



Cyber-Security in Peru

OE Watch Commentary: Cyber-attacks are nothing new, and while nearly all countries work stringently to avoid being the target of hackers, the cost to do so is high. Many countries with limited economic resources are not able to protect themselves as well as developed countries. The accompanying passages discuss Peruvian cyber-security considerations and actions the government is taking to mitigate possible threats, including the new Cyber-Defense Command at the Army Headquarters in Peru.

According to Peruvian news source *El Comercio*, the Peruvian government realizes that in order to protect itself against cyber-attacks, they need budget increases and a strategic vision. The passage notes that Peru currently spends 0.07% of its GDP to counter cyber-attacks. The Peruvian news source *Conexión Esan* discusses the government's strategic vision on the issue.

At present, Peru is working to expand its cyber-defense strategies. In fact, the country is already using the military to counter actual and potential attacks as discussed in digital military journal *Dialogo*. Proof that the country is taking cyber threats and security seriously is the new Cyber-Defense Command at the Army Headquarters in Peru. This center initiated operations in late October 2018 and is equipped with cutting edge technology. For example, facial recognition is the only way to enter this Command.

As Peru continues to advance in protecting itself from cyber-attacks, the government will continue to change laws as necessary. This is evident as Congress passed three new laws in July 2019 to include 4228, 4237 and 4352. These new laws pertain to both cyber-defense and cyber-security. As the final passage discusses, the amended laws regulate all cyber military operations and to “protect and defend sovereignty, international interests and digital information, which currently falls under the Ministry of Defense.” **End OE Watch Commentary (Fiegel)**



Metaphor of the cyber iceberg.

Source: Chiaerae via Wikimedia, https://commons.wikimedia.org/wiki/Category:Deep_web#/media/File:Surface_Web_&_Deep_Web.jpg, CC by SA 4.0

“He who wins will not defeat the enemy with a physical battle, but with a cyberspace battle.”

Source: “Qué posibilidades hay de que el mundo viva una gran guerra cibernética (What are the Possibilities of a Worldwide Cyber War),” *El Comercio*, 16 August 2019. <https://elcomercio.pe/tecnologia/tecnologia/posibilidades-hay-mundo-viva-gran-guerra-cibernetica-mexico-espana-colombia-argentina-noticia-658786>

Cyber-attacks occur every day and have the capacity to affect basic internet users, businesses and governments. In order to mitigate potential cyber-attacks, Peru is currently spending 0.07% of its GDP to support counter-cyber attacks. Furthermore, Peru plans to increase its cyber-security budget by 2021.

Source: “La visión estratégica del Perú a nivel de ciberseguridad Conexión (Peru’s Strategic View of Cyber-Security),” *Conexión Esan*, 17 June 2019. <https://www.esan.edu.pe/apuntes-empresariales/2019/06/la-vision-estrategica-del-peru-a-nivel-de-ciberseguridad/>

These bullet points represent part of Peru’s strategic vision to combat cyber-attacks:

- Create departments that will monitor and anticipate possible cyber-attacks
- Distance itself from traditional norms and focus on innovating technical mechanisms
- Generate a more comprehensive plan to prevent and/or react to cyber threats
- Provide information to problems related to cyber-security in the private sector
- The military will work in coordination with the government to protect information that could be targets of cyber-attacks
- Increase the number of employees necessary to enhance cyber-security

Source: “Ejército del Perú listo ante ciberataques (Peruvian Army Ready for Cyber Attacks),” *Dialogo*, 7 January 2019. <https://dialogo-americas.com/en/articles/peruvian-army-ready-cyberattacks>

The Cyber-Defense Command at the Army Headquarters in Lima uses cutting-edge computer systems and highly trained military units that are responsible for monitoring cyberspace security. Following its inauguration in October 2018, Peruvian Army Colonel Ernesto Castillo Fuerman stressed the importance of the Command Center by stating “If they (IT platforms) are rendered useless, the government won’t be able to hold up in critical operations. The military won’t be able to command or use their weapons systems.” He further added that, “He who wins will not defeat the enemy with a physical battle, but with a cyberspace battle.”

Source: “Congreso peruano aprueba leyes de ciberdefensa y ciberseguridad (Peruvian Congress Approves Cyber-Defense Laws),” *Niubox*, 25 July 2019. <https://niubox.pe/congreso-peruano-aprueba-leyes-de-ciberdefensa-y-ciberseguridad/>

Laws 4228, 4237 and 4352 were created by the Peruvian government for the following reasons:

- To establish norms that apply to all cyber-defense work in Peru. This law will regulate all cyber military operations
- To protect and defend sovereignty, international interests and digital information (which currently falls under the Ministry of Defense.