RESUMEN

Las guerras en la actualidad toman otra dimensión, ya no se trata de las clásicas operaciones que se desarrollan en el campo de batalla con las tradicionales armas de las Fuerzas Armadas y sus soldados enfrentándose por ocupar un territorio, actualmente se desarrolla otro tipo de guerra en otro escenario que es el ciberespacio. Existen ejemplos reales que se han desarrollado ciberguerras entre algunos países como el de Rusia y Estonia en el año 2007, Estonia fue atacada su infraestructura critica, se realizaron ciberataques en contra de instituciones públicas y privadas como bancos, periódicos en un país que el uso del internet es mayoritaria en las actividades diarias; Israel y EE.UU desarrollaron un virus llamado “Stuxnet” que dañó y retrasó el programa nuclear de Irán. Las revelaciones de Julián Assange con los cables WikiLeaks dejaron al descubierto los espionajes que realizó EE.UU a la mayoría de países y posteriormente Edward Snowden, agente de la NSA (Agencia Nacional de Seguridad de los EE.UU) hizo público documentos secretos a través de la prensa y confirmó que estamos propensos a ser espiados a través de las redes de internet, paginas sociales, teléfonos celulares, convencionales y otras herramientas que son uso diario de la mayoría de la población. El Ecuador no ha estado exento de este tipo de ataques, páginas del gobierno y correo electrónico del Presidente de la República han sido hackeadas, ante esta realidad el gobierno nacional asignó recursos económicos y dispuso la creación de un Comando de Ciberdefensa con la finalidad de proteger la infraestructura crítica de las Fuerzas Armadas y posteriormente del Estado. La presente investigación se basó en realizar entrevistas y encuestas a un grupo de expertos en el tema, para determinar cuáles son los factores fundamentales en el estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas ecuatorianas para el año 2017, en la construcción de los escenarios y finalmente determinar las estrategias para alcanzar el escenario más óptimo de la Ciberdefensa en nuestro país.

PALABRAS CLAVE:

CIBERDEFENSA.
INFRAESTRUCTURA CRÍTICA.
CIBERGUERRA.
CIBERESPACIO.
PROSPECTIVA.

ABSTRACT

Wars today take another dimension, it no longer is the classic operations taking place in the battlefield with the traditional weapons of the Armed Forces and their soldiers facing occupy a territory, now another kind of war develops in another scenario that is cyberspace. There are real examples that have developed cyber-wars between countries like Russia and Estonia in 2007, Estonia was attacked their critical infrastructure cyber-attacks were made against public and private institutions such as banks, newspapers in a country that use of Internet is majority in daily activities; Israel and US developed a virus called "Stuxnet" which damaged and delayed Iran's nuclear program. The revelations of WikiLeaks Julian Assange with wires uncovered spy reports that US made most countries and later Edward Snowden, agent of the SNA (National Security Agency US), secret documents made public through the press and confirmed that we are likely to be spied through internet networks, social pages, cell phones, conventional and other tools that are daily use of most of the population. Ecuador has not been exempt from such attacks, government websites and email the President of the Republic have been hacked, to this reality, the national government allocated financial resources and ordered the creation of a Cyber Command in order to protect critical infrastructure of the Armed Forces and later the State. This research was based on interviews and surveys with a group of experts in the field, to identify the key factors in the prospective study of Cyber Ecuadorian Armed Forces in 2017, construction of scenarios and finally determine strategies to achieve the most optimal scenario of Cyber in our country.

KEY WORDS:

CYBERDEFENSE.

CYBERWAR.

CYBERESPACE.

CRITICAL INFRAESTRUCTURE.

PROSPECTIVE.