the web. The more our lives are connected to the network, the more our real and virtual identities merge.

Furthermore, it is necessary to adapt concepts, security and defense practices to the challenges posed by the hybrid war, a widespread, pervasive and delocalized war that is the figure of the modern generation of conflicts that overcome the classic and geographically defined engagement of rival armies, integrating an extreme liquidity in the presence of new players on these innovative battlefields.

INTELLIGENCE

Intelligence derives from the direct, coordinated collection and processing of information relating to an operating environment in support of the decision-making process.

Information and intelligence are not synonyms: information is what can be known, but not all known information becomes Intelligence. Intelligence relies on a process through which the raw news acquired are evaluated and processed so that they can be judged as reliable information and therefore usable within a decision-making process:

a) determination of information needs;
b) drafting the research of activity plans necessary for the pursuit of the information objectives;
b) collection of information search, conducted with different methods;
c) information processing, activities and techniques necessary to transform news into meaningful and usable information;
e) dissemination and use;
f) feedback or informational return, allows to evaluate the effectiveness of the analysis methodology.

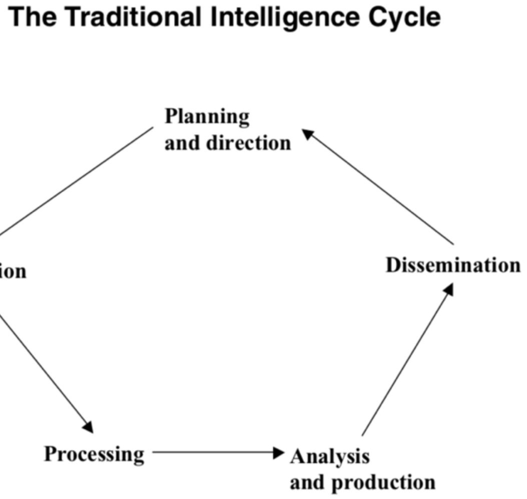

Image 1- (Source CIA) Traditional Intelligence Cycle

HUMINT

Human Intelligence (HUMINT) is a discipline of Intelligence that indicates any kind of information that can be collected through human sources to identify elements, intentions, composition, strengths, tactics, equipment, personnel and functionality of a country or actor. HUMINT uses human sources as an information-acquisition channel through different methods, both active and passive, with the aim of satisfying the request of the decision maker.

Humint includes:

a. reconnaissance;
b. direct interaction with individuals;
c. acquisition of information, for example by interrogation;
d. surveillance;
e. infiltration and espionage
f. counter-espionage.

There are two primary roles in H (Humint) operations. The first role is covered by the person to be recruited - called source or informant. A Humint source is a person from whom information can be obtained. Source may either possess first or second-hand knowledge: H sources include threat, neutral, or correlated to persons in

strategic positions sources.
The second role is that of the H recruiter or operator. The activity for the acquisition of information is essentially divided in:

a. **Spot:** Identify individuals who could become potential sources able to provide the information you need;
b. **Assessment**: Evaluation of the potential of the source to access information, as well as its motivations, its vulnerabilities;
c. **Recruit:** Conduct of the recruitment operation;
d. **Manage:** Organize and manage meetings with the source, give precise tasks, conduct de-briefings, and when necessary provide for the release of the same source (end of the report);
e. **Validate:** Validate the information collected.

The gathering of information deriving from human sources allows decision-makers to have a profound and unique vision of the intentions and capabilities of the adversary.

Organized crime and terrorist organizations are generally very difficult to penetrate by surveillance and undercover operations. In countries like Yemen, Iraq, Syria, Afghanistan and Somalia, H activity is extraordinarily difficult but it is essential.

HUMINT AND TERRORISM

In recent decades, western countries empowered the development of powerful technological intelligence tools to counter terrorism threat by analyzing big data acquired through the monitoring of social media. The rise in new systems development, able to acquire, analyze, decrypt, filter and verify a considerable amount of information pertaining to the main crisis areas and various threat factors, not only related to terrorism but also to other areas such as: the economic-financial market, hacktivism, geopolitics, energy resources, transnational criminal organizations, etc.
Technological means of information produce products of research that cannot be replaced by the contribution of human sources. For example, the web produce an enormous amount of news that, in the absence of online and offline HUMINT activity, make the task of selecting and prioritizing increasingly difficult.

Collection of information from open sources with models in use does not currently guarantee extensive analysis of the potential threat.
Penetration of terrorist groups through human sources or undercover agents is still an effective methodology to acquire information about plans, intentions and key characters of these aggregations.

Law enforcement, intelligence and other authorities are developing increasingly sophisticated tools to proactively prevent, detect and deter terrorist activity involving use of the Internet. The use of traditional investigative means, such as dedicated translation resources for the timely identification of potential terrorist threats, is also expanding.

CYBER HUMINT

Cyber HUMINT has given decisive contributions in crime fight and countering international terrorism making possible to identify potential sources / targets. Social media assumed important role in the recruitment of foreign fighters for the Syrian conflict, allowing contacts with potential volunteers, convincing them to leave and communicating instructions to reach the theater of war.
For these reasons, Cyber HUMINT adds to OSINT and SOCMINT activities - that only passively acquire data from open sources, social networks and Deep Web – interactions with sources and targets in a more similar way to what is performed by traditional HUMINT.

Two primary factors are determining virtual sources. The first is closely linked to origin and nationality, the second concerns affiliations of a person with a group or organization precisely because they are part of the system, and therefore able to release sensitive information. Basically, identification of nations and territories experiencing political instability and internal security issues and might pose a threat to national security.
The ability to socialize and create a bond is a must in the acquisition of H information, taking advantage of the motivation or vulnerability, the recruiter tries to create a confidence with the source and involve him in participating. Once the relationship is firmly established, the recruitment phase continues according to the criteria deemed relevant by the recruiter, ranging from financial compensation, immigration benefits, patriotism, revenge, or the fear of being imprisoned. A potential source could release information simply for family

reimbursements and / or religious differences. When the source is no longer reliable and / or credible, you can proceed with the release.

According to a retired CIA analyst, Lowenthal, the process of acquiring a source is divided into four phases: identification, development, recruitment and decoupling.

Identification is used to identify a potential human source that has access to the information you need. It requires knowledge of biographical data such as nationality and job, as well as motivations and vulnerabilities, since personality and behavior are crucial for success of operation. For example, if the person is introverted or is extrovert, aggressive or submissive. All this helps to develop a better strategy to induce the source to release information, just as it can be useful to establish a relationship based on a strong bond and mutual trust.

Despite the presence of numerous fake profiles, social networks and online dating sites are for the most part frequented by real people with situations of equally real relationships that maintain contact with people already known or create the conditions to know others.

Even what happens in virtual relationships can have repercussions in the real world. As explained by the FBI Internet Crimes Unit, the victims, who use dating sites believe they meet a good and honest person without ever having seen it, are perhaps divorced or widowed individuals, who are often offered flowers or other gifts with purpose of establishing a strong bond. Lately, fishers also offer financial help.

VIRTUAL AGENT

Not all operational agents are able to carry out this task since, it is necessary to possess a base of basic skills that require an aptitude for human relations, being able to interact naturally with others and to stimulate them to express themselves on the relevant topics by appropriately guiding the conversation. Humint is an activity largely dependent on human qualities, especially in the case of clandestine operations that require to move in environments of dubious morality and high risk.

Undercover agents must acquire ways, languages and mentality like those of the adversary and support the emotional weight of the "recitation" without suffering psychologically and enduring marked levels of stress.

Operational undercover agents must move freely in cyberspace and approach entities that can also take role of sources, for example recruited informants. A recruited source is a person aware of the role it plays and of the safety rules that must be observed in order not to take risks neither to the operative agent. In addition, other people, occasional sources, can provide useful information without being aware of the real identity of the person they are interacting.

These are operations that can last for years and should be conducted with caution. Agents often act as ordinary citizens, opinion leaders, community / organization contacts and for this reason they encounter their targets.

Possessing a communicative competence does not only mean knowing the language with which to express oneself, but also requires making one's own the rules of communication as well as the behavioral codes of the host culture. This must allow to produce messages in language in a pragmatic way, that is, having the desired effect; appropriate to the socio-cultural context of reference; and correct from the point of view of the register and formality requested at the given time.

CYB HUMIN' operator must easily adapt to a whole series of social and cultural situations. He must have learned or must be prepared to learn a wider range of behavioral patterns, ready to experiment with different behaviors to identify the most acceptable and effective ones.

Interactions with the target audience must interpret the expressions, intents, perceptions and expectations of the latter, keeping communication active, controlled and balanced. This requires the operator to be able to intervene at any time to investigate the words used, to explain meanings, and so on, and to understand all the signals involved in interaction (verbal and non-verbal).

It must be able to show warmth and attention, ability to generate trust and change behavior, communication style, register. This ability must be accompanied, in correlation with empathy, the ability to create synergy.

CYBER HUMINT

CH is carried out through a team of experts consisting of Case Officers, linguistic personnel and IT (Information Technology).

Within the intelligence cycle, once the target has been determined, the team takes care of the entire preparatory phase of the operation (technical preparation, creation of profiles, etc.) and subsequent exploitation through a real active participation that involves recruitment of sources and / or approach to the target, all rigorously online.

For this reason, the team created ad hoc prepares an operation like the way in which a traditional HUMINT activity is set up.

Particularly important is the technical preparation phase, where all the countermeasures (Virtual Private Networks, Proxies) must be implemented to make the "virtual agent" not attributable to government or military bodies.

The digital cover - under cover activity can be expressed in two ways: in the creation of a server that allows access to fake content of possible interest by an undetermined public, to trace and identify any users as well as in the creation and management of communication areas on networks or telematic systems.

In the latter case, the operational activity consists of the entry, by undercover agents, into real online chats, through fancy nick names, to take part in conversations already in progress between other users or to purpose of initiating communications with an indistinct public. The undercover agent penetrates a "criminal" node - generally not for a single episode but for a time that allows him to gain the trust of an individual or members of a group and to discover the internal logic and dynamics, for which it needs an accurate psychic and cultural preparation, of the creation of a fictitious identity with relative "path".

VIRTUAL PROFILE

Therefore, at the base there is the creation of a profile, which can be assimilated to the equivalent creation of a cover story. This story must be consistent, as must all the traces that must necessarily be released on the web to support it. CYB HUMINT is therefore a full-time activity that, on average, requires several months before it can be implemented via an active profile on the net without creating suspicion, months during which the social profiles must be fed with all the material necessary to outline exactly the characteristics of the "virtual agent". Exceptions are some "spot" activities that do not require solid cover histories but, for example, are used to quickly contact online sources and / or targets.

One of the most important phases of a CYB HUMINT operation is the "evaluation of the reliability of the information and the source", together with the analysis of all the elements examined during the online activity. Assessing the reliability of the information data collected and the source from which it originates, in order to avoid possible misdirection or errors of analysis evaluation that could compromise the success of the operation, is certainly the most delicate phase and a common process for the information cycle in the intelligence sector In fact, any information gathering evidence, before being brought to the attention of the analyst, must necessarily be subjected to an evaluation process aimed at the attribution of a numeric alpha code indicating the degree of reliability and reliability of information and source. This type of evaluation serves to give an added value to the hypothesis formulated in the planning phase of the intelligence operation, since the greater the reliability of the source and the information the more consistent and precise will be the formulated investigative framework.

The possible psychological profile that emerges from the interaction is subsequently evaluated by the analysts, who will indicate how to treat it and what can be expected from interaction with the target. The operative agent is therefore also required to have psychological capacities. It is not easy to create a network of contacts able to ensure a constant flow of information, not only psychological skills are required but also patience, perseverance, perseverance and the additional ability to manage possible conflicts with the source and to be able to manipulate it without make the conditioning evident.

Furthermore, the results of the research activities must allow an analyst to interpret, through other intelligence tools, the intangible, fluid and volatile elements of the antagonistic / subversive and terrorist movements, such as: the sharing of visions and objectives, the sharing of values, the trust, mutual respect.

TECHNOLOGIES

Effective planning and management of collections at all levels allows gathering of large amount of information. Sorting and analyzing information in a timely and efficient manner is essential for operations. To obtain and maintain the domain of information in each operation, the HUMINT team must rely on automation. Automation helps the HUMINT team to quickly report, store, analyze and evaluate the information collected and to provide the supported unit with accurate data in the form of timely, relevant, accurate and predictive information.

It is therefore essential to acquire technologies and methods of automated analysis capable of supporting analysts in their investigative activities in a more adequate and effective manner. The effectiveness of the intelligence prevention activity depends strictly on the collection and analysis of data and information of heterogeneous nature and source.

The quantity of data and information to be processed, with the aim of capturing concrete, detailed and correlated elements, useful to prevent threats and attacks, is consequently destined to grow exponentially. The use of IT systems allows:

- access to information on the web undercover, both on open sources accessible without any type of restriction, and on restricted access sources, which can support the investigator in understanding the organization of future attacks against national companies / infrastructures;

- creation and memorization of different virtual identities configured and used for the undercover activities, maintaining for each of them the attributes and parameters necessary to "correctly" qualify the single identities;

- support relations with subjects with different cultures and languages;

- survey and keep up-to-date the sources of information (web, social networks, chats, etc.), on which the system will allow to perform undercover activities;
- centrally memorize reports and statistics relating to the operation and activities performed through the platform.

PSYCHOLOGICAL CHARACTERISTICS

The Humint operator has the main task of interacting to identify fundamental information elements through the analysis, synthesis and solution of problems inherent in the collection of the same information.

Not everyone is able to carry out this activity, since it is necessary to have a set of basic skills that requires a strong disposition towards interpersonal relationships, managing to be naturally and confidently, appropriately guiding conversations on relevant topics.

The "profile" to operate at best in the specific sector corresponds to highly motivated and technically trained personnel, who are distinguished by the ability to:

- tackle problems of a different nature in heterogeneous contexts;
- work in a team;
- have a strong proactive and implementation drive;
- know how to manage oneself even in critical or pressing situations;
- modulate one's knowledge or behavior based on needs and contingencies, showing oneself flexible and adaptable in the face of new and unexpected situations;
- use the most effective communication style in relation to the goal to be achieved;
- can fit in the shoes of the other, identifying with points of view to create a harmony with the interlocutor;
- dealing with cultures other than one's own, having an open mind, free from prejudices or preconceptions.

It would be desirable for CYB HUMINT to identify turning points in the behavior of "vulnerable" subjects early on, to thoroughly monitor propensities and intercept "weak" signals, precursors of radicalization as well as on the web also in specific physical places such as schools, centers reception areas, places of detention etc, in a logic of prevention of criminal or specifically terrorist phenomena, finally allows to directly grasp the emotional and motivational state of the subjects of intelligence interest.

CONCLUSION

As demonstrated, the identification, recruitment and development of a human source can be done virtually.

Therefore, the effectiveness of intelligence research in cyberspace, precisely due to the intrinsic peculiarities of the digital environment in which they take place (delocalization and dematerialization), also presupposes sophisticated and incisive skills for interaction between intelligence operators - targets, which can only be ensured by activities conducted in covert ways on the electronic communication channels used by individuals or criminal groups.

The greater efficiency of information research activities in the cyber space can be achieved exclusively by carrying out them continuously and for long periods of time, using adequate and consistent coverage identities as well as suitable procedural techniques. These conditions can no longer be delegated to the initiative and solely to the professional skills of the operator, but must necessarily be based on adequate technological support.

Since most of the information of interest is "hidden" in forums and social networks with restricted access, intelligence operators must have a set of tools that allow them to accredit virtual identities, through which log in to the communities of interest.

This instrument requires the ability to identify the possibility of access, cultivate strong bonds, and the ability to influence an individual to act. The online virtual environment can be an important mechanism for the recruitment of virtual sources as many countries have understood, which consider it not only a possibility but a realistic option.

REFERENCES

[1]. Central Intelligence Agency, *Factbook on Intelligence.*

[2]. Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information.*

[3]. Mark W. Lowenthal, *Intelligence: From Secrets to Policy.*

[4]. Marc J. Rosenberg, “Performance technology: Working the system.

[5]. Richards J. Heuer, Jr., *Psychology of Intelligence Analysis.*

[6]. Gannon, John (2001) ‘The Strategic Use of Open-Source Information’, *Studies in Intelligence*, 45(3), pp. 67–71.

[7]. Lyngaas, Sean (2015) 'How (And Why) the CIA Plans to Expand Cyber Capabilities', *Federal Computer Week*, 24 February. https://fcw.com/articles/2015/02/24/cia-expand-cyber.aspx.

[8]. Campbell, Stephen H. (2013) 'Intelligence in the Post-Cold War Period: The Impact of Technology', *The Intelligencer*, 20(1), pp. 57–65.

[9]. Hughes, L. G. (1998). Global Threats and Challenges: The Decades Ahead.

[10]. Gioe D.V. (2017) 'The More Things Change': HUMINT in the Cyber Age. In: Dover R., Dylan H., Goodman M. (eds) The Palgrave Handbook of Security, Risk and Intelligence. Palgrave Macmillan, London.

[11]. Mercado, Stephen C. (2004) 'Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence*, 48(3), pp. 45–55.

[12]. Nader Naghshineh (2008) HUMINT OR WEBINT? Concept Study on Possible Routes for Improving Knowledge Discovery within Organizations, New Review of Information Networking, 14:1

[13]. Sir David Omand, Jamie Bartlett & Carl Miller (2012) Introducing Social Media Intelligence.