Posted on the CEEEP website
Date: November 18, 2021

THINK TANK DEL EJÉRCITO DEL PERÚ

Cyber Defense Sector Policy: an urgent need

Ernesto Castillo Fuerman, Brigadier General and an electronic engineer and a specialist in Cybersecurity and Cyberdefense from the UNI-INICTEL. He holds a master's degree and a doctorate in Management and Development, as well as a master's degree in Public Management. General Castillo has been the director of the Peruvian Army's Computerized Tactical Training Center, founder of the Peruvian Army's Cyber Defense Center and chief of operations at the Peruvian Army's Cyber Defense and Telematics; likewise, he has formulated the Army's Electronic Warfare and Cyber Defense Manual. Currently, he is the commanding general of the Peruvian Army's Cyber Defense and Telematics.

Summary

The critical infrastructures of a country, the command and control systems, as well as the weapons systems have computer platforms for their operation; However, as a result of a cyberattack, these platforms could become useless and paralyze a country, putting National Security, Defense and Development at risk. Therefore, it is essential to have a Sectorial Cyber Defense Policy, whose objectives and guidelines allow strengthening the development of capacities to neutralize threats and attacks in and through cyberspace, promoting culture, education, as well as Investigation, Development and Innovation. (I + D + i) in cyber defense among the Armed Institutions. This article analyzes the situation of Cyber Defense in Peru and proposes the statement, as well as the objectives and guidelines of the necessary Sectorial Cyber Defense Policy that the Peruvian State should have.

Keywords: Cyber attack, Cyber defense, Cyberspace, Cyber Defense Sector Policy.

Introduction

The increase in threats in cyberspace, as well as the use of new technologies to generate computer threats are common concerns in all countries, given that they significantly impact information security (in public and private spheres) and even, in the critical national assets and key resources of a State. In Peru, Law No. 30999, Cyber Defense Law, approved on August 26, 2019, defines Cyber Defense as the military capacity that allows to act against threats or attacks carried out in and through cyberspace, when these affect National Security[1]. Therefore, the development of capacities in the Armed Forces (Armed Forces) to face cyber attacks and cyberwar is an urgent need in the Peruvian State since, otherwise, sovereignty, national interests are put at risk, critical national assets and key resources of the State. However, in Peru, there is a lack of a Cyber Defense Sector Policy to guide the development of these capacities in the armed forces.

Taking into account the author's experience in having served as Director of Policy and Strategic Planning for Defense in the Ministry of Defense, this article analyzes the situation of Cyber Defense in Peru and proposes the statement, as well as the objectives and guidelines of the necessary Sectorial Cyber Defense Policy that the Peruvian State must have.

Cyber attack on estonia

The first large-scale cyber attack against a state was carried out in April 2007 in Estonia. As a result of this attack, the main public and private institutions in Estonia were paralyzed by an avalanche of cyberattacks that targeted numerous institutions, including Parliament and various ministries, as well as banks, political parties and the media. Faced with this, Estonia had to cut the entire internet line and format all its systems[2].

The cyber attack on Estonia revealed a new way of waging war, being able to ensure that the difficulty in identifying those who carried out the attack and the nature of the means used changed the image of what would be the conflicts of the future. In this regard, the Director of the Estonian Computer Security Center indicated that everything was very confusing in the days preceding the attack because they did not understand what was happening; He also stated that the magnitude and impact of the attack were much greater than they could have imagined. During these events, hackers attacked, replacing the portals of the official pages with insulting images against the Estonian Prime Minister. Internet traffic skyrocketed to saturate the servers and the Estonian population took to the streets of the capital as they felt that their government was gradually losing control of the situation. When the Defense Ministry tried to find out what was going on, it discovered that not only the news agencies had been attacked but also large commercial banks which, in a small country like Estonia, was a major concern at all levels. The cyber attack was on the verge of generating a revolt, as Estonians of Russian origin invaded the center of the capital, while computer systems were blocked, the distribution of gasoline and bread was interrupted and anarchy spread throughout the country[3].

In response to this cyber attack, the North Atlantic Treaty Organization (NATO) implemented in Tallinn, the Estonian capital, the NATO Cooperative Cyber Defense Center of Excellence, currently being considered a benchmark in cyber defense worldwide. Also, in January 2008, NATO enacted the Cyber Defense Policy with the aim of improving the Alliance's ability to protect its critical information and communications systems against cyberattacks[4]. Subsequently, in Warsaw, in July 2016, the NATO member Heads of State and Government pledged - through the Cyber Defense Pledge document - to be alert to cyber threats and to be able to defend themselves in cyberspace, as it occurs in the land, air and maritime domain, recognizing cyberspace as a new domain of military operations[5].

Cyber defense in Peru

After the case described, it is undeniable to affirm that the Peruvian State needs to create the environment and the necessary conditions to provide effective protection in cyberspace and face the threats that threaten its security. In this sense, taking into consideration that the Armed Forces require comprehensive action against cyber threats, it is necessary for Peru to have a Sector Cyber Defense Policy.

In this regard, in 2017, the Defense Policy and Strategic Planning Department of the Ministry of Defense formulated a draft Directive that established the Defense Sector Policies on Cyber Defense. This draft Directive -although it was not approved with a Ministerial Resolution- was taken into consideration for the formulation of the Multiannual Sector Strategic Plan (PESEM) 2017-2021, the same one that to achieve its Strategic Objective 1 (Guarantee National Defense) contemplated the implementation of Strategic Action 1.7 (Develop Cyber Defense protecting the critical infrastructure of the State from cyberattacks)[6]. Even the Institutional Strategic Plan (PEI) 2018-2020 of the Defense Sector contemplates achieving Strategic Objective 6 (Develop institutional Cyber defense)[7]. To this end, both the Joint Command of the Armed Forces (CCFFAA) and the Armed Institutions have created their cyber defense entities, promulgating Law No. 30999, the Cyber Defense Law.

In this regard, on March 25, 2019, the CCFFAA activated the Cyber Defense Operational Command (COCID), inaugurating its facilities on January 20, 2020[8]. The COCID has three Components (land, naval and air). On the one hand, the Land Component is made up of the Army Cyber Defense Center, inaugurated on October 29, 2018[9]. On the other hand, the Naval Component is made up of the Navy Cyber Defense Command, inaugurated on February 21, 2019[10]. Likewise, the Air Component is made up of the Air Force Cyberspace Operations Group, inaugurated on December 21, 2019[11].

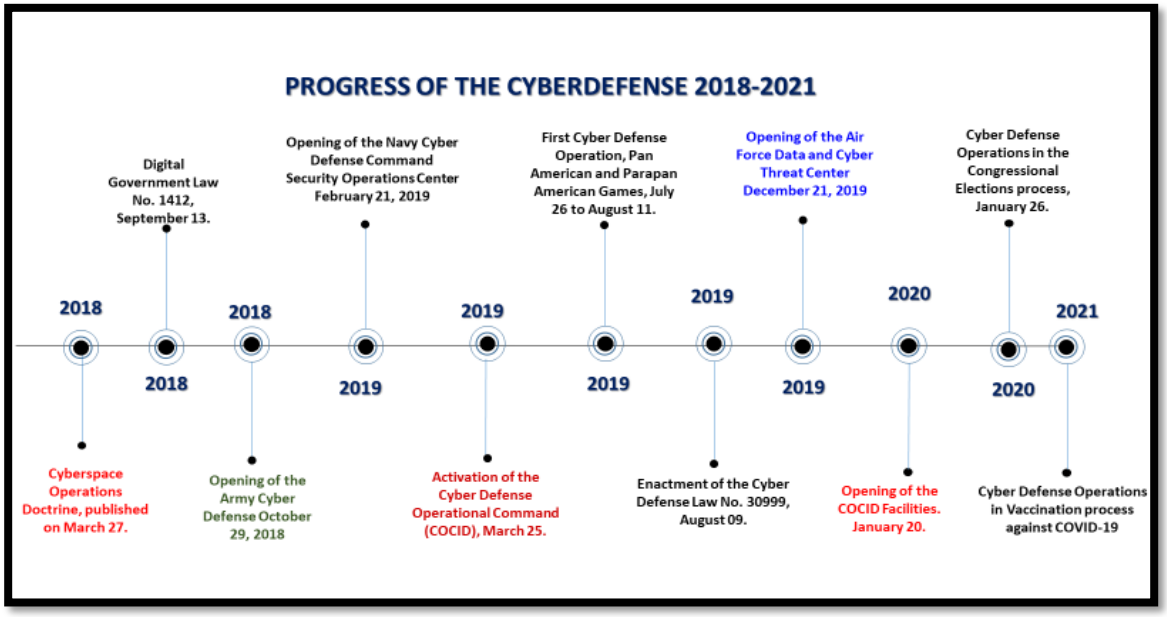

Figure 1. Progress of Cyber Defense in Peru Timeline (Own elaboration)

To date, COCID has carried out cyber defense operations during the XVIII Pan American Games and VI Parapan American Games in Lima 2019, the Congressional Elections of January 2020 and the execution of the COVID-19 Vaccination Plan for 2021. All of these Experiences have served to understand and identify the weaknesses of the Peruvian State in the digital environment, especially in the national critical assets of the public sector, which would lead to jeopardizing sovereignty, national interests, critical national assets and key resources of the State.

In this sense, Article 12 (on the control and protection of national critical assets and key resources) of Law No. 30999, Cyber Defense Law, states that "*the CCFFAA is in charge of the Cyber defense of national critical assets and key resources, when the protection capacity of its operators and / or the sector responsible for each of them and / or the National Intelligence Directorate is exceeded, in order to maintain national capacities, in the field of national security.*"[12] Therefore, to effectively fulfill this function, the Government must allocate the necessary resources to strengthen and develop capabilities in Cyber Defense of both the COCID and its Components.

Likewise, it is essential to formulate, approve and implement a Cyber Defense Sector Policy that indicates the objectives and guidelines that must be achieved by the Defense Sector. To this end, a proposal of the statement of this Policy is provided below, as well as its objectives and guidelines in order to provide ideas and facilitate their necessary formulation. In this sense, the statement of the Cyber Defense Policy could be: "Count on Armed Forces with an adequate Cyber defense capacity to face threats or attacks carried out in and through cyberspace, which put at risk sovereignty, national interests, national critical assets and key resources to maintain national capacities, considering the weaknesses of the State in the digital environment".

Likewise, taking as a reference the draft Directive formulated by the Policy Direction and Strategic Planning for Defense of the Ministry of Defense and the experiences obtained in recent years, the objectives and guidelines of the Sectorial Cyber Defense Policy could be the following:

Objective 1: "*Strengthen the cyber defense capacity of the armed forces to neutralize threats and attacks in and through cyberspace when they affect national security*", proposing -to this end- the following Guidelines: (1) Strengthen the COCID in order to neutralize cyber threats and respond to cyberattacks that threaten national security. (2) Enhance the military capabilities of the cyber defense organizations of the Armed Institutions, ensuring the cyberspace used by land, naval and air forces, as well as the cyberspace of critical assets and designated key resources. (3) Improve the capacities of the armed forces to have timely information against a possible cyber threat, developing early alerts and supporting operations against cyber attacks.

Objective 2: "Promote culture and education in cyber defense in the armed forces.", Proposing the following Guidelines: (1) Raise awareness among the personnel working in the Defense Sector of the risks derived from activities in cyberspace, in order to

consolidate the culture of cyber defense. (2) Develop knowledge, skills, experience and technological capabilities in the institutions of the sector to support and meet cyber defense objectives, certifying educational quality. (3) Promote the education, training, specialization of personnel in undergraduate and postgraduate courses and programs in Cyberdefense.

Objective 3: "To develop Investigation, Development and Innovation (I + D + i) in collaborative Cyberdefense between the Armed Forces.". For this, the following Guidelines are proposed: (1) Improve the Policies for I + D + i in cyber defense so that they are adequate and timely. (2) Implement infrastructure and adequate equipment for I + D + i in cyber defense. (3) Promote I + D + i projects culminated in the Armed Forces (4) Promote collaboration in I + D + i between the Institutions of the Armed Forces.

Objective 4: "Promote national and international cooperation in order to have cooperative security in the digital environment", proposing the following Guidelines: 1) Increase the presence of the Defense Sector of Peru in international organizations and forums on cyber defense. (2) Sign agreements with national and international organizations of countries with which Peru shares interests. (3) Encourage coordinated participation with other public and private institutions in international cyber defense drills and exercises. (4) Increase cooperation with national and international organizations on cyber defense, seeking standardization and alignment of processes.

Conclusion

Whoever wins the cyber war will fulfill what Sun Tzu expressed: "*Generals who are experts in command always make enemy armies bow without battle, that is the maximum victory*." In this sense, the critical infrastructures of a country, the command and control systems, as well as the weapons systems have computer platforms for their operation; However, as a result of a cyberattack, these platforms could become useless and paralyze a country, putting National Security, Defense and Development at risk.

In this regard, the National Policy defines the "what to do"; Consequently, it is essential to have a Cyber Defense Sector Policy, whose objectives and guidelines allow strengthening the development of capacities to neutralize threats and attacks in and through cyberspace, promoting both culture and education in cyber defense in the Armed Forces, as well as Investigation, Development and Innovation (I + D + i) in cyber defense among the Armed Institutions, as well as national and international cooperation in order to have cooperative security in the digital environment.

Final Notes

[1] *Ley Ciberdefensa*, art. 4, (august 09, 2019) Ley N° 30999 Congreso de la República, https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678061-ley-n-30999

[2] "Los 10 ataques cibernéticos más importantes hasta la fecha," *Teinteresa* (april 19, 2013), http://www.teinteresa.es/mundo/ataques-ciberneticos-importantes-fecha_0_904110101.html (accessed january 18, 2017)

[3] *Ciber Guerrilla: Hackers, piratas y guerras secretas* (Spain, 2016), Documentary Odisea Channel

[4] *NATO Policy on Cyber Defence*, (C-M 2007)0120.

[5] https://www.nato.int/cps/en/natohq/official_texts_133177.htm, (accessed october 11, 2021).

[6] Ministerio de Defensa, *Resolución Ministerial N° 2054-2017-DE/SG* (2017)

[7] Ministerio de Defensa, *Resolución Ministerial N° 2084-2017-DE/SG* (2017)

[8] "Ministro de Defensa inauguró instalaciones del Comando Operacional de Ciberdefensa," *Gob.pe plataforma digital única del Estado Peruano* (20 de enero de 2020), press release from the Armed Forces Joint Command, https://www.gob.pe/institucion/ccffaa/noticias/505601-ministro-de-defensa-inauguro-instalaciones-del-comando-operacional-de-ciberdefensa (accessed october 11, 2021).

[9] "El Ejército del Perú inaugura su Comando de Ciberdefensa," *Maquina de combate* (30 de octubre de 2018), https://maquina-de-combate.com/blog/?p=58478 (accessed october 11, 2021).

[10] "Inauguración del Centro de Operaciones de Seguridad de la Comandancia de Ciberdefensa," *Marina de Guerra del Perú Home Page* (febraury 21, 2019), https://marina.mil.pe/es/noticia/inauguracion-del-centro-de-operaciones-de-seguridad-de-la-comandancia-de-ciberdefensa/ (accessed october 11, 2021).

[11] "Fuerza Aérea presentó moderno Data Center y Centro de Monitoreo de Amenazas Cibernéticas," *Gob.pe plataforma digital única del Estado Peruano* (december 21, 2019), prees release from the Ministry of Defense, https://www.gob.pe/institucion/mindef/noticias/71274-fuerza-aerea-presento-moderno-data-center-y-centro-de-monitoreo-de-amenazas-ciberneticas (accessed october 11, 2021).

[12] *Ley de Ciberdefensa*, art. 12, Ley N° 30999