GOBIERNO DE MÉXICO | MARINA | SEDENA

GLOSARIO DE TÉRMINOS SEDENA-MARINA
EN MATERIA DE SEGURIDAD EN EL CIBERESPACIO

JUNIO 2021

GLOSSARY OF TERMS SEDENA-MARINA

IN THE FIELD OF SECURITY IN CYBERSPACE

The first version of the SEDENA-SEMAR Glossary of Technically Homologated Terms on Cyberspace Security was published in 2013 within the Mexican Armed Forces, which included nine general terms; with the present update, the purpose of having a list of those commonly used when addressing the topic of "Cyberspace Security" is still valid.

In this sense, in this new version, catalogued as of public use, the previous terms have been updated and new ones have been added, some related to the national capacities that the Mexican State has managed to develop, with the aim of achieving Security in Cyberspace, such as: Information Security, Cybersecurity and now Cyber Defense.

This document is intended to be a reference for academic research, joint work with National Security agencies, and any public or private organization that requires it to promote legislation, cooperation, innovation, research and technological development, to continue generating the capabilities of the Mexican State in favor of the security of Mexican society in Cyberspace, in compliance with the powers and missions of the SEDENA and MARINA in matters of National Security.

It is important to mention that the "Glossary of SEDENA- MARINA Terms on Security in Cyberspace" is subject to a continuous improvement process through the C.O.C. of the General Staff of the National Defense and the UNICIBER of the General Staff of the Navy.

A

Action in Cyberspace: efforts made through the use of Information and Communications Technologies (ICT) to defend and/or attack information assets in or through Cyberspace.

Defensive Action in Cyberspace (Cyberdefense): passive action of the Armed Forces in or through Cyberspace with the objective of neutralizing or mitigating the effects of cyberattacks, while maintaining their own operational capacity.

Offensive Action in Cyberspace (Cyber Offensive): active action of the Armed Forces in or through Cyberspace with the objective of limiting or destroying the operational capability of an adversary.

Information Asset(s): person or technology that knows or contains information, and which, because of its importance, must be protected to maintain its confidentiality, integrity and availability, including ICT assets.

Information and Communications Technology Asset(s) (ICT Asset): computer programs, computer goods, technological solutions or services, networks, systems or applications, their components and databases, electronic files and the information contained therein, which may or may not be part of an Essential or Critical Information Infrastructure.

Advanced Persistent Threat (APT): type of cyberattack with the purpose of accessing a network or system, infiltrating anonymously, stealthily and unnoticed to take control and perpetuate ICT assets to gain strategic advantage over a prolonged period of time through the use of techniques, tactics and procedures (TTPs). Also referred to by this acronym are some organized groups of experts associated or not with a nation-state.

Cyber Risk Analysis: procedure to estimate Security risks in Cyberspace derived from the manifestation of threats; first the vulnerability level of the asset is determined and then the associated risks are evaluated, to finally calculate the impact and implement measures and controls to reduce the effects to an acceptable level.

Areas of Knowledge of Cyberspace: are the professional and technical knowledge related to electronics, computer science, computer security, computing, development of ICT systems and equipment, communications, electromagnetic spectrum and information analysis.

Avatar (Cyberperson): representation or virtual identity of a person, group or entity to navigate and interact in Cyberspace without disclosing their real identity in the physical world.

C

Cyberspace Training Camp: isolated area of Cyberspace for the development of capabilities of a Cyberspace Security force and/or Cyber Defense force, favoring the simulation of Cyber operations within a controlled environment.

Cyberspace Security Capabilities: capabilities based on human, material, technological and financial resources allocated to provide Cyberspace Security; understood as Information Security, Cyber Intelligence, Cybersecurity and Cyber Defense in their respective areas of responsibility and competence.

Cyber Threat Hunt: operational, dynamic and proactive process of Cyber Defense and Cybersecurity, oriented to the detection and containment of Cyber Threats that evade traditional technological security measures and controls.

Cyber threat: potential external or internal source, with the capacity to cause an adverse effect in or through Cyberspace.

Cyber-weapon: computer program, software, system or application and its components, specifically designed to cause damage or detrimental effect to an information or ICT asset, which may have physical consequences in conventional operational environments.

Cyberattack: offensive or malicious action, external or internal, with the intention of causing an adverse effect in or through Cyberspace.

Cyber crisis: unexpected event where the Cyberspace Security capabilities of an organization are overwhelmed or have failed by a (s) Cyber threat (s) temporarily or permanently.

Cyber defense: capability of a nation-state translated into actions, resources and mechanisms in the area of national security and defense in cyberspace, to prevent, identify and neutralize cyberthreats or cyberattacks, including those that target a country's strategic installations.

Cyberspace: environment or intangible area of a global nature, supported by Information and Communication Technologies, in which public and private entities and society in general communicate and interact, contributing to national development and guaranteeing the exercise of rights and freedoms as in the physical world. For the Armed Forces, it is considered the fifth operational environment to provide Security and Defense.

Cyber espionage: is the illicit access to ICT in or through Cyberspace, to collect sensitive information in the political, economic, social, military or diplomatic fields.

Cyberwarfare: is a new classification of warfare, where Cyberspace is used as an operational environment for the conduct of hostile actions.

Cyber-identity: individuals or organizations with public registration, which maintain Internet addresses in accordance with the regulations, referring to names of organizations or entities in the physical world.

Cyberintelligence: intelligence activity that makes use of Cyberspace to obtain valuable information on all types of threats that threaten organizations or impact the National Security of the Nation-State. For the Armed Forces, this activity supports the areas of land, sea, air, outer space and cyberspace.

Cyber resilience: the ability of a system, organization or nation-state, in or through cyberspace, to continue to operate despite being subjected to a cyber incident or cyber attack; includes the ability to recover in the shortest possible time for continuity of operations.

Cyber risk: probability of a Cyber threat exploiting and exploiting a vulnerability, resulting in a negative impact on an organization or National Security.

Cybersecurity: the ability of a nation-state and all sectors of society to generate and implement public policies, legislation, standards, procedures and technological controls for the protection of Critical Information Infrastructures and Critical Information Infrastructures.

Cyberterrorism: use of Cyberspace as an end or means to generate terror or widespread panic, with the aim of influencing decisions or imposing ideologies against society and/or the institutions of a Nation-State.

Key Cyber Terrain: set of elements of any of the layers of Cyberspace (human, cyberhuman, cognitive, logical, ICT and geographic) that facilitate mission-critical activities, operations or functions and whose destruction, disruption or capture would generate an operational advantage for the adversary.

Catphish: individuals or organizations that register and maintain Internet addresses resembling or referencing names of organizations or entities in the real world in or through Cyberspace.

Cyber Defense CSIRT: operational technical centers with national capabilities to plan, conduct and execute Cyberspace Security activities, for the protection of the Critical Information Infrastructure of the Armed Forces and those corresponding to the country's Strategic Facilities assigned to them, in cooperation with the national effort for the maintenance of the integrity, stability and permanence of the Nation-State.

D

Cyber Crimes: illicit actions that are typified in the national and/or international legislation in force, perpetrated in or through Cyberspace using the Information and Communication Technologies as a means of communication.

E

National Mission Team in Cyberspace: a technical team made up of personnel from the National Security authorities; personnel from public and private organizations may be incorporated to assist the national effort in the fulfillment of Security in Cyberspace missions.

Armed Forces Mission Teams in Cyberspace: tactical-technical teams made up of Armed Forces personnel, to carry out defensive or offensive actions in the fulfillment of Security in Cyberspace missions.

F

Cyberspace Workforce: professionals and technicians of the institutions and agencies of the defense sector, public and private, who work in the areas of knowledge of Cyberspace.

Cyberspace Security Force: is the personnel of the National Security instances; as well as of public and private agencies, specialized in Information Security, Cybersecurity and/or Cyber Defense in their respective areas of competence.

Cyber Defense Force: it is the Security Force in Cyberspace of the Armed Forces, to carry out defensive or offensive actions in the fulfillment of the National Security missions.

H

Hacktivism or digital activism: phenomenon generated in or through Cyberspace to express ideas that promote civil disobedience activities, propaganda or political, social or ideological proselytism.

I

Cybersecurity Incident (Cyber Incident): interruption, unauthorized access or any failure that affects the information assets of Critical Information Infrastructures and Essential Information Infrastructures, which may or may not result in a cybercrime or cyberattack.

Critical Information Infrastructure(s) (CII): Essential Information Infrastructures considered strategic because they are related to the provision of goods and essential public services and whose affectation could compromise Public Security or National Security in terms of the laws on the matter.

Essential Information Infrastructure(s) (IIE): the networks, services, equipment and facilities associated or linked to ICT and Operational Technology (TO) assets, whose affectation, interruption or destruction would have an impact on the individual or public or private organizations.

Cyber Threat Intelligence: Cyber Intelligence process that analyzes Cyber Incidents, Cyber Threats and/or Cyber Attacks that attempt against the information assets of an organization OR that impact the National Security of the Nation-State, in which indicators of compromise and attribution are obtained in order to counter them.

O

Operations in Cyberspace: Activities carried out by the Nation-State in or through Cyberspace, in order to provide security to society. For the Armed Forces they are considered as military operations in Cyberspace in the fulfillment of the missions entrusted to them.

P

Cyberspace Operational Panorama: the current and future strategic, operational and tactical situation of the Cyberspace environment or environment, which supports decision-making in the planning, conduct and execution of cyber operations.

S

Information Security: capacity of public or private institutions and organizations to preserve the confidentiality, integrity and availability of information through risk management, as well as its authenticity, auditability, traceability, protection against duplication, non-repudiation and legality.

Security in Cyberspace: is the condition sought by any society in or through Cyberspace, achieved through Information Security, Cybersecurity and Cyberdefense actions as capabilities of a Nation-State.

Cyberspace Weapons System: system which integrates command and control functions, Cyber Weapons and technical supports necessary to provide Cyber Defense capabilities of a Nation-State.

T

Operational Technologies (OT): ICTs that generate or detect a change through the control and/or monitoring of processes and events in Critical Information Infrastructures or Essential Information Infrastructures.

V

Vulnerability in Cyberspace: failure, absence or weakness in the design, implementation or operation of an information asset or ICT, which can be exploited by a Cyber threat, thus materializing risks.

This Glossary of Terms was developed by the Specialist staff of the Cyberspace Operations Center of the E.M.D.N. (C.O.C. E.M.D.N.) and Cybersecurity Unit of the E.M.G.A. (UNICN). M.G.A. (UNICIBER E.M.G.A)), defined as:

E.M.D.N. Cyberspace Operations Center (C.O.C. E.M.D.N.): is the CSIRT of the General Staff of the Secretariat of National Defense. Its mission is: "To plan, coordinate, direct and execute the efforts of the Mexican Army and Air Force to identify threats from Cyberspace and mitigate their effects, as well as to prevent and respond to incidents that threaten the information and critical infrastructure supported by the Information and Communications Technologies of the Ministry of National Defense".

Cybersecurity Unit of the E.M.G.A. (UNICIBER E.M.G.A.): is the CSIRT of the General Staff of the Mexican Navy. Its mission is: "To plan, conduct and execute Information Security, Cybersecurity and Cyber Defense activities, for the protection of the Institutional Critical Infrastructure, and to contribute to the national effort for the maintenance of the integrity, stability and permanence of the Mexican State".

Aproved
SEMAR General Staff of the Navy
Cybersecurity Unit

Contralmirante C.G. D.E.M.
Jefe de la UNICIBER E.M.G.A.
Jesus Arellano Rodarte

Aproved
SEDENA National Defense Staff
Cyberspace Operations Center

Gral. Brigadier I.C.E. D.E.M.
Director del C.O.C. E.M.D.N.
Francisco Javier Villa Vargas

REFERENCES:

- Diccionario de términos, UNAM CERT, available at: https:/Avwww.seguridad.unam.mx/ diccionario/a, Mexico, accessed January 2021 Standard

- ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity, International Organization for Standardization (1SO). USA, 2012.

- Estrategia Conjunta de Ciberdefensa SEDENA -SEMAR. Secretary of National Defense - Secretary of the Navy, Mexico, 2019.

- Estrategia Nacional de Ciberseguridad, Government of Mexico, available at: https:/Avwww. gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad, 2017.

- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2014.

- Glossary of Cybersecurity Terms, Spanish National Cybersecurity Institute (INCIBE), available at: https://ww.incibe.es/sites/default/files/contenidos/guias/doc/ guia_glosario_ciberseguridad_metad.pdf, Spain 2107.

- Glossary of Cybersecurity Terms, Centro Especializado en Respuesta Tecnológica de la Policía Federal (now National Guard). https:/Avwww.gob.mx/policiafederal/ articulos/glosario-de-terminos-en-ciberseguridad?idiom=en Accessed January, 2021 Terms technically approved in Cyberspace Security Matters SEDENA-SEMAR, 2013.

- Guía de Ciberdefensa, Orientaciones para el diseño, planeamiento, implantación y desarrollo de una Ciberdefensa Militar. Inter-American Defense Board (IADB). https:// wwwi.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensal0.pdf, accessed January 2021

- Security Guide (CCN-STIC-401), Glossary and Abbreviations. Centro Criptológico Nacional, Spain, 2015.

- Administrative Manual of General Application in Matters of Information and Communications Technologies and Information Security (MAAGTICSI). Ministry of Public Administration. D.O.F. July 23, 2018. Manual de Operaciones Militares, Secretaría de la Defensa Nacional, Mexico, 2017.

- Tallinn Manual 2.0, On International Law Applicable to Cyber Operations, Second Edition, Cambridge University Press, USA, 2017.

- Terms homologated technically in terms of Security in Cyberspace SEDENA-SEMAR. Secretariat of National Defense-Secretariat of the Navy, 2013.