Alocução de Sua Excelência, o Ministro da Defesa Nacional da República Portuguesa, Professor Doutor José Alberto Azeredo Lopes, à sessão de Abertura da 2ª Conferência NATO sobre Ciberdefesa e os projetos de *Smart Defense*

Lisboa, Academia Militar, 28 de abril de 2016

Address by His Excellency, the Minister of National Defence of the Republic of Portugal, Professor José Alberto Azeredo Lopes, to the opening session of the 2nd Conference on NATO cyber defense and Smart Defense projects

Lisbon, Military Academy, 28 April 2016

Your Excellences, Ambassadors, Admirals, Generals,

Distinguished Guests,

Ladies and Gentlemen,

Allow me to start by saying how delighted and honoured I am to welcome you in Lisbon, at the Military Academy, for the *2nd NATO Conference on Cyber Defence and Smart Defence Projects.* Building upon last year's successful first edition, our initiative, fully supported by NATO Allied Command Transformation and by NATO Industry Cyber Partnership, reflects Portugal's commitment to the development of cyber defence, a critical dimension of our "common security" environment, in the era of globalization.

Indeed, since someone famously enunciated, in the last decades of the XXth century, that "time-space compression" was to be the "condition of postmodernity" that our world has continued to "speed up" and "spread out", as a result of technological innovations that elide spatial and temporal distances.

These have become an essential facet of contemporary life, one which we tend to look upon – and rightly so, I believe – in a positive light, because of their emancipatory potential at the economic level - with a new labour market emerging online – because of their cultural added value - as they make people from distant cultures easily mingle – or, finally, and more simply, because they

improve our daily lives, providing us with all kinds of services and connecting us to our beloved ones.

Thus, in the course of the last two decades, the world became more and more interconnected and highly dependent on the open, unimpeded and secure access to *internet* and *cyberspace*. It is a fact that we now rely on networked computing for all manner of economic, social, and civic activity. Therefore, it almost goes without saying that this dependency must be taken into consideration by our defence strategies, both at the national and at the international level. It requires that we redefine our analysis of the current security environment and that we courageously keep adjusting NATO's strategic vision, so that it moves on to encompass - at its heart and without hesitation - the development of an effective cyber defence cooperative methodology.

Cyberspace is often described as the new "strategic fluid": with its ultra-high speed and its omnipresence, it has already become the fifth domain of military operations, as critical to national and international defence as the classical domains of land, sea, air, and space. At the same time, it represents a challenge to traditional military concepts at every level of the prevention of warfare: strategic, operational, and tactical. The highly disruptive potential of a cyber-attack can be illustrated by simply reminding ourselves that NATO and all of us rely heavily on networking technologies to efficiently conduct missions and operations across the globe.

And there are indeed decisive issues in this area, ranging from the protection of national critical infrastructures to the safety of the Armed Forces' communications and information systems, at home and overseas. The risk of a loss of confidentiality, integrity, and availability of data resources, degrading our

ability to fulfill our missions, should lead us to set up an efficient operational framework for establishing situational awareness in cyberspace.

There is no room to question how fundamental it has become to acquire a better understanding of the *if*, *why* and *how* different actors may seek to exploit cyberspace in order to affect military capabilities and operations at NATO, EU or national levels. By the same token, robust, resilient and interoperable cyber defence capabilities are now required to support NATO structures and the Alliance's missions and operations.

In this regard, however, and although many nations have recently made great progress, we all must acknowledge there is vast room for improvement and that's where *smart defence* has a major role to play. In a context of severe budget constraints and scarcity of resources, *smart defence* emerged, in recognition of our vulnerability to cyber threats and as we sought to develop, practically, the cyber defence capabilities NATO needs to face future challenges.

Thus, let me elaborate briefly on some of the highlights of NATO's *Smart Defence* Projects and of Portugal's contributions in this field.

Allow me to mention, in this regard, the Multinational Cyber Defence Capability Development (MN CD2) Project, led by the Netherlands, the Malware Information Sharing Platform (MISP) Project, led by Belgium, and, "last but not least", the CIS E-Learning Project, led by Portugal.

In addition to this project and more prominently, as a founding member of the Alliance, committed to innovation and "transformation", Portugal will undertake to play a pivotal role, in leading the Nations to embrace cyber defence as part of the "core business" of the Alliance. Following the 2010 Summit, and with the

relocation of the NATO CIS School from Latina, in Italy, to Oeiras, near Lisbon, the School will "transform" into an Academy, the NCI Academy, with the acronym standing for *NATO Communications, Information and Cyber Academy*.

And it is a shared goal of Portugal and the Alliance that the Academy will come to perform a crucial role in *NATO's Cyber Defence Capability Development Process*, notably at the level of education, training and qualification of human resources. That is why, Portugal is also the leader of another *smart defence* program - the Multinational Cyber Defence Education and Training Project -aiming at setting up a *Cyber Defence Curriculum*, which will lay the conceptual, doctrinal and didactical foundations of the Academy's future labour.

As the host nation of this NATO Academy, I can assure you, Portugal is firmly engaged in supporting the on-going efforts to better qualify our common military structures and personnel in the field of cyber defence, while seeking to foster a new cooperative culture in this domain.

My speech would be incomplete, though, if I did not – even if only briefly - address the efforts of the EU in this field. As a matter of fact, I am convinced that, in general, a stronger complementarity between the EU and NATO is a geopolitical necessity, in our current security environment, and that cyberspace is the field *par excellence* where the two organizations can start bridging their distinct strategic cultures.

On the EU front, thus, allow me to mention that Portugal and France were appointed, in July 2015, as the Lead Nations of the *Cyber Defence Discipline* of the European Union Military Training Group and will also assume the responsibility to manage the future EU Centralized Cyber Defence Training and Exercises Platform. It is expected that this platform will be able to support three different domains

(EU, national and international) and will take on, in the future, a central role in what concerns *cyber security and cyber defence education and training.*

To sum up, by becoming a hub in the network of centres of excellence, Portugal stands ready to contribute and support stronger cooperative NATO-EU ties and enhance a cyber-defence strategic culture.

I am certain, in this regard, that the attainment of this Conference's objectives will contribute to strengthen national synergies and foster cooperation between all meaningful stakeholders towards a more open, inclusive and secure cyberspace.

Finally, I would like to end by noting that: as we prepare for the upcoming NATO Summit, we should keep in mind that the Alliance must do its part in forging a global consensus on the governance of the internet, so that the latter can serve the socioeconomic aspirations that our civil societies bestow upon it. Therefore, Warsaw should be the right occasion for us to uphold a *Cyber Defence Commitment* at the highest level, one which provides for the periodic assessment of its implementation, so as to ensure its credibility and effectiveness.

And on this note, your Excellences, dear High Military Officials, Ambassadors, distinguished guests, I wish you a challenging and productive conference, hoping it can feed the highest level of decision-making in the forthcoming times, inspiring the Alliance to take unequivocal steps in this matter of cyberdefence.

Take you for your attention,