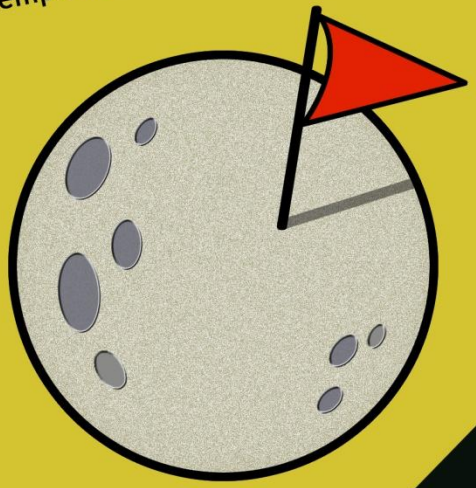
CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

cyber espaço
novas fronteiras

cyber ataques
algumas estratégias de mitigação

cyber segurança
preocupação global

outros
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

CYBER SECURITY VS. CYBER DEFENSE – A PORTUGUESE VIEW ON THE DISTINCTION.

CIBERSEGURANÇA VS. CIBERDEFESA – UMA VISÃO PORTUGUESA DA DISTINÇÃO.

MIGUEL FERREIRA DA SILVA[1]

[1]Correio eletrónico: mjnfds@gmail.com

SUMMARY: 1.DEFENSE AND SECURITY; 2.SOME INTERNATIONAL DISTINCTIONS; 3.PORTUGUESE CYBER DISTINCTIONS; 4. CONCLUSIONS.

ABSTRACT

The current Portuguese academic landscape shows a growing interest for research and debate on cyber security and cyber defense. Yet, as in most countries, there is not yet a consensus on which concept is what.

On the public sphere, and despite grate care in assuring the proper legal functioning of cyber security initiatives and institutions, there is a clear, although discrete, move to strengthen Cyber Defense capabilities and authorities. Amongst all the "Political Guidance for Cyber Defense" clearly being the leading Strategy.

Keywords: Cyber Security, Cyber Defense; concepts; political guidance.

RESUMO

A atual paisagem acadêmica Português mostra um crescente interesse pela pesquisa e debate sobre cibersegurança e ciberdefesa. No entanto, como na maioria dos países, não existe ainda um consenso sobre qual destes conceitos é o quê.

Na esfera pública, e apesar das cautelas em assegurar um funcionamento legalmente correcto das iniciativas e instituições de cibersegurança, há uma clara, embora discreta, tendência para reforçar as capacidades e as autoridades de Cyber Defesa. Entre todas sendo a "Orientação Política para a Ciberdefesa" claramente a principal estratégia.

Palavras chave: Cibersegurança; Ciberdefesa, conceitos; orientações políticas.

1. DEFENSE AND SECURITY.

The Portuguese translation of security – "segurança" – translates both the concept of security and that of safety. The fortunate translation (elsewhere rather problematic) encompasses in itself the holistic approach security has to have in cyber. As we know, in this particular environment – cyberspace – the barriers between actors of security (from individual users to States) and the types of risks (from continuity assurance to data theft) all further blur that distinction. In a way, the portuguese wording for cyber security is more accurate then itself, as it includes not only security but also safety. This becomes more obvious when most references to protective measures (usually referred to as cyber hygiene), and certainly within the scope of safety, are clearly included in the concept of "segurança" ("security").

There is however a more difficult distinction, one to which the legal and cultural understanding of the functions and duties if the State, vis-à-vis civil and economic rights, has an enormous impact. A properly capitalized "Defense" concept appeals to that basic function of the State to provide protection from outside threats. A concept mostly identified with Armed Forces, as well as with its capabilities for military action in defense of an entire nation.

We recognize the common doubts about the double meaning of "cyber defense", both as operational continuity assurance and military cyber capabilities.

- As operational continuity assurance, cyber defense might be understood as cyber security of a (yet another) unique critical infrastructure – the military.

- As cyber capabilities, understood as the capabilities to gain advantages upon an adversary, either we are considering self-resilience – where the defensive capabilities might be thought of as functions which could be traced back to cyber security (leaving only a problem of scale) – or we are considering offensive capabilities.

From a democratic "western" point of view, we usually understand "defense" as defensive, and not offensive. That, however, is a misconception in the cyber space. Even if, in cyber, we might think of (military) self-resilience as a type of security ("security of the force"), that in practice falls short of reality. First because "security of the force" may include preemptive action (offensive in nature during campaign),

but also as, for Defense institutions to be able to actively defend, they must also be capable of preemptive military action (offensive in nature also at the planning stage). Meaning that such function is not only aimed at the protection of the force itself but to the general goals of the Defense sector, i.e. the protection of the nation.

That doesn't mean such military capabilities, or operations, are necessarily considered as "offensive". In fact one could almost quote, in identifying "offensive action", U.S. Supreme Court Justice Potter Stuart[2] – " I'll know it when I see it". There is however an indisputable fact: Defense capabilities in Cyber differ, even when cumulative, with cyber security capabilities.

Furthermore, there is a generalized trend for understanding Defense as a part of a larger Security Sector. In this sense, the distinction between responses (as functions) follows the target objectives of the threats.[3] Such a view puts less emphasis in the specific actions (e.g. phishing, trojans) and their actors (e.g. a national of country "X", a criminal network). On the contrary it highlights the function to be activated (Security or Defense) and the nature of the threat (private or public).

That is to say that there are two levels of assessment: one that distinguishes the targets and actors, as private or public/state; and another that regardless of the target, distinguishes the objectives of the threat.

In the first case it's relatively easy to establish if the threat aims to harm a state, even when the targets are private (e.g. not only conventional inter-states armed conflicts, but also small scale terrorist attacks against general population or critical infrastructure of a specific state). On the other it is more difficult to assess whether the State faces a security challenge or a "defense level" attack (e.g. private motivations for attacks against public assets or information security breaches).

One thing seems to be widely accepted: more obviously then elsewhere, in the cyber space Defense cannot operate in the absence of (or without an adequate level of) Security, and there is an operational continuity between Security and Defense, which can only be assured by cumulative capabilities. Such overlap may pose some

[2] USSC Justice Potter Stuart, referring to "hard core" pornography, Jacobellis v. Ohio, 378 U.S. 184 (1964).
[3] We are highlighting a distinction between functions and threats instead of one between actions and actors.

challenges to the accepted principle limiting *Posse Comitatus*[4], so widely criticized were it is not observed. But a far more present challenge relates to the possible conflict of rights, as this necessary overlap between Security and Defense may put a stress between assuring safety and security and the full exercise of individual liberties by individual citizens.

2. SOME INTERNATIONAL DISTINCTIONS

According to the Open Technology Institute's listing of international definitions, and mostly using sources with entries in both concepts, one could make a few comparisons.[5] This source lists 34 countries (or international organizations) with a "definition" of cyber security, but only 8 with a parallel definition of cyber defense. It is interesting to see the differences among them:

- AUSTRIA -

Cyber Security

Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organizational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimize the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.

Note the emphasis in the protection of legally protected "assets" (thus including individual rights) by constitutional means (thus equally limited).

---

[4] Posse Comitatus Act of 1878 – 18 U.S. Code § 1385.

[5] Adapted from http://opentechinstitute.github.io/cyber-definitions/web/search.html?q=Cyber+Security and http://opentechinstitute.github.io/cyber-definitions/web/search.html?q=Cyber+Defense.
Notes: We didn't kept the original English version of *defence* instead of the American version (defense), for consistency; for comparison purposes, most sources mentioned here with own definitions in both concepts; Our italics, for highlighting purposes; mention to "(Translations)" are from the authors of the original compilation.

Cyber Defense

The term "cyber defense" refers to all measures to defend cyber space with military and appropriate means for achieving military-strategic goals. *Cyber defense is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army.*

An open definition encompassing all aspects of military activity and capabilities as mentioned above, yet focusing on the (military) function facing the threat (to military-strategic goals).

- EUROPEAN UNION -

Cyber Security

Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, *from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.*

Despite an ambiguous reference to confidentiality, the poor wording points us towards a safety perspective of security.

- FRANCE -

Cyber Security

The desired state of an information system *in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cyber security makes use of information systems security techniques and is based on fighting cybercrime and* establishing cyber defense.

The rather ample definition not only (more explicitly then Austria) points towards the operational integrity and availability of assets, in this case "an information system", but also encompasses a more proactive face of security (in fighting crime), recognizing the needed overlap with Defense capabilities.

Cyber Defense

The set of all technical and non-technical measures allowing a State *to defend in cyberspace information systems that* it *considers to be critical.*

Function seems to be the key assessment standard, although giving less emphasis to the threat and more to the (State) actor of the (defense) function. To note also that no reference is made to the nature of those executing the function, as nowhere do we read "military" as the only state power with this objectives.

- MONTENEGRO -

Cyber Security

Cyber security refers to efforts to prevent damage *caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.*

Cyber security seeks to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. General security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality".

The listing that follows the first definition attempt appears to deviate from the functions/threats logic and to focus on actions. Yet after a closer look that listing may offer examples of a subjective but wider view of continuity and availability, while still mentioning "organization and user's assets" and "confidentiality".

Cyber Defense

Cyber defense is mainly used in military context, *but it may be also related to criminal and espionage activities.*

NATO uses the following definition when referring to cyber defense: the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace."[6]

- NATO : NORTH ATLANTIC TREATY ORGANIZATION -

Cyber Defense

(Active Cyber Defense) A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source.

There seems to be an inner contradiction in the last part of the definition. As in the (possible) phrase "proactive measure" "for determining the origin of an operation that involves launching…", whatever is launched (preemptive, preventive, or cyber counter-operation) is *not* included in the definition. Only the measure for determining the origin is. As James Lewis[7] tells us such a position cannot hold, but it is useful to highlight the shyness of admitting it.

- ROMANIA -

Cyber Security

(Translation:) The state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information electronically for public and private resources and services in cyberspace. Proactive and reactive measures may include

[6] The reference to NATO is made, according to the source, by Montenegro. As we can see below the wording by NATO is not exactly the same as the one Montenegro seems to quote.
[7] Lewis, James A. *The role of offensive cyber operations in NATO's collective defence*, Tallin Papers n. 8, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallin, 2015.

policies, concepts, standards and guidelines for security, risk management, training and awareness activities, implementing technical solutions to protect cyber infrastructure, identity management, and consequence management.

Cyber Defense

(Translation:) Actions in cyberspace to protect, monitor, analyze, detect, counter aggression, and ensure appropriate response against specific cyber threats to national defense infrastructure.

- U.S.A. / RUSSIA -

Cyber Defense

Cyber Defense is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attacks.

In sharp contrast with the previous, this proposed definition enlarges the scope of "defense" to functions including most, if not all, of those of "security".

- COLUMBIA -

Cyber Security

(Translation:) Capacity of the state to minimize the risks they and their citizens are exposed to, in the face of threats and incidents of the cyber nature.

If in the concept of cyber defense (below) "State" as an actor and "national sovereignty" as a target limit the scope of "defense" to State actions, here the private sector and the individual are taken off their central role in security.

Cyber Defense

(Translation:) State capacity to prevent and counter any threat or incident that is cybernetic in nature which affects national sovereignty.

- BELGIUM -

Cyber Security

(Translation:) Cyber security is the desired situation or protection of cyberspace and is proportional to the cyber threat and potential consequences of cyber attacks. In a situation of cyber security, disruption, attack, or misuse of ICT does not cause any danger or harm. The consequences of abuse, disruption or attack may include restricting availability and reliability of ICT, the violation of the confidentiality of information, or the damaging of the integrity of information (addition, deletion, or modification [of information] are illegal).

The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks. At Defense Cyber Security comprises three pillars: Cyber Defense, Cyber Intelligence and cyber counter-offensive.

(Translation) a favorable situation where the protection of cyberspace is proportional to cyber threats and the possible consequences of cyber attacks. In a situation of cyber security, the disruption, an attack or abusive utilization of information and communications will not provoque danger or damage. The consequences of abusing, disruption or an attack can provoke inability to use, and untrustworthiness of information and communications systems, and the violation of confidentiality of information or damage the integrity of the information (illegal adding, deleting or modifying of information).

Cyber Defense

The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defense's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defense consists of following duties: Protect, Detect, Respond, and Recover.

3. PORTUGUESE CYBER DISTINCTIONS.

Reviewing the current Portuguese research in this field, we find a number of examples of commonly accepted conceptualizations. Among research products, the reference standard is offered by Lino Santos' entries at the (Portuguese) Encyclopedia of Law and Security[8].

3.1. Cyber security seems to be a more widely used, if not accepted, term. In fact, the Portuguese Encyclopedia of Law and Security has an entry for "cyberspace" [9] and another for "cyber security" [10] yet none for "cyber defense". In his work, Lino Santos tells us in this encyclopedia that "cyber security" may have a double meaning: one for the security of the entire "cyberspace" as an autonomous "entity" and another for the security of the cyber component of a specific system. Yet he offers three different approaches.

On a first approach, this same author recognizes the conceptual importance of the "subject" ("object" in the original) of cyber security for the definition.[11] In his particular case identifying these subjects of (cyber) security as: the State; market(s); and individuals.

On a second conceptual approach to a definition of Cyber Security, Santos highlights the "set of systems or domains that the state and society in general have to deal with cyber security". In this sense, he identifies four of them: simple protection; criminal prosecution; war; and diplomacy.

i. At the simple protection level we are redirected to the International Telecommunications Union definition, although with a substantial explanation of the technical, procedural and human resources needed to prevent, react and manage within cyber security.

ii. When addressing criminal prosecution, Santos highlights not only the possible new "cyber means" of perpetrating already established crimes against

[8] Bacelar Gouveia, Jorge and Santos, Sofia (Coord.), Enciclopédia de Direito e Segurança, Almedina, Coimbra, 2015.
[9] Santos, Lino, "Ciberespaço", op.cit., pp. 60.
[10] Santos, Lino, "Cibersegurança", op.cit., pp. 63.
[11] Ibidem, pp.64.

existing rights, but autonomous cybercrimes capable of harming rights connected with the cyberspace.

iii. The author's reference to war – without any prefix (re. "cyber") – points towards the continuity of military operational capability and the acquisition of advantages against adversaries. To note that despite a reference to National Defense as equally empowered to assure command and control in war and emergencies ("also in cyberspace"), no reference is made in this author's article to "cyber defense".

iv. In diplomacy only the aim – as prosecution of national objectives – is referred.

The third and last approach gives us six "axis of intervention" for the set of policies in most "known national cyber security strategies". In this sense Santos proposes the primacy of the function when grouping measures in different categories of policy efforts (an approach already explored by the author in his MPhil dissertation[12]):

i. Combating cybercrime. Which would include not only the updating and harmonization of relevant criminal legislation, but also regulating Information and Communications Technologies (ICT) industry so as to assure an "adequate level of cyber security". In this later sense the emphasis is given to the regulation of the telecommunications market.

ii. Standardization and certification. Understood as the national and international efforts to establish "references, rules, conditions or requisites of security" as well as the due compliance of products and services with those patterns.

iii. Training and awareness. As technological training and updating (capacity building), but also awareness and alert initiatives.

iv. Protection of critical infrastructures. Including risk analysis, preceded by mapping functional dependencies, and implementation of protective measures in critical functions.

[12] Santos, Jose Lino Alves dos. *Contributos para uma melhor governação da cibersegurança em Portugal*, Masters dissertation presented at the Universidade Nova de Lisboa, Lisboa, 2011. A shorter work by this author was publishes as a paper at pp. 217-305 in *Estudos de Direito e Segurança*, Vol. II. Jorge Bacelar Gouveia (Coord.), Almedina, Coimbra, 2014.

v. Warning and response. Actions to mitigate cyber security incidents and alerts for new vulnerabilities and emerging threats.

vi. Research and development. Not only aimed for technological development, but including other social areas of research ("namely ethics, behavioral security, criminology or risk").

3.2. In Octávio Militão's[13] research, cyber security is identified more with policing functions: "*Cyber security is the guarantee or control and 'policing' of cyberspace so as to ensure an effective response to criminal activity*". Safety is not considered, nor does the specific challenges of jurisdiction or level of threat considered.[14]

A much more complete view is presented on cyber defense: "*Cyber defense - has the task of ensuring the achievement of security and national defense missions, namely to guarantee state sovereignty in the global cyberspace.*"[15]

Later in his research, Militão underlines that both concepts "*are considerably different and each one encompasses a specific sphere of action in cyberspace*" [16] yet stating again a parallel between cyber security and police and intelligence services, on the one hand, and cyber defense and armed forces on the other:[17]

Cyber security	Security forces	Cybercrime
		Hacktivism
	IT ("Informatics")	Cyber espionage

[13] Militão, Octávio Pimenta. *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*, masters dissertation, FCSH, Univ Nova de Lisboa, April 2014.
[14] Although he is here quoting: Nunes, Paulo Viegas. "*Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço*", Conference, Beja, IV SimSIC, 2013.
[15] Here too quoting another article by the same original author: Nunes, Paulo Viegas. "*A Definição de uma Estratégia Nacional de Cibersegurança*", Cibersegurança, N.o133, IDN, 2012.
[16] Militão, op.cit., pp. 25.
[17] Idem.

	Services[18]	Cyber terrorism
Cyber defense	Armed Forces	Cyber war

It is therefore with surprise that this author further develops the concept of cyber security in this research: "*Cyber security is the set of measures that seek to ensure the wellbeing and the proper functioning of the action of a state and its people in cyberspace and beyond, if derived from actions directly deriving from it.*"[19]

3.3. On a more official stance, we now look to the use of the terms "Cyber Security" and Cyber Defense" in two Acts of the Portuguese Government. One creating the National Cyber Security Center, established in the Decree-Law n.º 69/2014,[20] of May 9th, and the other approving the National Security Strategy in Cyberspace, published as annex to the Resolution of the Council of Ministers n.º 36/2015, of June 12th.

3.3.1. The National Cyber Security Center was created by an Executive Act, thus a law. We must first consider the almost immediate need of the Portuguese Government to comply with guideline both from the European Union and from NATO, so as to establish such a Center. That being said, the architecture chosen for this institution hardly meets the needs announced in the preamble.

Furthermore, the concept of Cyber defense is:

a) Completely absent from any reference while defining the mission, duties and responsibilities of this new Center; and is only

[18] Although translated correctly from the original in Portuguese, we believe there might be a misunderstanding between the Portuguese and English terms for information/intelligence. In Portuguese "intelligence" is translated with the plural of "information", thus capturing the need for additional treatment on each information gathered. Yet it is common to mistranslate that Portuguese concept with the English for "information" instead of the correct "intelligence". On the other hand *informático* refers to IT related, e.g. IT technician. In this particular case the original author does use the Portuguese equivalent to "information technology", despite our belief that such use rises from the referred mistranslation. In the same dissertation, the original author later refers to these same types of threats as addressed by Intelligence Services. For accuracy purposes we kept the correct translation, although understanding it as referring to aimed to "intelligence services".

[19] Militão, op.cit., pp. 26.

[20] This Executive Act (Decree-Law n.º 69/2014, of May 9th) amends, by introducing three new articles, the Decree-Law n.º 3/2012, of January 16th. Therefore, any mention hereinafter to the law establishing the Center refers to the new version of the amended law of 2012.

b) Expressly mentioned as a responsibility of other(s) structure(s) in the n.º 3 of article 2.º-A. In fact that is what results from mentioning that the Center being created "*also operates in conjunction and close cooperation with the responsible national structures by cyber espionage, cyber defense, cyber crime and cyber terrorism*", r.e. other structures.

And despite its mission including the "*implementation of measures and instruments needed to anticipate, detect, react and recover in situations which, imminence or occurrence of incidents or cyber attacks, may jeopardize the functioning of critical infrastructure and national interests*" (at the end of n.º 2, article 2.º), the competences of the Center do not "*affect the powers and competences assigned by law to other public entities in matters of cyberspace security and is exercised in coordination with these*" (n. 2 of article 2.º-A). Meaning that the Center has, operationally at least, more of a coordination role.

That seems to be made explicit by the law itself when, in the following rule (n.º 3 of the same article 2.º-A), states that the Center also "*works in articulation and close cooperation with the national structures responsible for cyber espionage, cyber defense, cyber crime and cyber terrorism*". Such an interpretation is misleading, as, in continuation of the previous rule, what is here stated is that in this cases – which include Cyber Defense – the Center has less intervention.

Had we any doubt and paragraph h) of n.º 1 of the same article 2.º-A enlightens us by "empowering" the Center only to "*ensure the planning of the use of cyberspace in crisis and war situations, within the civil emergency planning* (context)".

Summarizing, the Portuguese National Cyber Security Center was established by a Law that only refers to Cyber Defense to state it is a duty of other agency(ies), further clarifying that even in a state if war, the Center is confined to continuity planning in the framework of civilian emergency response.

3.3.2. The National Strategy for Cyberspace Security (hereinafter "Cyber Security Strategy"). As a National strategy should, this one starts with an holistic view of the threat and pursue of objectives.

Among other less relevant themes for our purpose of accessing the Portuguese view of a distinction between cyber security and cyber defense, the Strategy, in its

preamble, refers at length the public, national level of a threat to the sovereignty and survival of the State:

"*The society, the economy and the state are dependent on information and communication technologies (ICT). We have witnessed* (…) *a growing reliance on ICT in vital functions of running the country.* (...)

Internally as international there are evident capabilities of political and religious activisms, criminals or terrorists to conduct actions impacting on the safety of critical information infrastructures, creating serious threats to the survival of democratic rule of law State and the space of freedom, security and justice.

The need to protect the areas that embody national sovereignty, ensuring the political and strategic independence of the country, as well as the growing number of incidents and malicious attacks, require that the security of cyberspace is regarded as a national priority."

These words immediately take us to identify an analysis that points to what might be called a Defense level event (threat, with reactive strategy, planning and operations).

It is this national Cyber Security Strategy that, in the 3rd paragraph of the first of its "six axis of intervention", explicitly sets the goal of developing cyber defense capabilities.

Three aspects of this strategy should be highlighted:

i. The mention to the command and control authorities, with the strategic responsibilities committed to the JCS and the planning and immediate response to the Cyber Defense Center and the branches – paragraph c) of n.º 3 of Axis 1;

ii. The reference to the dual use of military capabilities in this regard, i.e. promoting the use of military capabilities not only in military operations but also in national cyber security, including information sharing – paragraph d) of n.º 3 of Axis 1;

iii. A rather detailed set of objectives for a cyber defense capacity (and capabilities) building (infra) – paragraph c) of n.º 3 of Axis 1.

Regarding this later, and given its relevance for our understanding of the Portuguese conceptualization of "cyber defense", we follow the original wording, which this Resolution carries from an earlier, and still in force, Order of the Minister of Defense (Despacho n.º 13692/2013, from October 28th), establishing the "Political Guidance for Cyber Defense". This document is rather clear when addressing the objectives of the Portuguese Cyber Defense, which are not necessarily only defensive:

"*The objectives of cyber defense policy are:*

1) To ensure the protection, resilience and security of networks and ICS of National Defense against cyber attacks;

2) To ensure the freedom of action of the country in cyberspace and, where necessary and directed, proactive exploration of cyberspace to prevent or hinder their hostile use against the national interest;

3) Contribute cooperatively to national cyber security."

Clearly this wording is in sharp contrast with all the caveats and uncertainties of the academic approach. Yet it is here, in Defense policy, that we find clear basis of the distinction made by the Portuguese decision makers. If, in security, continuity and resilience are the objectives, in Defense the full spectrum of planning and operations may be considered, including the dual use of the force.

4. CONCLUSIONS.

The international conceptual diversity is somewhat mirrored in Portugal, with the available debates revealing the usual uncertainty about the distinction between cyber security and cyber defense.

At times there seems to be some reluctance in addressing military aspects of cyber security (as if the prohibition of some sort of *posse comitatus* of the military would not be as inadequate as the distinctions between domestic and foreigner in intelligence gathering). Since our subject doesn't dwell on civil rights and privacy, we will not anticipate any reasons for the absence of the military references in the civilian discourse.

We can find in the official cyber security centric documents a discourse much closer to safety, awareness, research and development. The operational emphasis is then guided to continuity of service: with prevention, recovery and resilience, all mainly aimed at critical infrastructures.

Oddly, it is the "Political Guidance on Cyber Defense" (an Order by the Minister of Defense) and the later "National Strategy for Cyberspace Security", which both recognize the needed interaction between cyber defense and cyber security. Thus admitting the need of capabilities, but building the bridge from the military unto the civilian side of the equation, and affirming the (necessary) dual use of such military capabilities.

In this sense we tend to follow the Defense´s view: the distinction is usually pointless, given the shared area of operations and the vast majority of actions. The differences may occur on the level of classification of the information on or about certain critical infrastructures (although far more civilian critical infrastructures are more vital), or in what is euphemistically or unintentionally called "*proactive exploration of cyberspace*" in the text of the "Political Guidance for Cyber Defense".

We can, in any case, affirmatively state that (like with reality and fiction) policy is, in this regard, more advanced then academia.