The importance of intelligence for security in cyberspace

Extended abstract

António Augusto Ramos Carvalho

Master in Information Security and Cyberspace Law

Instituto Superior Técnico – Universidade de Lisboa (december 2020)

Advisors: Professor Doutor Carlos Caleiro and Capitão-de-mar-e-guerra Fialho de Jesus

1. Introduction

1.1. Theme Relevance

In an increasingly digital and interconnected world, cyberspace is clearly one of the great subjects of nowadays, enabling a growing interest of the various actors of society. This new global common created by man, assumes an indisputable relevance in the way of life and the well-being of the populations, providing extraordinary opportunities for development. However, cyberspace also brings about a diverse set of challenges to the security for citizens, organizations and states.

Actually, it appears that disinformation, manipulation, fake news, propaganda and anonymity proliferate in cyberspace. In fact, although humanity lives in the information age, it seems that, paradoxically, more information does not necessarily mean more knowledge. Additionally, there are threats increase in cyberspace, with a great complexity factor, by state and non-state actors that develop their actions in a more and more sophisticated and disruptive way. In particular, it becomes evident that the danger inherent in the serious impact that the actions of these threatening agents can cause on critical infrastructures to support the normal functioning of societies.

Therefore, it is essential that States and organizations can handle with the constant uncertainty that hangs over cyberspace, in consequence of the multiple and complex threats that operate in this environment. To this end, intelligence comes up as an essential and decisive asset which allows to mitigate the uncertainty and to ensure a timely and informed support in the decision-making process.

1.2. Object, objectives, questions and research methodology

The study object of the current investigation is "Intelligence in Cyberspace", aiming to highlight the importance of intelligence and its sharing among the main actors have in cyberspace security.

The **General Objective (GO)** of this investigation is to **analyse the contribution and the importance that intelligence can play for the achievement of security in cyberspace**. In order to pursue this GO, the Specific Objectives (SO), showed in Table 1 were complementarily established.

Table 1 - Specific Objectives of the investigation

SO1	Characterize the cyberspace environment.
SO2	Describe the main domains and entities that, at national level, contribute to security in cyberspace.
SO3	Based on the analysis of intelligence, identify aspects which may contribute to security in cyberspace.

In order to achieve the established GO and to define the guiding thread of this investigation, it was identified the following **Central Question (CQ) - How can intelligence contribute to security in cyberspace**? In response to this QC, the following Derived Questions (QD), presented in Table 2, emerged and were defined.

Table 2 - Questions Derived of the investigation

QD1	How is the present cyberspace environment characterized?
QD2	What are the main domains and national entities that contribute to security in cyberspace and how do they coordinate?
QE3	How may intelligence contribute to security in cyberspace?

The investigation followed a deductive approach and a qualitative research method. For data collection, literature review and documentary analysis of legal and doctrinal references produced by specialists have been studied, and structured interviews with specialists in cybersecurity, cyber defence, combating cybercrime and intelligence have been conducted.

1.3. Study Structure

The present work is structured in five chapters. After the introduction, in the second chapter the cyberspace is characterized. To this end, some of the main characteristics of this unique environment have been identified, and it has been exposed how it constitutes a new domain for conducting military operations, in addition to understanding to what extend it challenges the traditional concepts of sovereignty and frontier. Also in this chapter, the threats present in cyberspace based on the motivation and profile of the authors are analysed.

Subsequently, in the third chapter, the main domains and entities that, at national level, contribute to security in cyberspace are described. In specific, it is characterized the domains of cybersecurity, combat of cybercrime, cyber defence, intelligence, cyber diplomacy and national and international cooperation, exposing how the main actors in those domains operationally articulates.

Then, in the fourth chapter, intelligence is analysed, emphasizing its importance, Cyber Situational Awareness (CSA) and the sharing of information for security in cyberspace. In this context, the Malware Information Sharing Platform (MISP) is also considered, as evidence of the relevance of using systems that allow the sharing of information and Indicators of Compromise (IoC) associated with cyber-attacks, enabling it to carry out an early threat assessment. Also in this chapter, there is a discussion of the investigation, analysing the contributions obtained from the expert interviews, validating the importance of intelligence and the necessity of its sharing in cyberspace.

Finally, the conclusions of the investigation are presented in the last chapter.

2. Cyberspace: the new conflict space

2.1. The main characteristics of cyberspace

First, when analysing cyberspace, it appears that a very particular set of characteristics stand out, intrinsic to the nature and use of this environment, which is important to discuss in order to understand the challenges that cyberspace poses on security and defence of states. Therefore, some of these particularities are identified, having as a guiding thread the joint investigation carried out by IDN-CESEDEN (2013) complemented by the opinion of the experts who have participated in the present study.

Table 3 - Summary table of the main characteristics of cyberspace identified in the investigation

Characteristic	Brief description
Dynamic character	• The different systems that compound cyberspace frequently change and modify.
Huge growth potential	• Visible in the functionalities it provides and in the speed of information exchange.
High processing and storage capacity	• Large amounts of information; • Unleashes a great speed of effects generation; • Have an echo effect and allow persistent memory of counterfeit facts.
Asymmetric character	• Imbalance between the ability to provoke hostile actions of great impact and the reduced resources needed.
Relative degree of anonymity	• It is difficult to detect the origin of an attack, which poses great difficulties into criminal investigation and the imputation of actions in cyberspace.
Spoofing	• Ability for malicious actors to dissimulate their presence in cyberspace.
Transversality	• An action or event that occurred in cyberspace can affect one or more domains of activity in modern societies.
Absence of regulation	• Free use space, with very little regulation; • Absence of mediation.
Amplification capacity	• Extremely effective mean for exploiting human vulnerability.
Reduced cost of access	• The financial cost for accessing cyberspace is low.
High capacity to produce physical effects	• Although it is a virtual space, its effects have repercussions in the physical domain, amplified in the possibility of reaching a wide range of equipment and industries.
Geographically dispersed infrastructures	• Subordinated to different legislative frameworks and to the intervention of numerous international entities. This aspect is widely explored by the most variable threat agents.
Borders undefined	• Elusiveness of boundaries in cyberspace; • It creates difficulties in determining how a State can exercise its sovereignty over an area or environment that it does not dominate and control.

2.2. Characterization of threats in cyberspace

The characterization of threats present in cyberspace is a fundamental aspect, which allows to define and implement appropriate strategies, in order to promote and materialize security in cyberspace. In order to pursue this objective, it is important to first determine the possible sources of threats in cyberspace, namely, the profile of the actors most likely to conduct cyber-attacks. According to IDN-CESEDEN (2013), the sources threats can be classified as: Hackers; Hacktivists; internal staff to organizations; cybercriminals; industrial spies; terrorists; nations. Regarding the motivations for conducting cyber-attacks, they may be independent of the threat's source and can be categorized as shown below in Table 4.

Table 4 - Motivations and sources of threats in cyberspace (IDN-CESEDEN, 2013, pp. 23-24)

Motivations	Description	Threat Sources
Fame or revenge	• The search for fame is intrinsically linked to hackers, who seek to gain recognition in different communities and forums. To this end, and as a "modus operandi", they endeavour to dethrone security barriers, without causing significant damage; • An organization's internal staff may also be driven by fame, although, as a rule, their actions are more related to discontent and revenge.	• Hackers; • Internal staff.
Economic Benefits	• Most common motivation; • It consists of the practice of fraudulent acts, the theft of information or in execution of attacks with a goal to obtaining economic benefits.	• Cybercriminals; • Industrial spies; • Internal staff.
Competitive advantages	• It may be associated with theft of State's secrets; • Or they may be the reason for the obtaining sensitive information from organizations or companies that allow a competitive advantage to third parties.	• Industrial spies; • Nations.
Political, ideological and religious[1] motivations	• They are at the origin of the conduct of harmful actions and attacks against public organizations and governments by different groups; • There are also conflicts between nations that are instigated by motivations of this nature.	• Hacktivists; • Terrorists.
Destruction or damage	• Motivation that is intrinsically linked to terrorists, who seek to carry out attacks with this goal; • Likewise, nations that are in conflict may also carry out attacks with this end.	• Terrorists; • Nations.

In this context, based on the motivation and profile of their authors, it is conceptualized that threats in cyberspace can be grouped into five main categories, namely: hacktivism; cybercrime; cyber espionage; cyberterrorism; and cyberwar. Nevertheless, the reality shows that each of these categories has diffuse limits and sometimes it is difficult to determine the real threat source.

[1] Although IDN-CESEDEN (2013) only identifies political motivations in this field, we agree with Santos (2011) who adds to the political motivations also the ideological and religious.

3. Security in Cyberspace

3.1. Domains and Competence Areas

To face the challenges and the set of threats that exist in cyberspace the States and the society, just as they deal with transnational and asymmetric threats, must develop and implement a set of "action plans" also called domains.

Based on the research initially proposed by Santos et al., (2012) and later complemented by Santos (2018), and adapting it according to the National Cyberspace Security Strategy (NCSS) 2019-2023 (GOV-PT, 2019) we consider that the following domains are essential and have a decisive contribution to security in cyberspace: cybersecurity; combating cybercrime; cyber defence; intelligence; cyber diplomacy and national and international cooperation. The Figure 1 represents the referred domains.

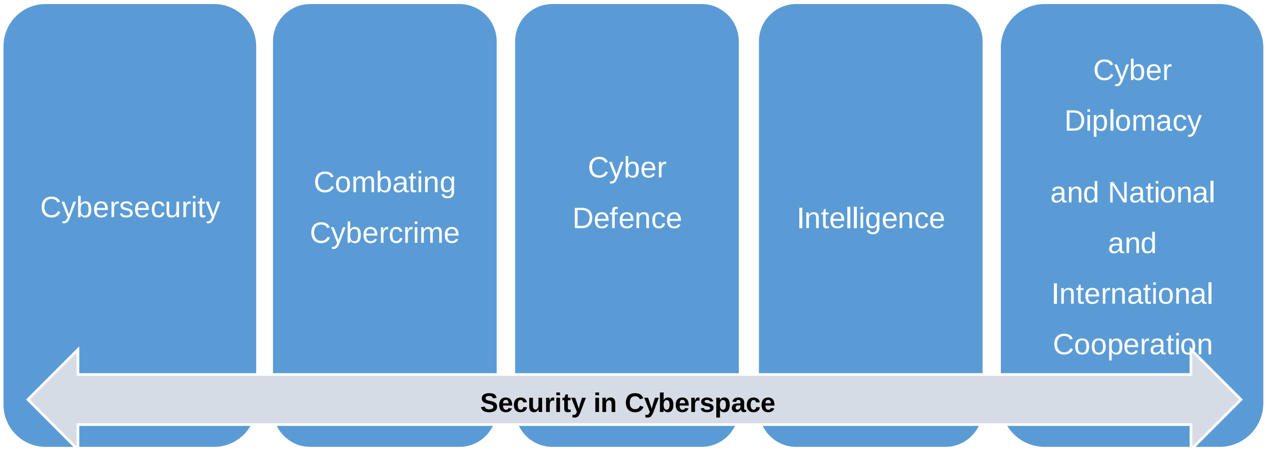

Figure 1 - The main areas that contribute to the security in cyberspace (Author, 2020)

In general, the domain of cybersecurity encompasses the technical, the procedural and the human resources that aim to guarantee, in the first instance, the Information Security (IS), because this is the primary protection barrier to infrastructures, services and information in cyberspace.

Thus, a cyber-attack is interpreted as a sequence of actions aimed at producing an unauthorized effect or an unwanted disturbance in the confidentiality, integrity, availability of information or in a service.

In turn, the main goal of the domain of combating cybercrime is to deterrence of the practice of crimes and, at the limit, the conviction of the perpetrator of a crime. This aspect is as Batista (2016) points out, the main differentiating element to the domain of cybersecurity, given that in cybersecurity the aim is the prevention, while in domain of combating cybercrime - criminal investigation - the focus is the reaction to a crime.

Cyber defence encompasses the main activities to prevent, monitor and react to threats that put national sovereignty at risk, as well the all the activities to support the operations in cyberspace.

The domain of intelligence is responsible for ensuring the production of decisive intelligence that allows the early detection of the threat agent’s intentions. For this, the intelligence area comprises all work developed with the aim to obtaining a deep knowledge about potential threat agents, namely: their intentions; capabilities; performance characteristics; and footprint or digital signature.

In the field of cyber diplomacy and cooperation, its action materializes into acting, bilaterally and multilaterally, in order to strengthen the solid existing alliances, exert influence and promote the implementation of policies, so that in collaboration with national allies and partners and international, could jointly reduce insecurity in cyberspace.

3.2. Coordination between the main domains

The set of domains listed and the main actors involved in each of them represent, to a large extent, the national security capacity of cyberspace. In fact, as Santos et al. (2018, p. 41) mentioned "the protection of cyberspace, constituting an extremely demanding task, cannot be guaranteed in isolation by any institution or State". Thus, it is essential to promote complementarity between the various domains, given that, in a conflict scenario, it may be necessary to act simultaneously in the various plans described, each one, with its scope of action and with its resources, procedures and transnational cooperation networks, within a specific legal framework.

In order to promote cooperation and information sharing between the main tactical and operational entities, which contribute to the security of national cyberspace, it was created an informal operational group, called G4. This group comprises the National Cybersecurity Center (CNSC); the Cyber Defence Center (CCD); the National Unit to Combat Cybercrime and Technological Crime (UNC3T); and the cybersecurity unit operating under the SIS (Figure 2).

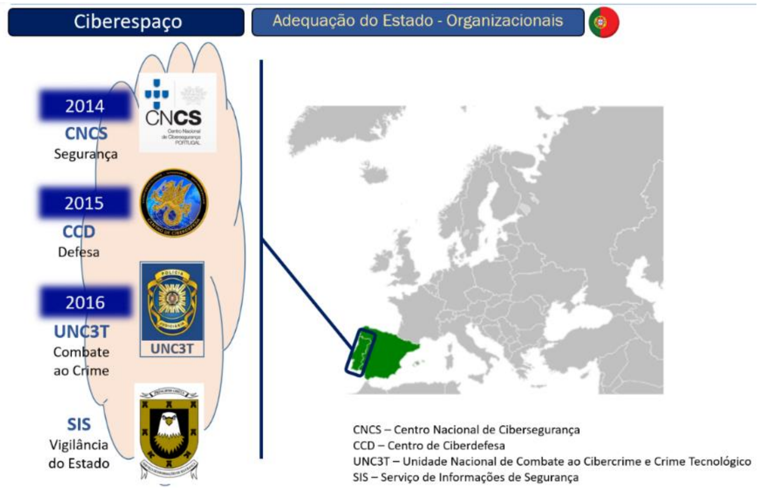
Ciberespaço
Adequação do Estado - Organizacionais
2014
CNCS
Segurança
CNCS
Centro Nacional de Cibersegurança PORTUGAL
2015
CCD
Defesa
2016
UNC3T
Combate
ao Crime
UNC3T
SIS
Vigilância
do Estado
CNCS – Centro Nacional de Cibersegurança
CCD – Centro de Ciberdefesa
UNC3T – Unidade Nacional de Combate ao Cibercrime e Crime Tecnológico
SIS – Serviço de Informações de Segurança

Figure 2 - Constitution of G4 - operational nucleus that permanent cooperate into the promotion of security in cyberspace of national interest (Jesus, 2019, p. 5)

4. Intelligence in Cyberspace

Taking into account the new and complex threats that arise against the security of the states and the existence of a low intensity conflict, intelligence appears as a fundamental component for obtaining a CSA with a view of prevention and deterrence of cyber-attacks. In the face of the increasingly disruptive capacity of cyber-attacks, causing more and more destructive and kinetic effects, it is recognized that intelligence in cyberspace is an essential asset to contribute to anticipating, preventing and mitigating cyber-attacks.

Therefore, what intelligence means is discussed next. To achieve this goal, it is necessary, according to Lowenthal (2006), to perform a holistic analysis of intelligence, which must take into account three essential elements, namely: the process, the product and the organization.

4.1. Intelligence as a process, product and organization

Intelligence as process refers to the sequence of activities by which certain types of information are required, aggregated, analysed, converted into knowledge and disseminated in order to support decision making processes. According to NATO (NATO, 2016), these activities are focused through the four intelligence core stages of direction, collection, processing and dissemination shown in Figure 3. Although, the intelligence cycle shows a certain simplicity, it is in fact a complex process, put into practice through the execution of multiple tasks, carried out at different rates, which may not necessarily be sequential.

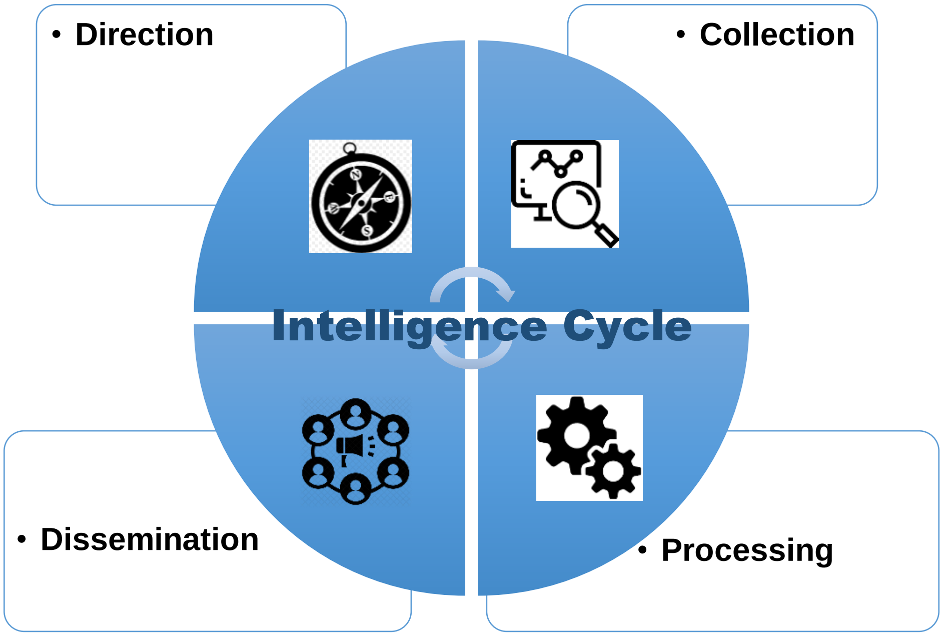

Figure 3 - The Intelligence Cycle adapted from AJP - 2 (A) (NATO, 2016, p. 4_2)

Intelligence as a product aims to describe the knowledge that is produced and disseminated in the course of the intelligence cycle, also identifying the main characteristics that they must obey in order to be considered useful, timely and accurate. Intelligence as an organization discusses the intelligence services, analysing its organic structure and its operating model, through which it leads the process of the production of intelligence.

4.2. Cyber Situational Awareness (CSA)

The permanent uncertainty that hovers over security in cyberspace, ensuing from the various threats of a diffuse nature, indefinite limits and in constant evolution, requires the existence of a capacity to detect and identify, in a timely manner, the indicators that may be related to potential and ongoing attacks. This capacity, called CSA, is often referred as the "holy grail" of cyberspace (Ali, 2016).

According to NATO (2020) CSA is a combination of a near real-time updated *(Recognized Cyberspace Picture)*, analysis and information management. According to the Team Leader of the Task Force Cyber at Supreme Headquarters Allied Powers Europe (SHAPE), Colonel Rizwan Ali (2016), in order to achieve a broad and robust CSA it is necessary to take into account three main aspects, namely: threat; network awareness; and mission awareness. The Figure 4 schematically represents the dependency relationship of these three factors for obtaining a robust CSA.

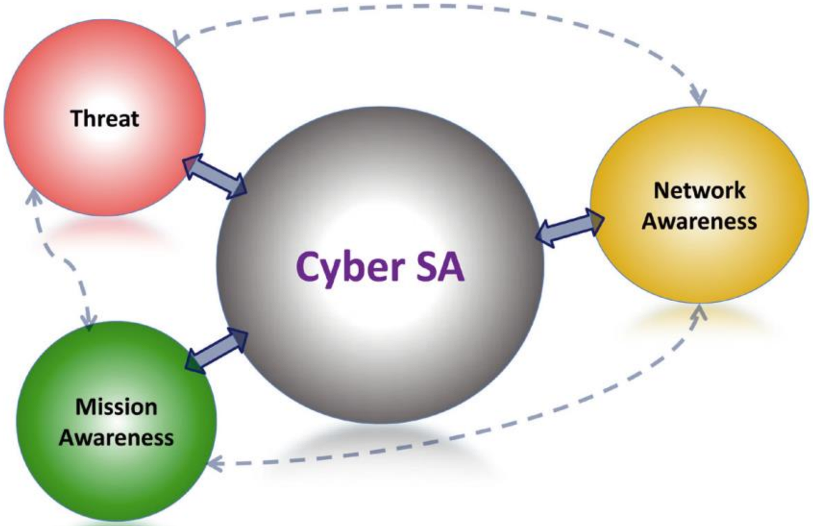

Figure 4 - The essential factors for obtaining Cyber Situational Awareness (Ali, 2016, p. 73)

4.3. Information sharing in cyberspace: the case of MISP

To obtain a robust CSA, it is essential efficient and timely sharing of information, knowledge and intelligence among the main authorities, entities and organizations, national and international, which contribute to the security in cyberspace, which makes it possible to carry out an early threat assessment. In order to achieve this objective, it is crucial to have a system that allows the sharing of these threat indicators in an automated, systematic and effective way. It has been in this context that NATO launched the MISP project in order to promote cooperation and information sharing among allied nations. At the national level, Portugal is operationalizing it at the G4 level.

According to MISP User Guide this platform “facilitates the exchange and sharing of threat intelligence, IoC about targeted malware and attacks, financial fraud or any intelligence within our community of trusted members. MISP sharing is a distributed model containing technical and non-technical information which can be shared within closed, semi-private or open communities (MISP Community, 2019, p. 10).

4.4. Investigation discussion. The importance of intelligence and the urgency of it's sharing in cyberspace

The intelligence about threats that hover over cyberspace and their intentions allows to mitigate the uncertainty and provide timely and informed support to the decision-making process, in order to be able to anticipate, defend and mitigate cyber-attacks. This assertion is corroborated by all the specialists participating in the present investigation, showing in Table 5, as a corollary, a list of the main aspects which intelligence can significantly contribute to the security in cyberspace.

Table 5 - Summary table of the main aspects identified in the investigation in which the intelligence can contribute to security in cyberspace

Expert	Contributions of information to security in cyberspace
SIS (2020)	• To contribute to obtaining a clear image of the digital footprints of malicious agents; • To timely identify attack infrastructures; • To support a specific awareness program, to public and private entities, sharing the specialized knowledge about the agents of the threat and their ways of acting;
Santos (2020)	• To contextualize the technical information that the set of operational entities gathers and deals with; • To feed and update the global and special threat framework and contribute to risk analysis; • To produce technical information that feeds the Situational Framework.
Bravo (2020)	• To unravel dangers and trends; • To sensitize decision makers to these dangers; • To actively oppose them (counter-information, misinformation, crisis management and 'CNO' technical actions).
Assunção (2020)	• Prevention; • Mitigation; • Imputation.
Rodrigues (2020)	• To ensure an adequate decision-making; • To provide an urgent advance notice for the cyber units that guarantee the defence of an organization's perimeter.
Silva (2020)	• Intelligence in the broad sense, and Counter-intelligence in the strict sense are fundamental to mitigate the threats • Through the integration and relationship with other Intelligence disciplines (e.g. HUMINT), a more complete and adjusted product can be developed with respect to real situational awareness.

5. Conclusions

The investigation first focused on "**characterizing the cyberspace environment**", a purpose established as the **SO1** of the investigation. In result of the study some identified characteristics allow responding to **QD1 -** "**how is the present cyberspace environment characterized**", of which the following stand out: it has a very dynamic character; it has enormous growth potential; it has a high capacity for storing and processing information; it enhances asymmetry, originated by the great imbalance between the possible high damages and the reduced means necessary to achieve them; anonymity and the consequent imputation difficulty prevail; it enables an actor's to mystifying its presence; it conveys transversality and interdependence between all sectors of a society; it does not have adequate regulation; it enables the capacity to expand human vulnerability; it has a low cost of access; its effects are reflected in the physical world; its infrastructures are geographically dispersed, therefore, subject to different legislative frameworks and to the intervention of several international entities; it intensifies the blurring of the limits of borders in cyberspace.

After having characterized the cyberspace, effectively, a new space of conflicts and disputes, the investigation focused on "**describe the main domains and entities that, at national level, contribute to security in cyberspace**." i.e., in **SO2**. As a result of the investigation, **the main domains and national entities that contribute to security in cyberspace were identified and characterized, and exposed how they are articulated**, answering to **QD2**

From the analysis carried out, it is concluded that in order to face the challenges and the set of threats existent in cyberspace, similarly to what states carry out to deal with an asymmetric or transnational threats, they should implement and operationalize a set of actions plans, based on these main domain: cybersecurity; combating cybercrime; cyber defence; intelligence; cyber diplomacy and national and international cooperation. In order to increase cooperation, stimulate information sharing and promote the articulation of actions between the main entities in these domains, the informal operational group called G4 was created. Specifically, this group includes, respectively, the CNSC, the UNC3T, the CCD and the SIS.

Regarding the **SO3** – **"Based on the analysis of intelligence, identify aspects which may contribute to security in cyberspace"** the respective QD3 was formalized - "**how may intelligence contribute to security in cyberspace?".**

In order to obtain a holistic view about intelligence it is necessary to take into account three essential elements, namely: the process, the product and the organization.

Intelligence as process refers to the Intelligence Cycle which is implemented in order to convert information into knowledge. Intelligence as a product aims to describe the knowledge that is produced and disseminated in the course of the intelligence cycle, also by identifying the main characteristics that they must obey in order to be considered useful, timely and accurate. Intelligence as an organization discussed the intelligence services, analysing its organic structure and its operating model, through which it leads the process of the production of intelligence.

Apart from intelligence, we conclude that for security in cyberspace, as in any other environment, it is essential to have a capacity to determine the dynamics of threats and perceive the intentions, movements and possibilities of potential attackers. This capacity in cyberspace is called CSA, and we verify that intelligence contributes decisively to its construction and sustainability. In addition, in order to obtain a robust and comprehensive CSA of interest, it is necessary to take into account three fundamental aspects, namely: threats; awareness of the network; and awareness of the context and environment where the mission or activity is carried out.

Besides the analysis of the important role that intelligence can play in security in cyberspace, we considered as an important contribution to knowledge the fact that we have highlighted the relevant and urgency of the sharing of intelligence and information among the main entities to obtain the security in cyberspace. For this purpose, it was also demonstrated the importance of the main actors with responsibility for cyberspace security, and the organizations which depend on cyberspace for the exercise of their activity, have sharing information platforms, such as MISP or other tools of Threat Intelligence, in order to be able to efficiently anticipate, prevent and mitigate any cyber-attacks.

6. References

Ali, R. (2016, 7). Cyber Situational Awareness for the NATO Alliance. *The Three Swords Magazine*(30), pp. 72-75. Retrieved 7 20, 2020, from https://www.jwc.nato.int/newsroom/The-Three-Swords-Magazine

Assunção, F. (2020, 11 2). A importância das informações para a segurança no ciberespaço. *Especialista Ciberdefesa - Centro de Ciberdefesa*. (A. Carvalho, Interviewer)

Batista, R. (2016, 9 27). Legislação do Cibercrime. *Cursi Geral de Cibersegurança: uma perspectiva Whole-of-Society*. Lisboa: CNSC.

Bravo, R. (2020, 10 26). A importância das informações na segurança do ciberespaço. *Especialista Combate ao Cibercrime - Polícia Judiciária*. (A. Carvalho, Interviewer)

GOV-PT. (2019, 6 5). Estratégia Nacional de Segurança do Ciberespaço 2019-2023. *Resolução do Conselho de Ministros n.º 92/2019*. Lisboa: DR. Retrieved 10 18, 2019, from https://data.dre.pt/eli/resolconsmin/92/2019/06/05/p/dre

IDN-CESEDEN. (2013). *Estratégia da Informação e Segurança no Ciberespaço: Investigação conjunta IDN-CESEDEN* (Vol. IDN Cadernos nº 12). Lisboa: Instituto da Defesa Nacional.

Jesus, H. (2019, 12 17). Ciberdefesa - Capacidade Nacional. *Biefing Visita MDN Angola ao CCD*. Lisboa: CCD.

Lowenthal, M. (2006). *Intelligence. From Secrets to Policy.* Washington, DC: CQ Press.

MISP Community. (2019). *MISP - User Guide. A Treat Sharing Platform.* Luxembourg: CIRCL. Retrieved from CIR.

NATO. (2016). *AJP-2 - Allied Joint Doctrine for Intelligence, Counterintelligence And Security Doctrine* (Edition A Version 1 ed.). Brussels: NATO Standardization Office.

NATO. (2020). *AJP-3.20 - Allied Joint Doctrine for Cyberspace Operations.* Brussels: Nato Standardization Office (NSO).

Rodrigues, N. (2020, 11 2). A importância das informações para a segurança do ciberespaço. *Especialista Informações - Centro de Ciberdefesa*. (A. Carvalho, Interviewer)

Santos et al. (2018). Defesa do Ciberespaço. In I. d. Nacional, *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 33-46). Lisboa: IDEN Cadernos.

Santos, L. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal.* Lisboa: Universidade Nova de Lisboa - Faculdade de Direito.

Santos, L. (2020, 10 28). A importânica das informações para a segurança no ciberespaço. *Especialista Cibersegurança - Centro Nacional de Cibersegurança*. (R. Carvalho, Interviewer)

Santos, L., Bravo, R., & Nunes, V. (2012, 1 3). Proteção do Ciberespaço: Visão Analítica. *FCCN - Fundação para a Computação Científica Nacional*. Retrieved from http://hdl.handle.net/10400.26/3578

Silva, C. (2020, 11 15). A importância das informações para a segurança no ciberespaço. *Especialista Informações - Centro de Informações e Segurança Militares*. (A. Carvalho, Interviewer)

SIS. (2020, 12 12). A importância das informações para a segurança no ciberespaço. *Contributo institucional do Serviço de Informações de Segurança*. (A. Carvalho, Interviewer)