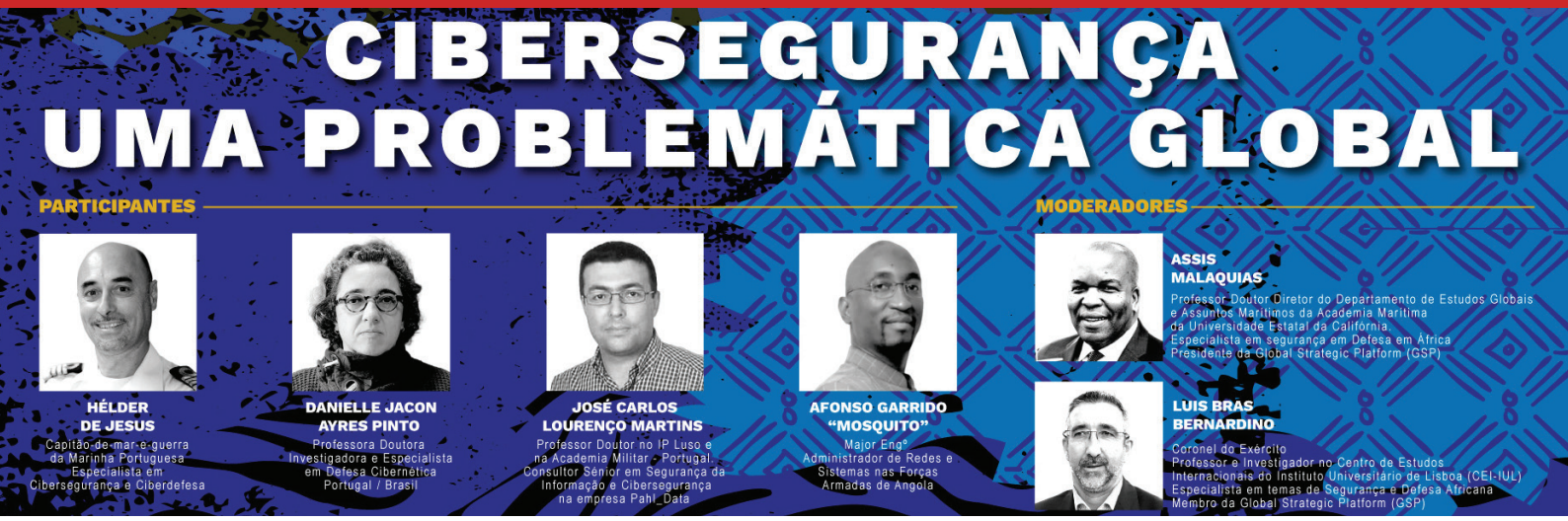
AFRICA SESSIONS

G|S|P GLOBAL STRATEGIC PLATFORM

FUNDAÇÃO MILLENNIUM BCP



CYBERSECURITY. A GLOBAL PROBLEMATIC

INTRODUCTION

Cyberspace has been changing the way our society works in our days, this applies to Individuals, Organizations, Corporations, and also to States.

The social barriers were eliminated, barriers like the geography or the concept of space and frontiers, because the physical gap became irrelevant, or timeless, meaning that the time zone and the relative gap lost their geopolitical and geostrategic significance.

In contrast, cyberspace allows us to carry out many different activities, being that most of them are associated with social and economic development, but others come from harmful interests from our society.

This last one is associated with actors that take advantage of the easy anonymity that cyberspace has to offer, the feeling of unaccountability that comes along as well as the difficulty of holding someone accountable. This becomes a challenge to the services that watch over their citizen's protection, also their companies and countries, like in Africa, a continent where this topic is still unknown. With this in mind, it considers that the asymmetrical and disruptive nature of the actions is a particular characteristic of cyberspace, this makes the protection and the defense of public interests more needed.

Cybersecurity works in this specific domain and has become an essential paradigm in the society that now is part of our global reality, particularly in Africa, were this problem starts to affect the society.

By this means it's important to discuss, comprehend, and establish behavior patterns, as well as to conduct rules that will guarantee that our integrity, security and sovereignty will prevail.

About the use of cyberspace, we have witnessed a big evolution that represents the globalization of mostly everything that involves our relationship with society.

During the 80s cyberspace didn't exist. However, during the 90s, cyberspace started to be present on our agendas, still with low relevance and mostly oriented towards information and communication. In the last 10 to 15 years cyberspace became a new geopolitical reality that had an impact on the world. Some examples are the situation that Estonia lived during 2007; the creation of a Military Command for Cyberspace by the US in 2015 and also the presidential elections in 2016, and more recently the attack of big international companies and the easy access to database websites of Governments and enterprises throughout the entire world, in particular in Africa.

Currently, almost everything happens in cyberspace, and cybersecurity became a priority for Organizations and States. Human security is now related to cybersecurity and the development started to depend on security on its cybernetic dimension.

Portugal's point of view as answers for the cybersecurity

Cyberspace consists of a complex environment, with interest and values, embodied in an area of collective responsibility. This results from the interaction between people, networks, and information systems. In this perspective, Portugal developed, in 2015 and updated in 2019, the "National Strategy of the Cyberspace Security 2019-2023". This Strategy clarifies a vision of a safe and thriving Portugal through an innovative, inclusive, and resilient action. That preserves the fundamental values of the Constitutional Democratic State and guarantees the regular performance of the institutions in the face of digital evolution in the society.

It is also established as principals: subsidiarity, complementarity, and proportionality, so that the strategic goals that go through maximization of resilience, promotion and innovation, are reached and also to generate and guarantee resources.

This strategy presents six operational axis: governance; prevention, education, awareness, the protection of the cyberspace and the infrastructures; response to the threats and the fight of the cybercrime; investigation, development, and innovation and lastly the national and international cooperation. The same strategy also establishes the concepts of Cybersecurity, Ciberdefence and the principals how to fight against cybercrime and cybercriminality.

States suitability of the Cyberspace – The main answers to the cyberthreats

In Portugal, the Information and Security Service (SIS) has a department that focuses on cyberspace and created (2014) the National Center of Cybersecurity (CNCS). In 2015 created also the Ciberdefence Center (CCD) and in 2016 the National Unity of Cybercrime and Technologic Crime Combat (UNC3T). These four elements (G4) form a group that works and shares information to fight the threats of cyberspace.

They accept four dimensions of security in Cyberspace: the Defense; connected to the

sovereignty; mission accomplishment and the military operations in the Cyberspace; the Security "per se", which relates to fighting Cybercrime, protection of critical infrastructures and essential service operators; the markets for the economic development, directly connected to the rights, liberties, and guarantees, freedom of speech and privacy.

In terms of legislation, Portugal because is a member of the European Union (EU), transposes to the legal intended board the main collective documentation about cyber. And in this sense, it can be referred to a directive aimed at guaranteeing network security (SRI/NIS - 2016) that was transposed through the Portuguese Law nº 46/2018.

This document has established an administration of cyberspace to a national level and the High Council of Cyberspace Security (CSSC), it's important to highlight the CSIRT national network, the creation of the National Cybersecurity Authority, and the CERT.PT domain, as the point of contact for the response to cyber incidents of security.

The rules of procedure (EU) 2019/881 was also transposed to the Portuguese legislation, throughout the Decree nº65/2021 30 of September, that establishes the minimum requirements of security and the implementation of a national board of certification for Cybersecurity. Establishes the need for permanent points of contact, active inventory, annual reports, notifications of the incidents, and other components.
Concerning the military component, the Portuguese Ministry of National Defense considers ciberdefence and interoperability priorities. It has political orientations ratified for cyber defense and has the intention of ratifying a strategy for this specific area. Because cyber defense is a priority for the Portuguese Armed Forces.

Regarding the Portuguese Major General Staff of the Armed Forces, there is a guideline that was established between 2018-2021 witch dictates, as one of the main goals, the creation of ciberdefence capability. It was established five lines of action, specifically: the strategic formulation, the reinforcement of connections between national and international entities, increase the sensibility, and establishing the schooling of Cybersecurity and Cyberdefense at the Military University Institute (IUM).

The Impact of security in Cyberspace. The main threats that affect Enterprises and States. On the current geopolitical panorama, it exists a triad that involves the EUA, Russia, and China and their constant quest for power, and "... the geopolitical threats fit in that dynamic currently faced by the world..." as stated by Professor Danielle Ayres Pinto. The main threats of the Enterprises and the States are the constant theft of data; cybernetic espionage; disinformation and fake news. This last one is considered also by Professor Danielle Pinto as "... one of the most complex cybernetic threats because it can't be controlled...".

The companies, as the main actors of cyberspace, are directly affected by the cybernetic attacks, which means, that it impacts their economy and their capability of providing their products to citizens. Enterprises that are connected to critical infrastructures and are vital services of the society are the ones that suffer the most. The big problem for the States it's the way they control the order of cyber-attacks, how they ensure the citizen's protection, the operation of the basic Institutions, and their democracy role.

According to Professor Lourenço Martins, the issue of the threats is related essentially to the effects and the actors, because "... in the effects and actor´s perspective it is effectual, the cyberespionage, the attacks of the critical infrastructures and essential service providers, the organized cibercriminalization and the manipulation of the public opinion are the main threats of the cyberspace...".

Major Mosquito Garrido from Angola says that "... in our day's information is power, the one that owns it, owns the power....". In this regard, most of the start of current problems have an attempt to acquire information by illegal means, like cyberespionage, sabotage of the critical infrastructures and other States and Enterprises, industrial espionage, and criminal organization activities in cyberspace.
For him it is necessary to take into consideration the fake news and manipulation of the public opinion, since "... it became relatively common the dissemination and manipulation of the information, installing the panic on their readers...", especially when it affects the vital services of the State.

Due to the covid-19 pandemic, the world spread to the digital, this turned the digital economy fundamental and key for the global economy. With the emigration to the digital space, we now share cyberspace and the internet, which means we become active agents in cyberspace and possible victims of cyber criminality. Major Mosquito uses as an example the case of Angola and Portugal, where some banks and institutions saw their services compromised, just like their technological infrastructures. Saying that, he underlines "... it's important that the Governments, being this a global problem, to strengthen themselves so they can prevent and mitigate the risks of the cyberspace..."

Looking at solutions for the main threats on the Cyberspace

In today's geopolitics, we must think beyond the traditional conflicts, making cyberspace part of the strategic plans. As it was mentioned by Professor Danielle Ayres Pinto "... to solve the threats of cyberspace it's not enough to have technical skills as a way to ensure the protection process, it is necessary to understand the dimensionality of this attacks and know how to proceed...". The solutions are the investment in cybernetic security systems, suitable to protect and prevent possible attacks; maintain control of the data and conceive, to the cybernetic security, the same recognition and investment as the traditional threats. Apart from that, it is necessary to proceed with "cybernetic sanitation", by educating the citizens so they won't be vulnerable actors.

For Professor José Carlos Martins, a possible solution would be "... to work on the maturity based on the certification of organizations and the use of artificial intelligence...".

The triad, international cooperation, politics, and compromise revealed themselves as fundamental in the search for solutions to the cyberspace threats. Like it was mentioned also by the Navy Captain Hélder de Jesus "... politics emerge of the need to put cybersecurity as a governmental priority, and the need to sensitize the population about this subject. the subject of compromise emerges because the Cybersecurity should be seen as an investment and not as a cost when we invest on the cyberspace the State, the Enterprises and the society will benefit from it...".

Perspectives for the future of the Cybersecurity

The challenges can be arranged in three essential areas: human resources, innovation technology, and leadership, as was mentioned by the Navy Capitan Hélder de Jesus. Regarding human resources "... one big challenge will be the lack of good professionals. Concerning technology, he refers to the fact that as it gets more advanced so does the complexity of the attacks and threats. Last but not least, is the leadership, it's the area that has to ensure the investment in Cybersecurity, so it can generate and create additional resources".

Now focusing on the perspectives for the future, essentially there are six main challenges, states Professor Danielle Ayres Pinto. The first one is to know how to protect the data of Enterprises and States and prevent them from being used for scrupulous purposes. Second how to create a mutual trust among companies and States. Third is to know how to control and prevent the spread of fake news and disinformation; Fourth, how to promote the risk management. Fifth, how to prevent the computer from becoming a weapon and last how to prevent the people from becoming disposable due to not knowing how to work with the system, turning invisible to the cybernetic world; and finally how to achieve the technology equality, both in States and as individuals.
According to Major Mosquito Garrido "... technology is constantly changing and metaverse is going to be a challenge to the Cybersecurity, because it will turn the Cyberspace into a differentiated space...". He also says that artificial intelligence and machine learning will eventually become decryption machines of today's technology and ".... one of the challenges is to prevent that technology from falling into the wrong hands, so global security won't be compromised.

We can conclude that it will be necessary to manage the complexity of the existing systems to align them with security pointers (indicators). Sensitize people about the dangers found in cyberspace, so they can adopt a culture of security and accountability and invest in training cybersecurity experts.

Conclusion

In conclusion, according to Professor Luís Bernardino and Professor Salim Valimamade, cyberspace will be the most complex informational platform, this meaning that network knowledge will be a powerful factor for States and Organizations with impact the society. With this in mind, cybersecurity and ciberdefence are support tools to the development and central element on the capacity of controlling and swaying information.

In a world increasingly global and interdependent, technology operated by States, Enterprises and Organizations reveal the main role of the "technologic man" and the necessity of investing on cybersecurity as a survival condition and, for the States the cybernetic sovereignty is a basic condition to have a more secure and developed society.

Lisbon, 26 February 2022
Amilly Soares
Beatriz Maria de Abreu Gomes