Information security specialty

Especialidad seguridad de la información

LÓPEZ, Fabricio†

Universidad Iberoamericana, Mexico.

ID 1st Author: *Fabricio, López*

DOI: 10.35429/JEDT.2020.6.4.16.19 Received January 25, 2020; Accepted June 30, 2020

Abstract

The Cyberspace also called 5th dimension, susceptible to suffer Cyber Attacks that cause incidents and affect the operation, the economy and the reputation of an organization, company or country. The use of information technologies is a key element in the economic advance of any country, allowing the development of activities within its own territory, as well as outside it. These activities are supported by computer systems for processing, storage and communication, becoming critical infrastructures for a country. All these infrastructures and computer systems become an attractive target to generate attacks, which can destabilize their operation, cause damage to their reputation or financial and sometimes generate conflicts of nations. This proof of this type of behavior, it is possible to analyze and observe the case of North Korea, where it is responsible for the attacks of Cybernetic War on South Korea, creating economic losses for this country of around $ 805 Million Dollars. Concepts such as Cybernetic Espionage, Cyber Terrorism and Cybernetic Activism should be studied and understood by modern societies as part of their awareness and preparation for the possibility of a new World War developing from the Cybernetic Space.

Cybernetic Warfare, Cyber Activism, Critical Infrastructures, Capacities

Resumen

El Ciberespacio también llamado 5ª dimensión, susceptible de sufrir Ciberataques que provocan incidencias y afectan el funcionamiento, la economía y la reputación de una organización, empresa o país. El uso de las tecnologías de la información es un elemento clave en el avance económico de cualquier país, permitiendo el desarrollo de actividades dentro de su propio territorio, así como fuera de él. Estas actividades se apoyan en sistemas informáticos de procesamiento, almacenamiento y comunicación, convirtiéndose en infraestructuras críticas para un país. Todas estas infraestructuras y sistemas informáticos se convierten en un objetivo atractivo para generar ataques, que pueden desestabilizar su funcionamiento, causar daños a su reputación o financieros y en ocasiones generar conflictos de naciones. Esta prueba de este tipo de comportamiento es posible analizar y observar el caso de Corea del Norte, donde es responsable de los ataques de la Guerra Cibernética a Corea del Sur, generando pérdidas económicas para este país de alrededor de $ 805 Millones de Dólares. Conceptos como el espionaje cibernético, el terrorismo y el activismo cibernéticos deben ser estudiados y comprendidos por las sociedades modernas como parte de su conciencia y preparación para la posibilidad de que se desarrolle una nueva guerra mundial desde el espacio cibernético.

Guerra cibernética, ciberactivismo, infraestructuras críticas, capacidades

Citation: LÓPEZ, Fabricio. Information security specialty. Journal-Economic Development Technological Chance and Growth. 2020. 4-6:16-19.

† Researcher contributing first author.

Introduction

According to the ISACA Cybersecurity Fundamentals Glossary, a Critical Infrastructure is defined as the set of systems that, when affected or destroyed, would have an effect that would weaken the economic security of a company, community or nation.

Information and Communication Technologies (TIC) are an element of great relevance in the world economy, generating development at a social, economic and political level. The increase of users, organizations and governments that are connected to the Internet and that use this medium to perform different operations, ranging from electronic money transfers, issuance of official documents for citizens within a political territory, consumption of communication services (television, telephony, etc.), purchases and reservation of transport services, etc.

All these activities carried out within the Cybernetic Space are subject to the inherent risks of the use of this type of technology, examples of which are identity theft, identity theft, information theft, electronic fraud, espionage, denial of services, etc.

Today, terrorist organizations such as Al-Qaeda use the Internet and computer systems to plan future terrorist attacks, taking advantage of the degree of anonymity and allowing them to recruit followers and funds in a non-visible way.

Organizations such as the CERT (Computer Emergency Response Team) by its acronym in English, composed of experts with knowledge in the handling of security incidents and who support in the response to incidents, threat analysis and exchange of critical information of security, with the purpose of continuously improving the position of Cyber Security between countries.

Context

Vulnerabilities, the gateway

The search for technology companies to improve the performance and functionalities that can be delivered to an organization in terms of information technologies has generated a change in the mentality and the way in which vulnerabilities are evaluated and managed within the companies, organizations and countries.

It is important to consider that a critical infrastructure is integrated with multiple information systems and technologies, which are susceptible to cyber-attacks that will try to find the vulnerabilities associated with their construction and development, in order to exploit them to obtain a benefit.

Some examples of critical infrastructures in a country are:

- Airports.
- Parastatals.
- Communications companies.
- Seaports.
- Railway and road infrastructures.
- Etc.

Each one of these infrastructures provides a value and an operative capacity, the affectation or disqualification puts the security of the country completely at risk.

The STUXNET virus was launched in 2008 and aimed at affecting SCADA devices and centrifuge control equipment in uranium enrichment plants. This virus opened a new era in terms of what is known as a conventional war, allowing countries like Israel and the United States to affect Iran's nuclear weapons production and delaying this nuclear program for at least 3 years.

Another attack that caused major repercussions on communication infrastructures, are DDoS Distributed Services Denial Attacks such as the one registered in 2016 to the domain name provider DYN, causing the fall of platforms such as Facebook, Twitter, Spotify, among others. The attack had global repercussions affecting a large number of users in Europe and North America.

ISSN-2524-2024

This attack took advantage of multiple vulnerabilities on Internet-connected devices such as printers, cameras and monitors of babies infected with Mirai malware.

Cyber Warfare

The Geneva Convention of 1949 and Article 51 of the Charter of the United Nations define the rules of conventional warfare, which prohibit the use of certain weapons and there are certain rules of protection for civil and medical assistance agencies.

Unlike Conventional War Cyber Warfare is not subject to the rules and regulations of the aforementioned Conventions. Identifying the rules of engagement in a Cyber Warfare is very complex because it is difficult to establish what really constitutes a War.

- Are DDoS attacks on a military target Cyber Warfare?

- Is an attack by a group of state-sponsored Hackers with a financial objective an act of Cyber Warfare?

Dr. Dorothy Denning professor in the Department of Defense Analysis of the Naval Postgraduate School in Michigan, made an adaptation of the different classes of Cybernetic War, with the purpose of being able to determine more accurately the consequences, characteristics and impact of the same, this classification consists of 4 types:

- Cyber warfare Class 1 - In charge of the protection of personal information or personal privacy. While the results can still be devastating, Class 1 is considered the lowest.

- Cybernetic Warfare Class 2 - Concerned about economic and industrial espionage, which can be directed against nations, organizations, universities or other organizational structures. This form of Cyber War is on the rise.

- Class 3 Cyber War - Officially it is a Global War and Terrorism, which includes Cyber Terrorism, but which also includes attacks on other parts of critical infrastructure.

- Cybernetic Warfare Class 4 - The use of all techniques from Classes 1-3 in combination with military activities in an effort to gain an advantage on the battlefield or a force multiplier.

Cyber warfare is then a conflict related to information at the national, military level, as well as low intensity conflict activities aimed at inflicting limited levels of damage.

According to the Clausewitz triangle (People, Politics, Militias), none of the cyber-attacks recorded in the past, meets the criteria to be considered an act of war.

Conclusions

The term Cybernetic War is a subject of great relevance at this time and it is increasingly frequent the use of this term globally. The conflicts between countries and the interventions that can be developed have passed from the physical plane to a virtual plane in the Cybernetic Space.

This has also caused criminal organizations to carry out terrorism and may jeopardize the stability of a nation, in search of economic, territorial or power benefits.

It is important to be able to develop a clearer and more forceful definition that allows to identify and classify if the activities and effects of a Cyber Attack can be considered part of a Cybernetic Warfare. The standardization of criteria and the standardization in the classification of types of Cyber Warfare by the countries, such as those proposed by Dr. Dorothy Denning will allow to evaluate and take the pertinent actions in the event that a declaration of War is determined, is important to consider that the Cybernetic Warfare alone does not have the possibility of exerting a force or damage on human life and that it will require a conjunction with other types of attacks or activities outside the Cybernetic Space.

References

Mehan, J. E. (2014). Cyberwar, Cyberterrorism, Cybercrime and Cyber Activism: An In-depth Guide to the Role of Standards in Cybersecurity Environment. Ely, Cambridge, UK: IT Governance Publishing.

ISSN-2524-2024

Mehan, Julie E. Cyberwar, Cyberterrorism, Cybercrime and Cyber activism: An In-Depth Guide to the Role of Standards in Cybersecurity Environment. vol. 2nd ed, IT Governance Publishing, 2014. EBSCOhost.

Gabriel, R. A. & Metz, K. S. (1992) A Short History of War: The Evolution of Warfare and Weapons. Professional Readings in Military Strategy No. 5, Strategic Studies Institute, US Army War College. Retrieved on 12 September 2007 from www.au.af.mil/au/awc/awcgate/ gabrmetz/gabr003a.htm

CICR (2010). Los Convenios de Ginebra de 1949 y sus Protocolos adicionales. Retrieved on 20 March 2018 from https://www.icrc.org/spa/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm.