ISSN: 2955-8018 (Print)
ISSN: 2810-899X (Online)

REVISTA
SEGURIDAD Y PODER TERRESTRE
CENTRO DE ESTUDIOS ESTRATÉGICOS DEL EJÉRCITO DEL PERÚ

Vol 2, N°2, April - June, 2023, pp. 107-113
DOI: https://doi.org/10.56221/spt.v2i2.29

ARTICLE

Cyberdefense: The Challenges of the Virtual World

Enrique Saúl Rivero Belveder

https://orcid.org/0000-0002-1830-5131

eriverob@esge.edu.pe

Cyberdefense: The Challenges of the Virtual World

Enrique Saúl Rivero Belveder

Summary

The importance and evolution of Information and Communication Technologies (ICTs) in cyberspace operations have increased the dangers posed by cybercriminals. In this sense, the platforms or systems of the country's institutions could be violated causing a national state of emergency.[1] Therefore, the Armed Forces ("FF.AA.") are subject to the provisions contained in Article 51 of the Charter of the United Nations. It is also governed by the norms of international law such as the Universal Declaration of Human Rights (UDHR) and International Humanitarian Law (IHL). The following will explain the situation of cyberdefense in Peru, the operations in and through cyberspace, the causes and consequences suffered by the country by cybercriminals, as well as recommendations, in order to improve and strengthen capabilities to detect and neutralize cyber-attacks.

Keywords: *Cyberdefense, Cyberspace, Cybercrime, Cybercriminal, Armed Forces.*

Introduction

The use of the Internet and the automation of integrated systems within the network, added to the different existing technological platforms, became one of the main objectives achieved as an organization, although they are still vulnerable to future attacks in cyberspace. This, as a concept, is the non-physical digital world where everyone can have access through a connection to the data network.

On August 26, 2019, the Congress of the Republic passed Law No. 30999, the Cyberdefense Law, Article 4 of which defines it as "the military capability that allows acting against threats or attacks carried out in and through cyberspace when these affect national security". [2] The Army's Directorate of Telematics and Statistics (DITELE) is responsible for

1 UN, "Carta de las Naciones Unidad Paz, dignidad e igualdad en un planeta sano", Naciones Unidas (2023), https://www.un.org/es/about-us/un-charter

2 CR, "Ley de Ciberdefensa – Ley N° 30999 – Poder Legislativo" El Peruano (August 27, 2019), https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

carrying out institutional strategic planning, articulating and promoting the modernization process through the automation of information systems. In this sense, the various branches of the Armed Forces are competent and capable of military cyberdefense, this comprises the Peruvian Navy, the Air Force and the Joint Command of the Armed Forces (CCFFAA).

Cyberdefense Situation in Peru

The CCFFAA activated the Cyberdefense Operational Command (COCID) inaugurated by the then Minister of Defense, Walter Martos Ruiz, on January 20, 2020,[3] located within the 6th Division of the Joint Chiefs of Staff of the Armed Forces (6th DIEMCFFAA). Likewise, COCID has three components: land, naval and air. The terrestrial one is placed under the responsibility of the Army Cyberdefense Center, inaugurated on October 29, 2018. [4] The Navy's Cyberdefense Command, was inaugurated on February 21, 2019.[5] Meanwhile, the Air Force Cyberspace Operations Group, was inaugurated on Dec. 21, 2019. [6]

Based on the aforementioned Law No. 30999, the main critical assets that could affect national security fall into three areas to be considered:

Critical Infrastructure. Sanitation sector and infrastructure, pipeline network stations, power plants and networks, water and wastewater infrastructure, national financial system, transportation system, power production and telecommunication networks.

3 CCFFAA, "Ministro de Defensa inauguró instalaciones del Comando Operacional de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas", Plataforma digital única del Estado peruano, (January 20, 2020), https://www.gob.pe/institucion/ccffaa/noticias/505601-ministro-de-defensa-inauguro-instalaciones-del-comando-operacional-de-ciberdefensa

4 MC, "Ejercito inaugura el Comando de Ciberdefensa, Maquina de Combate (October 30, 2018), https://maquina-de-combate.com/blog/?p=58478

5 Peter Watson, "La Marina del Perú emprende la mejora de la infraestructura de su Comandancia de Ciberdefensa" Infodefensa (July 2, 2022), https://www.infodefensa.com/texto-diario/mostrar/3811580/armada-peru-mejora-infraestructura-comandancia-ciberdefensa

6 MINDEF, "Fuerza Aérea presentó moderno Data Center y Centro de Monitoreo de Amenazas Cibernéticas", Plataforma digital única del Estado peruano (December 21, 2019), https://www.gob.pe/institucion/mindef/noticias/71274-fuerza-aerea-presento-moderno-data-center-y-centro-de-monitoreo-de-amenazas-ciberneticas

Information Systems. Command and control system, computer systems for institutional services, systems within the organization's private network, intelligence system of the Armed Forces and the Peruvian National Police (PNP).

Software and/or Programs for the Operation of Military Equipment and Systems. Drone piloting system and robotic process automation (RPA) equipment, tank operation system, warplane system, and submarine system.

Cyberattacks conducted by cybercriminals against the Peruvian State

Anonymous Hacks Peruvian Congress Website.[7] The famous self-styled Anonymous hacktivists are an international group of anonymous hackers, faceless and without a defined ideology. They do not belong to any political party and are distributed worldwide. Commonly, they are software specialists, who carry out sabotage as a protest against a person, government or the State itself.

In Peru, the Congress of the Republic, in November 2020, after ousting the then President of the Republic, Martin Vizcarra Cornejo, for "moral incapacity" and assuming the mandate of the Executive Branch, Manuel Merino de Lama, there were several social protests. According to the market research company Ipsos Peru, 94% of Peruvians rejected the appointment of Manuel Merino de Lama, by the Legislative Power, as head of State. This decision generated great unrest in the population, mainly among young people, who led, for six days, several protests that left more than 63 people injured and caused the death of two citizens. This situation took place at the height of the COVID-19 pandemic.

However, in this context, security in cyberspace was no longer safeguarded, which caused Peru to be the target of cyber-attacks on web portals, social networks, internal computer systems, among others, thus violating national security.

7 LV, "Anonymous hackea web del Congreso de Perú, causante de grave crisis política" La Vanguardia (November 14, 2020), https://www.lavanguardia.com/internacional/20201114/49466261194/anonymous-hackea-web-del-congreso-de-peru-causante-de-grave-crisis-politica.html

Russian Cybercriminals Attack and Steal Information from the General Directorate of Intelligence (DIGIMIN) of the Ministry of the Interior

Among the most critical events in the country, on April 29, 2022, hackers from Russia affected the national intelligence system. The cybercriminals, self-styled *Conti Group*, claimed that they managed to access the computer systems of the General Directorate of Intelligence of the Ministry of the Interior (DIGIMIN), due to the lack of data encryption within the network, which is recurrent in many digital platforms of state institutions.

Conti Group stole secret documents and demonstrated it in a blog, with the following message: "They will suffer very seriously if these are made public. Torture, intimidation and surveillance is what the intelligence department is famous for. Almost all of them are classified as secret," they said..[8] Its purpose was to negotiate payment in exchange for information. "You must understand that this is sensitive information (...) take care of it. We want to remind you, once again, that we are only interested in money. We are not interested in politics. If you ignore this message, a cybercrisis awaits you." However, they never specified the capital requested.

This organization uses malware, known as ransomware, a malicious program used to hijack data through the cyberspace network, intended to cyberattack state entities and private companies worldwide. This time the victim was the Peruvian State.

Based on these cyber-attacks, we recommend that the CCFFAA, through COCID, implement the single cyberdefense directive for the operation of the Armed Forces, considering the following:

- Add cyberdefense to the curriculum design and syllabus in officer and non-commissioned officer training schools of armed institutes, to promote a graduate profile that contains the vision of the cybersoldier.

8 LR, "Hacker rusos exigen pago millonario al Ministerio del Interior", La República (April19, 2022), https://larepublica.pe/politica/2022/04/29/hackers-rusos-exigen-pago-millonario-al-ministerio-del-interior-ministerio-del-interior-pedro-castillo-mdga/

They, digital natives, will be responsible for the critical assets of an entire country.

- Promoting research, development and implementation of projects, as well as conducting competitions between armed institutes. Research is the creative work on how to create technological projects with the use of science and technology to strengthen cyberdefense and, in this way, develop and implement security and backup of critical assets. Also, to encourage competitions, at least one competition per year should be held among the armed institutes, such as: CCFFAA, EP, MG, FAP, and *Capture The Flag* (CTF).
- The Armed Forces must bear the responsibility of managing and providing security to the critical platforms of the Peruvian State. Three components of the COCID: Army Cyberdefense and Telematics (land), Navy Cyberdefense Command (naval) and Air Force Cyberspace Operations Group (air), which must provide the administration and proficiency to prevent and conduct actions in response to cyber-attacks by accessing the servers and data network of the different technological platforms.

Conclusions

The world is currently governed by the digital era where technology is constantly being renewed and developed. Wars are not won with tanks, rifles, armaments, or military reserves, but with highly trained personnel in cyberdefense-related IT resources. A simple piece of *malware* can cause a national state of emergency.

One of the objectives for which the title of cybersecurity and actions in cyberspace was placed on modern warfare is that the institutions of the Armed Forces can act in defense against possible cyberattacks. Therefore, there is a need for a single cyberdefense directive that includes the recommendations in the points mentioned above.

About the author:

Enrique Saúl Rivero Belveder is a Lieutenant in the Peruvian Army, Systems Engineer from Universidad César Vallejo, with a degree in Military Sciences from Escuela Militar de Chorrillos and a bachelor's degree in education from Universidad Ricardo Palma. He also holds diplomas in Geomatics from the National Geographic Institute and in Risk Management and Natural Disasters from the Army War College. His areas of interest are education, teaching and cyberdefense.