CYBERINTELLIGENCE

FROM INTELLIGENCE GATHERING TO CYBER THREAT DETECTION

Antonio VILLALÓN-HUERTA[*]
Ismael RIPOLL-RIPOLL[*]
Héctor MARCO-GISBERT[*]

Abstract:

Intelligence plays a key role in the detection and neutralisation of threat actors in cyberspace, particularly when dealing with advanced ones. However, the relationship between intelligence and the final detection capabilities is not well–defined in most cases. Even the role of information gathering disciplines, which are the basis of intelligence and therefore of cyber intelligence, is confusing and not consensual between authors. In this work we contextualize intelligence gathering disciplines in the cyber intelligence arena. We discuss the role of all of these disciplines in the characterization of advanced threat actors, from the strategic to the tactical views. Once characterization has been performed, we analyse the detection capabilities that intelligence provides, in the form of indicators of compromise, both low–level and behavioural ones. Following this approach, in this work we are defining the road from initial intelligence gathering to threat detection.

Keywords: *Intelligence, Cyber Intelligence, CYBINT, Tactics and Techniques, TTP, Indicators of Compromise*.

Introduction

Advanced Threat Actors are actors with high capabilities (technical, economic, etc.) that perform hostile activities through cyberspace. The threat from these actors is a real fact, as being targeted

[*] Chief Security Officer at S2 Grupo. Valencia, Spain; email: antonio.villalon@s2grupo.es

[*] Assistant Professor at the Department of Computing Engineering, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain; email: iripoll@disca.upv.es

[*] Associate professor and cybersecurity researcher at Department of Computing Engineering, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain; email: hecmargi@disca.upv.es

by one of them is non-discriminatory: every organization with valuable information, every critical operator for basic services and even every single citizen is a potential target. We face two types of advanced threat actors: those linked to nation–states and those linked to criminal gangs. Both of them have the budget, the intent, the time and the capability to perform hostile activities. This is a growing trend that is expected to increase for years: beyond classical operations related to espionage, attack or crime, cyberspace provides threat actors enormous benefits such as accessibility, plausible deniability or geographical offshoring.

Intelligence plays a key role in the detection of hostile cyberspace operations. However, this role is not always well–defined, as in many cases threat analysts focus on pure threat detection mechanisms, not considering the intelligence process nor the threat's features in this detection. As an example, the main *de facto* standard for the characterization of advanced threat actors, MITRE ATT&CK, presents different concept problems in tactics such as Reconnaissance, where elements such as information needs, intelligence gathering and reconnaissance techniques are wrongly mixed.

In this work, we discuss the process that enables threat detection from intelligence gathering. Intelligence as a product turns information gathered, through multiple disciplines, into strategic, operational and tactical intelligence. This intelligence enables the characterization of threat actors, i.e., the identification of the main features of a threat actor or even of a particular operation. Finally, some of these features, the observable ones, are expressed as indicators of compromise, pieces of information that can be used to identify a potentially compromised system.

The main contributions of this work are as follows:

- To discuss the role of intelligence gathering disciplines in cyber intelligence.
- To define the mandatory road map to turn raw information into actionable intelligence.
- To define the main features for the characterization of threat actors.
- To discuss threat actors' detection through observable features.

The rest of the paper is organized as follows. In the next section we present the main concepts related to intelligence, intelligence gathering disciplines and cyber intelligence, later discussed in this work. Next, we discuss the process from intelligence to threat detection. Starting with intelligence gathering, we delve into threat actors' characterization to end with threat actor's detection, which is the final goal of the intelligence: enabling the detection and response capabilities to neutralize the threat. Finally, in the last section we present the main conclusions of our work.

Background

Intelligence. NATO (Office, 2018) defines intelligence as "the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision–makers". The same work also defines the intelligence cycle as "the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users". The intelligence cycle as exposed in Staff (2013) is shown in figure one (fig. 1). There are different versions of this cycle, and their alternatives and key differences have been discussed in different works (Hulnick, 2006; Phythian, 2013; Mocanu, 2015) provides key differences between relevant models. However, we can summarize its approach by considering the following five steps:

- Direction. "Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies."
- Collection. "The exploitation of sources by collection agencies and the delivery of the data obtained to the appropriate processing unit for use in the production of intelligence."
- Processing. "The conversion of data into usable information suitable for analysis."
- Analysis. "Integration, evaluation, interpretation etc. of information to turn it into intelligence."

- Dissemination. “The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it.”

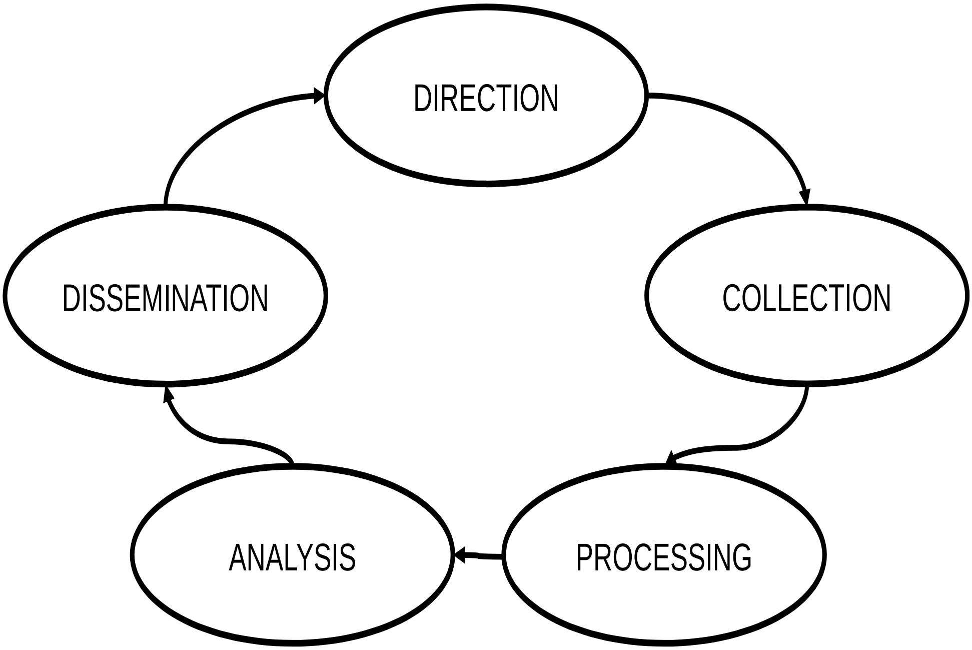

Figure 1: Intelligence Cycle (Source: Authors’ view)[1]

Ackoff (1989) and Liew (2007 and 2013) provide precise definitions of data, information and intelligence. Madureira et al. (2021) identify intelligence as a product as one of the five dimensions of intelligence; it is the final result of the intelligence cycle (Bimfort, 2007). The intelligence cycle is a simple explanation of a complex process; intelligence as a process is is also a key dimension of intelligence (Madureira et al., 2021). In Villalón-Huerta et al. (2022) we stated that it starts “when someone (an authority, a government, etc.) has particular intelligence needs in order to make the best decision about a particular subject”. When dealing with government intelligence, this subject is usually relevant for national

[1] Authors’ view previously published in Villalón-Huerta et al. (2022).

security. At this point the cycle starts first by identifying the requirements and planning the acquisition of the information to be processed and analyzed, in order to generate intelligence.

"Once planned, the next stage is to acquire information, and this acquisition can be performed through different intelligence collection disciplines" (Boury-Brisset et al., 2011) commonly referred as "the INTs" (Villalón-Huerta et al., 2022); "the essential elements of these INTs are not formally defined" (Clark and Oleson, 2018), nor are them consensual "between authors, but they define the families of sources the information can be gathered from: a simple public website, a satellite, an intercepted artifact, a mole etc." These intelligence collection disciplines are discussed in next section.

Once data has been gathered, processing turns it into "a form suitable for the production of finished intelligence" (Richelson, 2018). This stage includes tasks such as decryption, translation or data conversion. As a part of the cycle, it is mandatory to the next one: analysis, in which the intelligence, the final product, is generated. This analysis must include the information gathered and processed no matter which collection discipline it comes from. In this sense, we can refer to all–source intelligence, defined by Army (2004) as "the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence."

"Finally, once the intelligence as a product has been generated, it is delivered to and used by the customer, the entity which had the information needs stated before, in a suitable form for its use and by a variety of means. This product will be used to help the decision-making process and, possibly, to start a new iteration of the intelligence cycle." (Villalón-Huerta et al., 2022) After the product is disseminated and consumed, different intelligence needs, and additional information or new tasks can be arised (Bartes, 2013).

Intelligence gathering disciplines. As stated before, intelligence collection disciplines are not consensual between authors, so they motivate different discussions. There are five commonly accepted disciplines by the US Intelligence Community (Lowenthal, 2019;

Lowenthal and Clark, 2016; Phythian, 2013; Clark and Oleson, 2016): geospatial (formerly imagery) intelligence (GEOINT), signals intelligence (SIGINT), measurement and signatures intelligence (MASINT) – which includes technical intelligence or TECHINT –, human intelligence (HUMINT) and open source intelligence (OSINT).

"IMINT is defined as the technical, geographic, and intelligence derived through the interpretation or analysis of imagery and collateral material" (Cardillo, 2018), and it is considered inside GEOINT in some works (Randol, 2010; Clark and Oleson, 2018), although it is also considered as an independent discipline in many others (Goldman, 2015; Carlisle, 2015). Most references seem to consider GEOINT as the integration of imagery, IMINT, and geospatial information (Defense, 2017; Cardillo, 2018), so we will deal with GEOINT as a global discipline comprising IMINT. It is important to note that there is no collection system that gathers data from GEOINT (Clark, 2013): geospatial information is collected via IMINT, OSINT, SIGINT, HUMINT or MASINT.

The role of TECHINT, intelligence gathered from the collection, processing, analysis and exploitation of data and information pertaining to foreign equipment and materiel (Bautista, 2018), is much more discussed. It is considered inside MASINT by the references which identify only five main disciplines and by specific military works (US Air Force, 2021; North Atlantic Treaty Organization, 2022). However, it is considered a discipline by itself in different references (Carlisle, 2015; D. E. Johnson and Howard, 2012). Other works identify TECHINT as all intelligence gathered from technical sources – vs. human sources –, (Guliyev, 2010; Shulsky and Schmitt, 2002; Crosston and Valli, 2017; L. K. Johnson, 2017). Finally, some authors, such as (Herman, 1996), differentiate between main and smaller sources for intelligence gathering disciplines. These smaller sources (for example, NUCINT, Nuclear Intelligence) are referred as secondary sources, as the term "small" does not properly describe the meaning of this category. Saunders (2000) makes a discussion about those disciplines and their consideration. In addition to these differences, there have been also some efforts to add new intelligence collection disciplines to the list, such as those proposals in (Taylor, 2007; Faint, 2011; Arslan and Yanık, 2015), generating even more confusion into the community.

In this work we will not enter into the discussion about which disciplines have to be considered: we will simply deal with the five generally–accepted disciplines. We will include TECHINT inside the MASINT discipline and, in the same way, we will include IMINT inside GEOINT, in order to highlight that imagery intelligence plays a key role in the cyber battle space (much more than GEOINT, as cyber is a domain of conflict not directly related to GEO in many cases). In summary, we are considering the following five disciplines, without detailing subcategories for the purpose of this work:

- Human Intelligence (HUMINT). Intelligence collected and provided from human sources (Staff, 2013).
- Geospatial Intelligence (GEOINT). Intelligence gathered from geospatial data through the application of geospatial techniques and by skilled interpretation, in which the location and movement of activities, events, features and people play a key role (Council, Committee, et al. 2006).
- Measurement and Signature Intelligence (MASINT). Technically derived intelligence that "enables detection, location, tracking, identification and description of unique characteristics of fixed and dynamic target sources" (Lowenthal and Clark, 2015). As stated, it includes TECHINT, intelligence gathered "from the collection, processing, analysis and exploitation of data and information pertaining to foreign equipment and materiel" (Bautista, 2018).
- Signals Intelligence (SIGINT). Intelligence produced by "exploiting foreign communications systems and non-communications emitters" (Staff, 2013), which comprises three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).
- Open-Source Intelligence (OSINT). Intelligence gathered from publicly available information that is "collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Williams and Blum, 2018).

Cyber intelligence

Cyber Intelligence, CYINT or CYBINT, is intelligence related to cyberspace, a concept that has no single definition. While HUMINT is considered as intelligence from human sources, CYBINT cannot be the equivalent, intelligence from cyberspace; the term is generally "used to convey the idea of widely scoped and better qualified knowledge of actual or potential events regarding cyberspace that may endanger an organization" (Bonfanti, 2018). CYBINT cannot be considered as a collection discipline, but an analytic one: this is, with its focus on the analysis stage of the intelligence cycle, relying on data collected from the gathering disciplines stated before (Alsmadi, 2019; Seedyk, 2018): SIGINT, HUMINT, MASINT, OSINT and GEOINT.

In 2011 Intelligence and National Security Alliance (INSA) published (Fast et al., 2011) the first formal and high-level approach to the "emerging discipline" of CYBINT, providing a "framework to approach the development of intelligence in the cyber domain" and stating it as a new discipline in the US Intelligence Community, but without providing an accurate definition of the term. The same year some authors stated the earliest definitions of cyber intelligence, referred to it as "the process of obtaining specific types of valuable information and knowledge through the Internet" (Petratos, 2011) or "collecting, relating, analysing, and reporting information about a topic, an organization or a person, from sources available on the internet and other open sources" (Tekes, 2011). These initial definitions make a clear reference to intelligence gathered from Internet, and have been superseded during the decade with more accurate terms that better fit the concept that today we have of the term.

With the early concept of intelligence from Internet, in 2012 (Hurley, 2012) started a discussion about what CYBINT is, differentiating "from" and "for" cyber, "depending on the scope of the information gathering activities, the means employed to carry them out and their final goal". Bonfanti (2018) states that intelligence "from" is "knowledge produced through the analysis of any valuable information collected within or through cyberspace", while intelligence "for" refers to capabilities to enable cyberspace operations regardless of the source, method or medium: this is, different collection disciplines providing valuable intelligence to these operations.

In 2013, Bamford et al. stated that CYBINT "should not be limited to an understanding of network operations and activities, but should include the collection and analysis of information that produces timely reporting, with context and relevance to a supported decision maker" (Bamford et al., 2013). Although yet undefined, what was clear is that the term refers to a "multifaceted approach to framing, thinking about, and reacting to cyber adversarial activity", not only regarding intelligence from cyber space.

Although still nowadays there is no consensus about a formal CYBINT definition (relevant discussions can be found at Kandiko, 2018; Seedyk, 2018; Bonfanti, 2018), one useful and simple approach was proposed in (Townsend et al., 2013), which states CYBINT as the acquisition and analysis of information "to identify, track, and predict cyber capabilities, intentions, and activities that offer courses" of action to enhance decision making. This definition fits well in what is usually understood as CYBINT by security product vendors and services providers, as the product derived from the analytic discipline, focusing in cyber intelligence for cyberspace but also including intelligence gathered from cyberspace, as long as it is useful for cyber activities. In fact, when we refer to intelligence gathered from cyberspace to satisfy information needs outside this battlefield, we could simply refer to classical collection disciplines. For the purpose of this work, we will be using this definition.

In addition to CYBINT, a term that is usually used among the information security community is Cyber Threat Intelligence, or CTI, first defined (McMillan, 2013) as "evidence–based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." In other words, CTI focuses (Coats, 2019) on all source intelligence on threats: programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, potential impacts, infrastructure and data, characterization and structures. The term is used without the cyber prefix – this is, Threat Intelligence or TI –, and its goal is (Conti et al., 2018) "to help organizations in recognizing the indicators of cyber attacks, extracting information about the attack methods, and consequently responding to the attack accurately and in a timely manner." CTI can be considered as a subset of CYBINT: CYBINT includes CTI, but CTI does not represent all of CYBINT (Ettinger, 2019). While CTI focuses on the single analysis of threats, cyber intelligence includes this analysis, but also analysis of areas such as geopolitics, military or diplomacy; CTI, from its definition to its goal or its components, focuses on threats, not in their external context.

In intelligence, including CYBINT and CTI, it is possible to identify different levels to deal with; in fact, it is possible to identify these levels in all intelligence–related activities. Each of these levels refers to intelligence with a specific goal, time of life, type of product etc. They are defined as follows (Bamford et al., 2013; Joint Chiefs of Staff, 2010; Abu et al., 2018):

- Strategic. Level at which an actor determines global strategic security objectives and guidance, and develops and uses resources to achieve these objectives. In the cyber domain, strategic intelligence provides knowledge to understand threats and risks at a senior management level: main actors and their motivations, victims and their relations, links to geopolitical events, etc. The final product is usually in the form of written reports with a long lifetime and a non–technical approach, about who and why.
- Operational. "Level at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas." (Bamford et al., 2013; Joint Chiefs of Staff, 2010; Abu et al., 2018) In the cyber domain, operational intelligence provides knowledge about the context and trends of past incidents (Meeuwenberg, 2017): tactics, techniques, patterns, actor profiles, etc. The final product is in the form of short written reports with a medium lifetime, about how and where.
- Tactical. "Level at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces." (Bamford et al. 2013; Joint Chiefs of Staff, 2010; Abu et al. 2018) This is the most basic form of intelligence, and in the cyber domain it provides knowledge about

the identification of threats targeting the infrastructure in the form of hashes, IP addresses, domains or detection rules. The final product is in the form of atomic indicators in a machine–readable format, such as Yara rules, IDS signatures or blacklists, suitable to load them in different security devices. Tactical intelligence has a short lifetime and tries to answer what is happening or what is to happen in short term.

These levels, and their associated products, are shown in figure 2. Other works (Sari, 2018; Mutemwa et al., 2017; Leszczyna and Wróbel, 2019) change the definitions and layers of tactical and operational levels of intelligence, while studies such as (Noor et al., 2018) include a fourth level, called technical, at the lowest part of the heap.

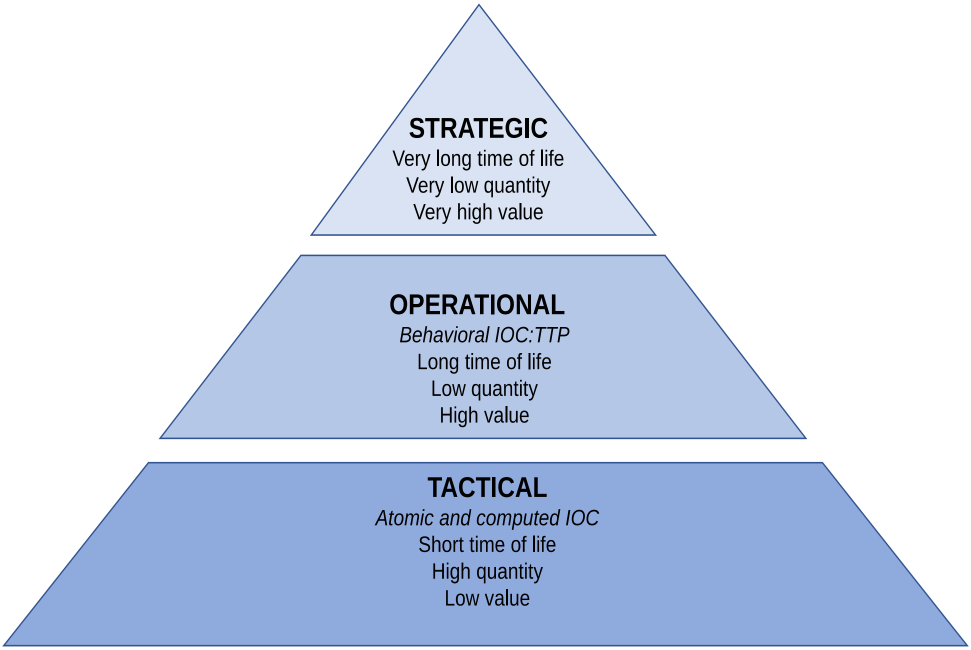

Figure 2: Intelligence levels (Source: Authors' view)[2]

[2] Authors' view previously published in Villalón-Huerta et al. (2022).

From intelligence gathering to threat detection

In this section we discuss the process that turns information into actionable intelligence. We divide it into three parts. The first one gathers information to identify the main features of an operation. Second part refers the characterization of threat actors and their operations, through the previously generated intelligence. Finally, third part is related to threat detection and specifies, when possible, the extracted features to turn them into actionable intelligence. This process is summarized in figure three (fig. 3).

The detection and the later analysis of an offensive cyberspace operation can be performed through all of the intelligence gathering disciplines we have exposed in section "Intelligence gathering disciplines", from SIGINT to OSINT. All these disciplines are relevant to identify features of an operation, from the strategical to the tactical ones. In this way, they all are helpful to characterize the operation. Through this characterization, they all allow the detection of hostile activities, especially through operational and tactical intelligence. Both intelligence types are specified as actionable indicators of compromise (low level ones, atomic and computed, and behavioural ones, tactics and techniques).

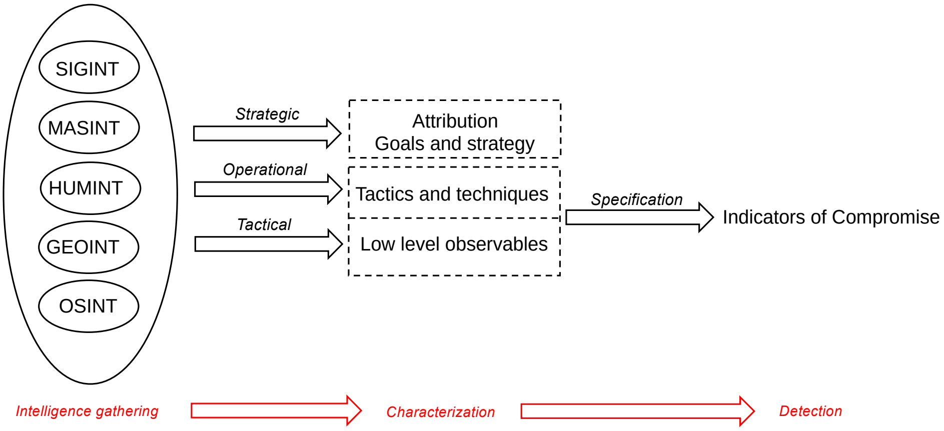

Figure 3: The role of information gathering disciplines in threat detection (Source: Authors' view)

Intelligence gathering

Although intelligence gathering disciplines are relevant for cyber intelligence, not all of them have the same weight on the detection equation. The main intelligence gathering discipline in cyber intelligence is SIGINT, recognized as the primary driver for operations within the cyberspace operating environment (Franz et al. 2019; Oakley, 2019). In fact, many of the services or units historically focused on SIGINT activities are nowadays tasked with cyber operations, such as US National Security Agency, NSA, (Loleski, 2019; Kris, 2021), UK Government Communications Headquarters, GCHQ, (Aldrich, 2021) or Israel Defence Forces Unit 8200 (Cordey, 2019). Cyberspace has become the main way to communicate, and interception and gathering of network signals muddies the traditional notion of SIGINT (Richards, 2014). Most detection approaches are based nowadays on SIGINT capabilities: this is, on the detection of anomalous activities in one's own infrastructure, through the monitoring of systems and networks. SIGINT provides tactics, techniques and procedures of implants communicating laterally and externally (command and control and exfiltration), as well as the relevant atomic indicators regarding these communications.

MASINT, specifically TECHINT, plays also a key role in the cyberspace domain. In the kinetic sphere, TECHINT refers to the collection and analysis of adversary's equipment and materiel; in cyberspace, media and software, particularly malware (Fanelli, 2015), are the equivalent to this equipment and materiel. Through disciplines such as malware analysis and forensic analysis, TECHINT provides relevant information not only in the tactical level, but also in the operational and strategical, from the most technical indicators of compromise to aspects such as an adversary's budget or interest in its target (Richmond, 2011; Porche III et al. 2011).

HUMINT remains fundamental for understanding threats' capabilities and intentions (Gioe, 2017) in cyberspace, not being replaced by any of the other acquisition disciplines. While these ones provide vast volumes of intelligence, human sources provide excellent – not vast, but excellent – information about adversaries. It is particularly relevant the interest of different services in deploying cover HUMINT capabilities targeting units in hostile services or telecommunications industries – GCHQ Human Operations Team, HOT, is an example (Duvenage and Solms, 2014). In addition, overt capabilities among interest groups to get effective information sharing regarding cyber capabilities, interests or activities of potential adversaries is also a particularly relevant element for HUMINT approaches (Brown, Gommers, and Serrano, 2015). An example of an overt cyber intelligence sharing effort is the European Government CERT (EGC) group (Ilves et al., 2016).

OSINT is also a big player in cyber intelligence. Although it is difficult to identify very targeted attacks through open-source intelligence, OSINT provides useful information about general trends that could be relevant to intelligence analysis. In fact, most cyber intelligence shared nowadays is on the form of threat intelligence feeds and private intelligence reports regarding advanced threat actors; both of these examples must be considered OSINT. As in intelligence not related to cyberspace, from an analytic perspective one of the main problems to face in OSINT is the reliability of the source where information is gathered from (Steele, 2007; Gong et al., 2018). Although different analysis on the quality of intelligence feeds is available (Meier et al., 2018; Li et al., 2019; Griffioen et al., 2020), we identify this as a relevant problem in cyber intelligence. In addition to threat intelligence feeds, the monitoring, analysis and research of information coming from the Internet (Lande and Shnurko-Tabakova, 2019) is a must, so a global monitoring schema must include open-source monitoring for the tracking of adversarial capabilities: this is, OSINT.

Finally, GEOINT related to cyber is clear in military operations: Army (2010) states that "cyberspace can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona)." The lowest of these three layers, the physical one, includes the geographic component, referring to the physical location of elements of the network and denoting a physical aspect tied to the rest of components. It is commonly accepted that information cannot exist without a physical infrastructure to support it. Cyberspace has been created as a domain by this infrastructure and has a relevant geospatial component (Taneski et al., 2019). For this reason, there have been some efforts to "visualize" cyber using intelligence fusion and GEOINT techniques, trying to connect the "bits and the bytes" with the "bricks and mortar" (Price, 2014). To ensure this connection it is mandatory to geolocate network activity, tracking actions in both network time and space (Franz et al., 2019) towards cyber-physical spatialization in order to detect hostile operations. Relevant geolocations have been shown during armed conflicts (Higgins 2016; McCrory, 2020), as examples of all-source intelligence.

As we have stated before, all information gathering disciplines are relevant for the characterization, and further detection and analysis, of hostile activities. Although GEOINT is the less exploited one, all of them can provide strategical, operational and tactical intelligence. For this reason, an accurate security approach must consider all of them, not only for pure detection but for the whole analysis and modelling of the threat actors' activities and interests. In fact, the mix of different intelligence acquisition disciplines is common in real world operations (Oakley, 2019): we return to the all–source intelligence concept. All of these disciplines provide the mandatory intelligence for the characterization of threat actors and their activities, thus all of them can enable the detection of hostile activities in our infrastructures, as we have summarized in figure three (fig. 3).

Threat characterization

The characterization of threat actors is the recognition and analysis of its features, in order to identify their attribution, goals and strategies, tactics and techniques and tools and artifacts. Although this characterization can be performed through all the intelligence gathering disciplines, SIGINT and TECHINT are the most relevant ones in most cases, as the characterization usually starts by direct observables that are turned into indicators of compromise. However, to discuss the whole characterization of threat actors, we must consider both direct observables and non–observable elements, such as goals, strategy and even attribution. As these ones are not directly seen in an operation, they must be inferred from an intelligence analysis, apart from the purely technical aspects of the operation. This analysis, outside of the scope of this work, will infer, with an associated probability, why a threat actor is conducting a hostile operation against a particular target. The identification of goals, strategies and attribution provides valuable information to establish tailored security countermeasures to face specific threat actors.

In table one we summarize the main families of features regarding threat actors. We must differentiate between observable features (those that can be directly seen on an operation) and non–observables ones (those that are not directly seen, so they must be inferred or acquired by external intelligence). Low–level observables are linked to tactical intelligence and tactics, techniques and procedures (TTP) are linked to operational intelligence. Both of them can be expressed in the form of indicators of compromise, as we will discuss in next section. On the other hand, non–observables are mostly linked to strategical intelligence. It is important to highlight that when we refer to observable features, not all of them can be observed through cyberspace, but they can be gathered through different intelligence gathering disciplines. As we have stated, all of them are relevant for an accurate characterization of a threat actor, although strategical intelligence is rarely actionable.

Table 1: Threat actors' features (Source: Authors' view)

Non–observables	Attribution
	Goals and strategy
Observables	TTP
	Low–level indicators

Threat characterization starts with low–level observables and ends with the attribution, one of the main relevant problems that threat intelligence analysts face nowadays. All of the discussed features are important to the whole characterization of a threat actor, from its arsenal to its interests. However, we defend that the characterization of advanced threat actors must be mainly approached by the analysis of their tactics and techniques. They are the most valuable observables in the context of a cyberspace operation. This value is linked to the fact that lower level observables, such as atomic indicators of compromise, or even tools or artifacts, are easily modified by an actor, so their value is limited. On the other hand, characteristics such as goals and strategies, or even attribution, are not direct observables in a hostile operation and in most cases, they must be inferred from the operational and tactical levels, where observables are usually found. In table 2 a brief description of TTP is provided.

Table 2: Threat actors' features (Source: Authors' view)

Tactics	The employment and ordered arrangement of forces in relation to each other.
Techniques	Non–prescriptive ways or methods used to perform missions, functions, or tasks.
Procedures	Standard, detailed steps that prescribe how to perform specific tasks.

Tactics represent what a threat actor is doing at the highest level of description, to accomplish a certain mission. In literature, they have been structured in frameworks such as MITRE ATT&CK (Strom et al., 2017; Xiong et al., 2022), in different kill–chain models such as the Cyber Kill Chain (Hutchins et al. 2011) and in models such as The Cyber Diamond Model (Al-Mohannadi et al., 2016). Techniques specify how a tactic is implemented. From an intelligence point of view, their value is very high for the characterization of a threat actor, as well as for its detection. Finally, procedures are particular implementations of a given technique, linked to specific threat actors of even operators. Being so particular is not useful for the detection of an offensive cyberspace operation, as in general terms they do not provide relevant information that is not provided by their superior techniques, so they are out of the scope of this work.

Tactics and techniques, operational intelligence, describe the modus operandi of a threat actor and they are a key element for its characterization, as they are not easily modified. To be effective, tactics and techniques must be represented in a machine-readable format that can be loaded into security devices and automatically provide accurate results. We consider this is one of the biggest challenges we must face today. Common formats and languages have been developed in order to allow this specification and the sharing of tactics and techniques in the form of actionable intelligence. However, the lack of a common standard is a current problem, as most of these formats are vendor–dependent. Without such a common standard, actionable intelligence is based nowadays mostly in atomic and computed indicators of compromise, easy to consume but with a very short time of life. This fact opens a window of opportunity for threat actors, as low–level indicators of compromise are easy to evade.

Threat detection

Once threats have been characterized by the identification of their main features, these features must be exploited to detect hostile activities in a compromised infrastructure. This detection is carried through Indicators of Compromise (IOC), the specification of observable features in order to search their presence in an infrastructure. IOC are defined (Harrington, 2013) as a piece of "information that can be used to identify a potentially compromised system". They play a key role in Cyber Threat Intelligence, as they enable and accelerate the detection of hostile activities in targeted infrastructures. IOC allow the specification both of the usage of "technological capabilities, such as tools or artifacts, and of the tactics, techniques and procedures developed by threat actors."

IOC can be classified into three categories (Cloppert, 2009; Hutchins et al., 2011): atomic, computed and behavioural. The first two types are considered low–level IOC and they are linked to tactical intelligence. Examples of such indicators are IP addresses, file hashes or malicious domain names. Behavioural indicators represent the tactics and techniques of threat actors, and they are linked to operational intelligence. All of them are relevant to detect compromises, but tactical intelligence has a shorter lifetime than operational intelligence, and it can also be more easily evaded, so it is less useful in general terms.

Being SIGINT, the main information gathering discipline for the detection of hostile activities, most of the current approaches to this detection rely on the specification and sharing of atomic and computed indicators of compromise. As stated, these indicators have a limited value and time of life, as they are easily modified by threat actors. For an effective detection capability, it is mandatory to work at the operational intelligence level, this is, the one related to tactics, techniques and procedures: behavioural indicators of compromise. For this reason, we defend that the specification of tactics and techniques is a key element for threat detection.

However, it is known that not all detection is based on indicators of compromise. In this sense, threat hunting is defined (Shu et al., 2018) as "the process of proactively and iteratively formulating and validating threat hypotheses based on security relevant observations and domain knowledge." Threat hunters acquire relevant information from the infrastructure, such as network traffic or endpoint activity, and they analyse this information to formulate and validate hypotheses. This process is an intelligence activity, specifically a SIGINT one. It gathers signals information, analyse it to identify hypotheses, in the form of observables, both low–level and behavioural ones, and validates these hypotheses. If they are valid ones, observables are specified and their search is automated.

In addition to the exploitation of indicators of compromise or threat hunting activities, intelligence sharing, as a dissemination approach, must also be particularly considered in an effective detection scheme. Intelligence sharing, from strategical to tactical, is a must for threat detection, as in most cases we face global threats and there is a consensus that no intelligence actor can successfully act alone (Kalkman and Wieskamp, 2019). Collaboration between organizations is a key point to prevent, to detect and to neutralize threats. As an example, we can refer to formalized CERT groups such as FIRST or TF-CSIRT (Kossakowski, 2019), US ISAC (McCarthy et al., 2014) or UK WARP (Proctor, 2011). Intelligence must be shared among a community, a group of trusted stakeholders who work together to address shared threats or vulnerabilities (Willis, 2012), usually with common interests; the formalized groups referenced below are examples of communities. Inside each type of community, elements such as the trust model or the sharing intelligence policy define how intelligence is shared.

Information shared must meet three requirements to be considered valid threat intelligence (Dalziel, 2014): it must be relevant, actionable and valuable. As we have stated, most shared intelligence is in the form of low-level data (Pawlinski et al., 2014), especially atomic indicators (Sauerwein et al., 2017): this is, a very tactical approach that focuses on elements such as malicious IP addresses, DNS domains or URL. Operational and strategical intelligence are much less shared, although they are more valuable than tactical one.

Finally, to share intelligence, it is mandatory to establish exchange mechanisms over a technological platform that can be deployed in many forms such as centralized or peer to peer. Sauerwein et al. (2017) states that there is no common definition of threat intelligence sharing platforms, being most of them focused on the exchange of tactical intelligence in STIX format. In fact, what we call threat intelligence sharing platforms, such as MISP, are focused on this kind of tactical intelligence, but are not usually suitable for strategic intelligence sharing.

Conclusions

As we have stated in this work, intelligence plays a key role in the detection of offensive cyberspace operations. However, it is not always clear how intelligence must be applied to the characterization of advanced threat actors and to the detection of their operations. In this paper we have discussed the process that turns raw information into valuable actionable intelligence to detect hostile operations. Through the application of all intelligence gathering disciplines, information is acquired, processed and analysed to identify the main features of threat actors or of their operations. This intelligence can be exploited at strategical, operational and tactical levels: all of them are relevant in the cyberspace arena, and all of them can be obtained from each of the intelligence gathering disciplines.

The identified features that characterize a threat actor can be divided into observable and non–observable ones. As their name implies, observable features can be directly seen on the targeted infrastructure, while non–observable ones must be inferred. Observable features are particularly relevant for the detection of advanced threat actors. They can be expressed as indicators of compromise, defined as pieces of information that can be used to identify a potentially compromised system. These indicators are actionable intelligence that enables and accelerates the detection of hostile activities in targeted infrastructures. Particularly, operational intelligence, in the form of behavioural indicators of compromise, is a must for an accurate detection capability. In this way, the path from raw information to actionable intelligence is defined. We defend that threat detection must be based on the result of intelligence acquisition and analysis, and on the further characterization of advanced threat actors. With this structured approach, intelligence-driven threat detection can be performed and, which is most important, enhanced over time.

Reference:

1. Abu, Md Sahrom, Siti Rahayu Selamat, Aswami Ariffin, and Robiah Yusof. (2018). "Cyber Threat Intelligence – Issue and Challenges." *Indonesian Journal of Electrical Engineering and Computer Science* 10 (1): 371-379.

2. Ackoff, R. L. (1989). From data to wisdom. *Journal of applied systems analysis*, 16(1), 3-9.

3. Aldrich, Richard J. (2021). "From Sigint to Cyber: A Hundred Years of Britain's Biggest Intelligence Agency." *Intelligence and National Security,* 36 (6): 910-917.

4. Alsmadi, Izzat. (2019). "Cyber Intelligence Analysis." In *The NICE Cyber Security Framework*, 91-134. Springer.

5. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW): 69-76.

6. Army, US. (2004). "Field Manual 2-0 Intelligence." US Department of the Army.

7. Army, US. (2010). "TRADOC Pamphlet 525-7-8. Cyberspace Operations Concept Capability Plan 2016-2028." United States Army.

8. Arslan, C, and M Yanık. (2015). "A New Discipline of Intelligence: Social Media." *Military and Security Studies*, 69.

9. Bamford, George, John Felker, and Troy Mattern. (2013). "Operational Levels of Cyber Intelligence." *Cyber Intelligence Task Force, Intelligence and National Security Alliance*.

10. Bartes, F. (2013). Five-phase model of the intelligence cycle of competitive intelligence. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 61(2), 283-288.

11. Bautista, Wilson. (2018). *Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Incidents*. Packt Publishing Ltd.

12. Bimfort, M. T. (2007). A definition of intelligence. Studies in Intelligence, 2.

13. Bonfanti, Matteo E. (2018). "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice." *Cyber, Intelligence, and Security* 2 (1): 105-121.

14. Villalón-Huerta, A., Ripoll-Ripoll, I, and Marco-Gisbert, H. (2022). "Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise", *Electronics*, Volume 11, Issue 3, 2022, 416.

15. Boury-Brisset, Anne-Claire, Anissa Frini, and Réjean Lebrun. (2011). "All-Source Information Management and Integration for Improved Collective Intelligence Production." Defence Research; Development Canada Valcartier (Quebec).

16. Brown, Sarah, Joep Gommers, and Oscar Serrano. (2015). "From Cyber Security Information Sharing to Threat Management." In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43-49.

17. Cardillo, Robert. (2018). "Geospatial Intelligence (GEOINT) Basic Doctrine." National System for Geospatial Intelligence.

18. Carlisle, Rodney. (2015). *Encyclopedia of Intelligence and Counterintelligence*. Routledge.

19. Clark, Robert M. 2013. "Perspectives on Intelligence Collection." *Journal of U.S. Intelligence Studies* 20 (2): 47-53.

20. Clark, Robert M., and Peter C. Oleson. (2016). "Intelligence in Public Literature." *Studies in Intelligence* 60 (1): 81–96.

21. Clark, Robert M., and Peter C. Oleson. (2018). "Cyber Intelligence." *Journal of U.S. Intelligence Studies* 24 (3): 11-23.

22. Cloppert, Mike. (2009). "Security Intelligence: Attacking the Cyber Kill Chain." *SANS Computer Forensics* 26.

23. Coats, Daniel R. (2019). "National Intelligence Strategy of the United States of America 2019." *Office of the Director of National Intelligence, Washington, DC*.

24. Conti, Mauro, Tooska Dargahi, and Ali Dehghantanha. (2018). "Cyber Threat Intelligence: Challenges and Opportunities." In *Cyber Threat Intelligence*, 1-6. Springer.

25. Cordey, Sean. (2019). "The Israeli Unit 8200–an OSINT-Based Study: Trend Analysis." ETH Zurich.

26. Council, National Research, Mapping Science Committee, et al. (2006). *Priorities for GEOINT Research at the National Geospatial-Intelligence Agency*. National Academies Press.

27. Crosston, Matthew, and Frank Valli. (2017). "An Intelligence Civil War: HUMINT Vs. TECHINT." *Cyber, Intelligence, and Security* 1 (1): 67-82.

28. Dalziel, Henry. (2014). *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Syngress.

29. Defense, US Department of. (2017). "Joint Publication 2-03. Geospatial Intelligence in Joint Operations." US Department of Defense.

30. Duvenage, Petrus, and Sebastian von Solms. (2014). "Putting Counterintelligence in Cyber Counterintelligence: Back to the Future." In *13th European Conference on Cyber Warfare and Security ECCWS-2014 the University of Piraeus Piraeus, Greece*, 70.

31. Ettinger, Jared. (2019). "Cyber Intelligence Tradecraft Report. The State of Cyber Intelligence Practices in the United States." Carnegie–Mellon University. Software Engineering Institute.

32. Faint, Charles D. (2011). "Exploitation Intelligence (EXINT) a New Intelligence Discipline?". *American Intelligence Journal* 29 (1): 65-69.

33. Fanelli, R. (2015). "On the Role of Malware Analysis for Technical Intelligence in Active Cyber Defense." *Journal of Information Warfare* 14 (2): 69-81.

34. Fast, Barbara, Michael Johnson, and Dick Schaeffer. (2011). "Cyber Intelligence. Setting the Landscape for an Emerging Discipline." *Cyber Intelligence Task Force, Intelligence and National Security Alliance*.

35. Franz, George, Galen Kane, and Jeff Fair. (2019). "Reshaping Intelligence Operations in the Cyberspace Domain." *The Cyber Defense Review* 4 (1): 33-40.

36. Gioe, David V. (2017). "'The More Things Change': HUMINT in the Cyber Age." In *The Palgrave Handbook of Security, Risk and Intelligence*, 213-227. Springer.

37. Goldman, Jan. (2015). *The Central Intelligence Agency: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies [2 Volumes]: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies*. ABC-CLIO.

38. Gong, Seonghyeon, Jaeik Cho, and Changhoon Lee. (2018). "A Reliability Comparison Method for OSINT Validity Analysis." *IEEE Transactions on Industrial Informatics* 14 (12): 5428-5435.

39. Griffioen, Harm, Tim Booij, and Christian Doerr. (2020). "Quality Evaluation of Cyber Threat Intelligence Feeds." In *International Conference on Applied Cryptography and Network Security*, 277-296. Springer.

40. Guliyev, Fuad. (2010). "National Intelligence Estimate. The Outlook for Intelligence Collection." *Journal of Azerbaijani Studies*.

41. Harrington, Chris. (2013). "Sharing Indicators of Compromise: An Overview of Standards and Formats." *EMC Critical Incident Response Center*.

42. Herman, Michael. (1996). *Intelligence Power in Peace and War*. Cambridge University Press.

43. Higgins, Eliot. (2016). "A New Age of Open Source Investigation: International Examples." In *Open Source Intelligence Investigation*, 189-196. Springer.

44. Hulnick, A. S. (2006). What's wrong with the Intelligence Cycle. Intelligence and national Security, 21(6), 959-979.

45. Hurley, Matthew M. (2012). "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance." *Air and Space Power Journal* 26 (6): 12-33.

46. Hutchins, Eric M, Michael J Cloppert, and Rohan M Amin. (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (1): 80.

47. Ilves, Luukas K, Timothy J Evans, Frank J Cilluffo, and Alec A Nadeau. (2016). "European Union and Nato Global Cybersecurity Challenges." *Prism* 6 (2): 126-141.

48. Johnson, David EA, and Newton Howard. (2012). "Network Intelligence: An Emerging Discipline." In *2012 European Intelligence and Security Informatics Conference*, 287-288. IEEE.

49. Johnson, Loch K. (2017). *National Security Intelligence*. John Wiley & Sons.

50. Joint Chiefs of Staff. (2010). *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms*. Department of Defense.

51. Kalkman, Jori Pascal, and Lotte Wieskamp. (2019). "Cyber Intelligence Networks: A Typology." *The International Journal of Intelligence, Security, and Public Affairs* 21 (1): 4–24.

52. Kandiko, Ulises Leon. (2018). "Cyber Intelligence: Reinventing the Wheel." *Triarius. Prevention and Security Bulletin on Terrorism and the New Threats* 2: 27.

53. Kossakowski, Klaus-Peter. (2019). "Computer Security Incident Response Team (CSIRT) Services Framework." FIRST.

54. Kris, David S. (2021). "The NSA's New SIGINT Annex." *Journal of National Security Law & Policy*.

55. Lande, Dmytro, and Ellina Shnurko-Tabakova. (2019). "OSINT as a Part of Cyber Defense System." *Theoretical and Applied Cybersecurity* 1 (1).

56. Leszczyna, Rafał, and Michał R Wróbel. (2019). "Threat Intelligence Platform for the Energy Sector." *Software: Practice and Experience* 49 (8): 1225-1254.

57. Li, Vector Guo, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. (2019). "Reading the Tea Leaves: A Comparative

Analysis of Threat Intelligence." In *28th USENIX Security Symposium (USENIX Security 19)*, 851-867.

58. Liew, A. (2007). Understanding data, information, knowledge and their inter-relationships. Journal of knowledge management practice, 8(2), 1-16.

59. Liew, A. (2013). DIKIW: Data, information, knowledge, intelligence, wisdom and their interrelationships. Business Management Dynamics, 2(10), 49.

60. Loleski, Steven. (2019). "From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers." *Intelligence and National Security* 34 (1): 112-128.

61. Lowenthal, Mark M. (2019). *Intelligence: From Secrets to Policy*. CQ press.

62. Lowenthal, Mark M, and Robert M Clark. (2015). *The Five Disciplines of Intelligence Collection*. Sage.

63. Madureira, L., Popovič, A., & Castelli, M. (2021). Competitive intelligence: A unified view and modular definition. Technological Forecasting and Social Change, 173, 121086.

64. McCarthy, Charlie, Kevin Harnett, Art Carter, and Cem Hatipoglu. (2014). "Assessment of the Information Sharing and Analysis Center Model." National Academies Transportation Research Board.

65. McCrory, Duncan. (2020). "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States." *The RUSI Journal* 165 (7): 34-44.

66. McMillan, Rob. (2013). "Definition: Threat Intelligence." *Gartner*.

67. Meeuwenberg, Ylona. 2017. "Threat Intelligence Sharing as Part of Supply Chain Management Enhancing Security." PhD thesis, Eindhoven University of Technology.

68. Meier, Roland, Cornelia Scherrer, David Gugelmann, Vincent Lenders, and Laurent Vanbever. (2018). "FeedRank: A Tamper-Resistant Method for the Ranking of Cyber Threat Intelligence Feeds." In *2018 10th International Conference on Cyber Conflict (CyCon)*, 321–344. IEEE.

69. Mocanu, M. (2015). "Intelligence Cycle Model Dilemmas and Solutions." *Romanian Intelligence Studies Review,* (14), 165-178.

70. Mutemwa, Muyowa, Jabu Mtsweni, and Njabulo Mkhonto. (2017). "Developing a Cyber Threat Intelligence Sharing Platform for South African Organisations." In *2017 Conference on Information Communication Technology and Society (ICTAS)*, 1-6. IEEE.

71. North Atlantic Treaty Organization. (2022). "AJP-2.7. Allied joint doctrine for joint intelligence, surveillance and reconnaissance".

72. Noor, Umara, Zahid Anwar, and Zahid Rashid. (2018). "An Association Rule Mining-Based Framework for Profiling Regularities in Tactics

Techniques and Procedures of Cyber Threat Actors." In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 1-6. IEEE.

73. Oakley, Jacob G. (2019). "Cyber Collection." In *Waging Cyber War*, 57-70. Springer.

74. Office, NATO Standarization. (2018). *NATO Glossary of Terms and Definitions (English and French)*. NSO.

75. Pawlinski, P, Przemylaw Jaroszewski, Piotr Kijewski, Lukasz Siewierski, Pawel Jacewicz, Przemyslaw Zielony, and Radoslaw Zuber. (2014). "Actionable Information for Security Incident Response." European Union Agency for Network; Information Security.

76. Petratos, Pythagoras. (2011). "Definition and Importance of Cyberintelligence: An Introduction."

77. Phythian, Mark. (2013). *Understanding the Intelligence Cycle*. Routledge.

78. Porche III, Isaac R, Jerry M Sollinger, and Shawn McKay. (2011). "A Cyberworm That Knows No Boundaries." Arlington, VA, USA: RAND Corporation.

79. Price, Douglas R. (2014). "A Guide to Cyber Intelligence." *Journal of US Intelligence Studies* 21 (1): 55-60.

80. Proctor, Tony. (2011). "The Development of Warning, Advice and Reporting Points (WARPs) in UK National Infrastructure." In *International Workshop on Critical Information Infrastructures Security*, 164-174. Springer.

81. Randol, Mark A. (2010). *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*. DIANE Publishing.

82. Richards, Julian. (2014). "The Cyber Challenge for Intelligence." In *Intelligence in the Knowledge Society. Proceedings of the XIXth International Conference*, 97-108.

83. Richelson, Jeffrey T. (2018). *The US Intelligence Community*. Routledge.

84. Richmond, Jeremy. (2011). "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict." *Fordham Int'l LJ* 35: 842.

85. Sari, Arif. (2018). "Context-Aware Intelligent Systems for Fog Computing Environments for Cyber-Threat Intelligence." In *Fog Computing*, 205-225. Springer.

86. Sauerwein, Clemens, Christian Sillaber, Andrea Mussmann, and Ruth Breu. (2017). "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives." In *Proceedings Der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 837-851.

87. Saunders, Kimberly. (2000). “Open Source Information: A True Collection Discipline.” PhD thesis, Citeseer.

88. Seedyk, Christopher. (2018). “Characterizing Cyber Intelligence as an All-Source Intelligence Product.” *DSIAC Journal* 5 (3).

89. Shu, Xiaokui, Frederico Araujo, Douglas L Schales, Marc Ph Stoecklin, Jiyong Jang, Heqing Huang, and Josyula R Rao. (2018). “Threat Intelligence Computing.” In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1883-1898.

90. Shulsky, Abram N, and Gary James Schmitt. (2002). *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.

91. Staff, Joint Chiefs of. (2013). “Joint Publication 2-0. Joint Intelligence.”

92. Steele, Robert David. (2007). “Open Source Intelligence.” In *Handbook of Intelligence Studies*, 147-165. Routledge.

93. Strom, Blake E, Joseph A Battaglia, Michael S Kemmerer, William Kupersanin, Douglas P Miller, Craig Wampler, Sean M Whitley, and Ross D Wolf. (2017). “Finding Cyber Threats with ATT&CK™-Based Analytics.” MITRE Technical Report MTR170202. The MITRE Corporation.

94. Taneski, Nenad, Aleksandar Petrovski, and Dimitar Bogatinov. (2019). “Geography in Geospatial Intelligence-C4IRS and Cyber Security.” In *Security and Crisis Management–Theory and Practice*, 65-73.

95. Taylor, Stan A. (2007). “The Role of Intelligence in National Security.” *Contemporary Security Studies*, 249-267.

96. Tekes, R Osman. (2011). “A Common Architecture for Cyber Offences and Assaults-(Organized Advanced Multi-Vector Persistent Attack): Cyber War Cyber Intelligence, Espionage, and Subversion Cyber Crime.” PhD thesis, University of London. London, UK.

97. Townsend, Troy, Melissa Ludwick, Jay McAllister, Andrew O Mellinger, and Kate A Sereno. (2013). “SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings.” Carnegie–Mellon University. Software Engineering Institute.

98. US Air Force. (2021). “Air Force Doctrine Publication 3-60, Targeting”.

99. Williams, Heather J, and Ilana Blum. (2018). “Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.” RAND Corporation.

100. Willis, Brian. (2012). “Sharing Cyber-Threat Information: An Outcomes-Based Approach.” Intel Corporation.

101. Xiong, Wenjun, Emeline Legrand, Oscar Åberg, and Robert Lagerström. (2022). “Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix.” *Software and Systems Modeling* 21 (1): 157-1.