# Ciberguerra, el ataque a infraestructuras criticas como política internacional y porque Argentina tiene que trabajar en este aspecto.

Luis Maria Mozzoni
Mayo 2019.

Universidad Blas Pascal
Maestría en Dirección y Gestión de Organizaciones
Análisis Político Internacional

**Abstract**

Las infraestructuras críticas son las instalaciones que resultan esenciales para un país, ya que manejan servicios básicos y estratégicos para el normal funcionamiento del mismo, como ser la distribución de energía eléctrica o la provisión de agua.

Históricamente se consideró que, por ejemplo, un malware solo podía afectar datos, ya sea en archivos, bases o aplicaciones, pero que no podía afectar hardware. En la actualidad existen crecientes cantidades de ataques que tienen la capacidad de no solamente comprometer datos, sino también hardware. El problema radica en que, los dispositivos y tecnologías que se utilizan para gestionar sistemas de control industriales, no fueron diseñados ni pensados con aspectos de ciberseguridad y hoy están interconectados con otras redes hasta incluso directamente a Internet por lo que se convierten en vulnerables a estos nuevos tipos de ataques.

Los ataques a infraestructuras críticas son potenciales amenazas en todo el mundo, no solo por cuestiones económicas sino también por cuestiones políticas y estratégicas.

Argentina no está exento a esta situación por lo que es necesario entender su situación actual en cuanto a la política nacional de ciberseguridad y protección de infraestructuras críticas.

## Tabla de Contenidos

## Introducción

"Un ciberataque masivo y bien coordinado en la infraestructura de una red eléctrica podría devastar la economía de una región y causar pérdida de vidas humanas a gran escala ", con esa definición, el Dr. Richard Andres, del US National War College, define lo que podemos empezar a entender como ciberguerra [1]

¿Pero que es la ciberguerra?

La guerra cibernética se ha definido como cualquier medida hostil contra un enemigo diseñado para descubrir, alterar, destruir, interrumpir o transferir datos almacenados, manipulados o transmitidos a través de una computadora [2]

El ciberespacio se ha convertido en el quinto dominio de guerra, después de la tierra, el mar, el aire y el espacio. ¿Y cuáles son las motivaciones para esto? Hoy un país puede quedar paralizado por una nación enemiga sin necesidad de una invasión militar, con sólo controlar la infraestructura electrónica e informática del adversario, como las redes de comunicación, las usinas de energía o los bancos. El punto clave es que, en un conflicto cibernético, la distancia terrestre entre los adversarios es irrelevante, ya que en el ciberespacio no existen fronteras, somos todos vecinos. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas. Las TTP (tácticas/técnicas/procedimientos) son la infiltración en redes, la recopilación de datos, la interferencia de señales, los programas informáticos falsificados y contaminados (a partir de la instalación de "puertas traseras"), ataques a sistemas enemigos a través de virus o diferentes tipos de malware, entre otras. Al contrario de las guerras tradicionales, en una ciberguerra no gana el que tiene más poder de fuego, sino el más innovador, esto, considerando que ninguna red o infraestructura es 100% segura.

1 - Disponible en: https://www.cfr.org/report/cyberattack-us-power-grid

2 - Disponible en: https://www.icrc.org/en/document/cyber-warfare

1. Nuevos Conceptos

1.1 Nuevo dominio

Para que entendamos la relevancia de este nuevo dominio, en el año 2013 a pedido del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN se creó el "Tallinn Manual on the International Law Applicable to Cyber Warfare" [3], denominado comúnmente "Manual de Tallin", que lleva el nombre de la capital de Estonia, donde se compiló y perpetró el primer ataque cibernético de un país a otro. Este manual es una guía importante para situaciones que se puedan plantear en el ciberespacio. En este se indica por primera vez el procedimiento a seguir por parte de los estados y las alianzas militares en caso de ciberataques masivos.[4]

1.2 Infraestructura critica

Un nuevo concepto que adquiere vital importancia es el de infraestructuras críticas. Estas son infraestructuras (mayormente del tipo industriales basadas en tecnología SCADA) que operan y se interconectan mediante redes y sistemas informáticos. Estas pueden ser tanto públicas como privadas y son claves para el funcionamiento de los servicios de un país, como, por ejemplo, los sistemas de gestión hidrológica, los conductos de gas, las redes de transmisión y distribución eléctrica, los sistemas bancarios, de telecomunicaciones, de control de tráfico aéreo, ferroviario o vial, entre otros, que pueden resultar como potenciales objetivos en el marco de un conflicto bélico virtual.

Según estadísticas del Instituto Nacional de Ciberseguridad de España (Incibe), las ofensivas a través de la red contra los operadores de estas instalaciones críticas, no paran de aumentar y se han multiplicado por siete en solo dos años. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. Y, además, en el primer cuatrimestre de 2017 se han registrado 247, por lo que de seguir así se superarán los 700 incidentes este ejercicio y se batirá otro récord. [5]

---

3 - Disponible en: http://nuclearenergy.ir/wp-content/ uploads/2013/11/tallinn_manual.pdf

4 - Disponible en: http://www.cefadigital.edu.ar/bitstream/123456789/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf

5 – Disponible en: https://www.incibe-cert.es/blog/seguridad-industrial-2018-cifras

Y el interés contra estos objetivos no solo radica en una cuestión política, sino que se potencia en la debilidad sobre la que están implementados los mismos, basados en tecnologías antiguas como SCADA, que únicamente buscan asegurar la disponibilidad del activo, a costa de perder la capacidad de confidencialidad y la integridad de los mismos.

Hay ejemplos testigos de lo que puede llegar a ocurrir en un país o lo que se puede llegar a realizar dentro del contexto de una ciberguerra, como ser el ataque masivo de denegación de servicio distribuida (DDoS) a Estonia en 2007, el ataque a la central nuclear de Natanaz, en Irán en 2011 o el troyano BlackEnergy que provoco un corte de suministro electico masivo en la región de Ivano-Frankivsk, al sureste de Ucrania**.**

Así como las infraestructuras críticas son protegidas de ataques físicos, también deben ser protegidas de ciberataques. Aquí juegan un papel muy importante los dueños de estas instalaciones; que deberán tomar medidas para combatir estas amenazas. De la misma forma que reconocen y establecen diferentes barreras de seguridad física de protección, deben hacerlo con los aspectos de ciberseguridad.

Esto nos lleva a preguntarnos cuál es la situación de la República Argentina en cuanto a la política de definición y protección de sus infraestructuras críticas.

### 1.3 Definición de Infraestructura Critica

El Plan Nacional de Protección de Infraestructuras Críticas de España, define a las infraestructuras criticas como: “Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.”. Esto fue reafirmado en la Directiva europea 2008/114/CE.[6]

6 – Disponible en: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Así mismo, el USA Patriot Act de 2001, realiza la siguiente definición: “Sistemas y activos, ya sea físicos o virtuales, tan vital para los Estados Unidos que su incapacidad o destrucción provocaría un impacto sobre la seguridad, la economía nacional, la salud pública o la seguridad nacional, o cualquier combinación de las anteriores.” [7]

Por su parte, el consultor internacional Manuel Sánchez Gómez-Merelo realiza un listado donde podemos encontrar, por ejemplo:

- Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional);
- Industria Química y Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.);
- Agua (embalses, almacenamiento, tratamiento y redes);
- Centrales y Redes de energía (producción y distribución);
- Tecnologías de la Información y las Comunicaciones (TIC);
- Salud (sector e infraestructura sanitaria);
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.);
- Alimentación (producción, almacenamiento y distribución);
- Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).

Como se observa en el listado se incluyen instituciones gubernamentales u organismos del estado, como también empresas del sector privado. Y se consideran críticas, porque, como también indica Merelo, “……un ataque masivo y coordinado a alguno o varios de estos sectores establece una condición importante y crítica para una nación, pues se pone en juego la estabilidad de la misma y la confianza de la ciudadanía en el Estado para enfrentarse a estas amenazas…” [8]

7 – Disponible en: https://www.congress.gov/bill/107th-congress/house-bill/3162

8 – Disponible en: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

2. Situación Argentina

En el año 2011, en base a una serie de consideraciones como ser “Que la seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas”, a través de la resolución JGM Nº 580/2011 se crea en Argentina el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” [9]

Este programa tiene entre otros objetivos, la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas necesarias para el correcto funcionamiento del Sector Público Nacional, las organizaciones de jurisdicción provincial, la sociedad civil y las organizaciones privadas, sin embargo, no se define explícitamente a la ciberseguridad, solo se introduce la noción de Infraestructura crítica.

Tal como consigna el Art. 7º, “La OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, en su carácter de autoridad de aplicación, brindará el apoyo técnico y administrativo necesario para la implementación del “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”.

Ese mismo año, la ONTI través de la disposición Nº 3/2011 aprueba el "Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, mediante el cual las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorias, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado podrán adherir al “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” [10]

9 – Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

10 – Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/187698/norma.htm

Dentro de los adherentes, podemos encontrar por ejemplo a la Universidad Nacional de Cordoba, que el 15 de Julio de 2014, a través de la resolución 1221 firmada por el Rector Tamarit, en su artículo N°1 “Hacer lugar a lo solicitado a fS.1 por la Prosecretaría de Informática y, en consecuencia, adherir al "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad", creado por Resolución JGM N° 580/11, obrante a fs. 2 que en fotocopia forma parte integrante de la presente, y suscribirlo” [11]

3. Ciber-X

Futurismo y ciencia ficción son características que rodean la definición de esta palabra. Precisamente en este género literario es donde se popularizo este concepto, atribuyendo su primera utilización al autor William Gibson, en su novela “Neuromante” publicada en 1984. Este utilizo el término “Ciberespacio” para referirse a una realidad simulada que se encontraba implementada dentro de los ordenadores y de las redes digitales de todo el mundo. [12]

En otras palabras, el ciberespacio es aquel “dominio global y dinámico compuesto por las infraestructuras de tecnologías de la información (incluida Internet), las redes, los sistemas de información y telecomunicaciones”.

Según la Real Academia de Ingeniería, un ciberataque es “Forma de ciberguerra o ciber terrorismo donde, combinado con ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a la misma” [13]

Podemos entonces afirmar que un ciberataque es “toda acción intencionada que se inicia en un equipo informático, con el objetivo de comprometer la confidencialidad, disponibilidad o integridad del equipo, red o sitio web atacado y de la información contenida o transmitida a través de ellos, todo esto realizado dentro en el ciberespacio” [14]

---

11 – Disponible: http://www.digesto.unc.edu.ar/rectorado/rectorado/resolucion/1221_2014_1/at_download/file

12 – Disponible en: https://www.brainpickings.org/2014/08/26/how-william-gibson-coined-cyberspace/

13 – Disponible en: http://diccionario.raing.es/es/lema/ciberataque

14 – Disponible en: https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2015/CIGRAS-2015.09.10-09-Ciberataques%20Estamos%20Preparados-Enrique%20Larrieu-Let.pdf

### 3.1 Ciberataque

Como ejemplos de ciberataques podemos encontrar

- Ataques de DoS/DDoS (denegación de servicio / denegación de servicio distribuida)
- Infecciones por malware
- Phishing
- Filtración de información

Los ciberataques, a diferencia de un ataque físico tradicional, tiene una serie de características interesantes, entre las cuales podemos destacar:

- Facilidad (bajo costo, programable desde cualquier ubicación, etc.)
- Alto impacto
- Rapidez con la que generan pánico
- Mucho más baratas que las armas tradicionales.
- Difíciles de detectar.
- Difícil de atribuir a un atacante particular
- Difíciles de protegerse contra ellas, teniendo en cuenta todas las vulnerabilidades de software desconocida.

Y como principales motivaciones detrás de un ciberataque podemos mencionar diferentes tipos:

- Publicidad
- Hacktivismo
- Venganza
- Económicas
- Políticas

Y dentro de las motivaciones políticas detrás de un ciberataque, podemos destacar dos posibles objetivos claros:

- Desestabilizar una región
- Provocar el caos social

La sola difusión mediática por ejemplo del hecho que instalaciones vitales para el país o la población en general, son vulnerables a este tipo de ataques, provoca irremisiblemente el pánico entre la población, aun no cumpliendo total o parcialmente con su objetivo.

Finalmente, podemos también indicar que en un ciberataque tenemos diferentes tipos de actores.

- Cibercriminales, que buscan la monetización de sus ataques.
- Hacktivistas, que buscan el daño directo contra la víctima o su imagen.
- Insiders, que buscan la venganza a través del daño directo contra la víctima o su imagen.

Pero como afirma la compañía de ciberseguridad Kaspersky, si tomamos como ejemplo el malware “flame” podemos encontrar un caso de malware que no está diseñado para robar dinero de cuentas bancarias. Este difiere de otros programas maliciosos y herramientas de ataque que usan los hacktivistas. Entonces, excluyendo a los ciberdelincuentes, a hacktivistas o insiders, llegamos a la conclusión de que pertenece a nuevo actor diferente [15]:

- Los Estados.

Tal como indica Sanchez Medero, la ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos
entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático. [16]

Algunas potencias en materia de ciberguerra son Estados Unidos, China y Rusia, pero también podemos mencionar a Israel, Francia, Taiwán, Irán, Australia, Corea del Sur, India y Paquistán, entre otros.

15 – Disponible en: https://www.kaspersky.com/about/press-releases/2012_resource-207-kaspersky-lab-research-proves-that-stuxnet-and-flame-developers-are-connected

16– Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3745519

### 3.2 Motivaciones

Para entender la motivación de una ciberguerra, nos tenemos que remontar a abril de 2007. Para esa fecha, sucede lo que se conoce como "ciberguerra estonia", motivada por el traslado del “Soldado de Bronce de Tallin”, que había sido levantado en agradecimiento a los soviéticos que liberaron a Estonia de los nazis. El problema, para los estonios, es que su país fue absorbido por la URSS, y muchos estonios consideran invasores al Ejército Rojo. De una u otra forma, los servicios de seguridad rusos respondieron a lo que consideraban un sacrilegio con un contundente ataque informático, cuyos blancos fueron numerosas instituciones públicas, entre ellas, el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación. El ataque, inusitado por su envergadura, es estudiado hoy por muchos países y estrategas militares.

Un año después de aquella guerra, en 2008, la OTAN decidió crear en Tallin el Centro de Excelencia para la ciberdefensa, un proyecto en el que participan una serie de países para diseñar estrategias de defensa contra ataques por Internet. [17]

### 4.1 Ataques a Infraestructuras Criticas

Al pensar en ciberataques a infraestructuras críticas, nos tenemos que remontar mucho antes de que Internet existiera. Podemos afirmar que el primero tuvo lugar en 1982, cuando atacantes consiguieron instalar un troyano en el sistema SCADA que controlaba el oleoducto siberiano y que provocó una enorme explosión en el mismo. El ataque fue orquestado por la CIA, y no se supo de él hasta el año 2004, cuando se publicó el libro “At the Abyss: An Insider’s History of the Cold War”, donde desvelaba esta historia. [18]

En 2008 tuvo lugar el que sin duda ha sido el caso de ciberataque a infraestructuras críticas más conocido de la historia: Stuxnet. Al día de hoy se sabe que fue un ataque coordinado entre la inteligencia israelí y la norteamericana, con el objetivo de retrasar el programa nuclear iraní.

---

17 – Disponible en : https://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

18 – Disponible en: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf

Crearon un gusano que, al infectar los ordenadores que controlaban las centrifugadoras de uranio de la planta iraní de Natanz, hacía que éstas fueran a máxima velocidad mientras que al mismo tiempo la información mostrada en las pantallas de los terminales lo ocultaban, haciendo creer a los ingenieros que todo iba de forma normal. Esto causó la rotura física de todas las centrifugadoras de uranio de la planta. [19]

El 23/12/15 es también una fecha trascendental en ciberseguridad. Ese día, un grupo de hackers introdujo software malicioso y accedió a los sistemas de una red eléctrica provocando un corte de suministro eléctrico masivo. Durante horas, el troyano BlackEnergy tumbó la red que abastecía a 600.000 hogares de la región de Ivano-Frankivsk, al sureste de Ucrania. Nadie ha reclamado la responsabilidad de este incidente en particular. Sin embargo, Ucrania ha culpado desde entonces a Rusia, debido a la anexión de Crimea por parte de Rusia. [20]

Podemos también nombrar ejemplos de ataques como:

Industroyer: En pleno invierno, Kiev perdió el acceso al servicio eléctrico por más de una hora, esto debido a Industroyer, código malicioso diseñado para afectar plantas de distribución eléctrica.

DDoS a Browns Ferry: Ocurrió en agosto de 2006 en Alabama. La planta nuclear Browns Ferry sufrió un ataque de denegación de servicio, el cual, afectó el sistema de recirculación del agua en la planta.

SQL Slammer: Mediante una vulnerabilidad en los servidores de SQL, se provocó daños en la red de monitorización de la planta nuclear Davis-besse, ubicada en Ohio, EE.UU. El ataque dejo sin funcionamiento el sistema que supervisa el comportamiento de dicha planta durante un lapso de un poco más de cinco horas. [21]

---

19 – Disponible: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra

20 – Disponible en: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

21 – Disponible en: https://revistaitnow.com/los-7-ataques-mas-severos-la-infraestructura-critica/

## 4.2 Ataques en Argentina

Si bien al momento, en la República Argentina no se concretaron o al menos observaron casos específicos de ataque a infraestructuras críticas, el historial de ciberataques va en aumento, tanto para organismos públicos como privados.

Según el último informe anual de amenazas de la empresa Symantec, que analiza a 157 países y detalla los principales hallazgos alrededor de las amenazas globales, tendencias y motivaciones de los ciber delincuentes, Argentina continúa ocupando el 2° lugar regional en phishing y ataques por internet, 3° en spam y cryptojacking, 4° en bots, y 5° en malware, ataques a la red y ransomware. [22]

Adicionalmente, el Global Cybersecurity Index 2018 de la ITU ubica a Argentina en el puesto 94 del ranking global compuesto por 175 países, y en la posición 11 del ranking regional de America, compuesto por 33 países.

Este índice GCI es un índice compuesto producido, analizado y publicado por la Unión Internacional de Telecomunicaciones (UIT) para medir el compromiso de los Estados Miembros de la UIT con la ciberseguridad y refleja sus cinco pilares: legal, técnico, organizativo, desarrollo de capacidades y cooperación. Combina 25 indicadores en una medida de referencia para monitorear el compromiso de ciberseguridad de los Estados Miembros a los cinco pilares respaldados por la Agenda de Ciberseguridad Mundial (ACG). [23]

No obstante, casos concretos reflejan la problemática que está viviendo el Estado Nacional en este tema.

En febrero de 2017, la cuenta de twitter de la ministra Patricia Bullrich fue hackeada y fueron publicados mensajes en primera persona que la ridiculizaban.

En junio de 2017, el sitio web del Ejército Argentino sufrió un hackeo que permitió colocar una imagen genérica del grupo terrorista ISIS, con la leyenda “ISIS está llegando a la Argentina”.

En agosto, de 2017 el sitio web de Gendarmería fue atacado y los hackers cambiaron headers de la página web para demandar la aparición con vida de Santiago Maldonado.

En abril de 2018, el sitio web de la Policía de la Ciudad de Buenos Aires fue hackeado por un grupo, que colgó en la web más de 3GB de información de las bases de datos de la fuerza de seguridad.

Según estadísticas del Ministerio de Modernización, en el 2015 se registraron 2.252 hackeos; en el 2016 un total de 422.672 y en 2017 la cifra creció 3.131.268 incidentes informáticos registrados tanto en el Estado como en las empresas. Pero hay muchos más, ya que estos apenas son los que se pudieron advertir o denunciar.[24]

22 – Disponible en: https://www.symantec.com/es/es/security-center/threat-report

23 – Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

24 – Disponible en: https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf

## Conclusion

“Se torna necesaria la elaboración en nuestro país de una Estrategia Nacional de Ciberseguridad que contemple los propósitos y objetivos tendientes a desarrollar un marco normativo, conjuntamente con las medidas técnicas, organizacionales, de políticas y procedimientos que permitan proteger adecuadamente el ciberespacio, incluyendo las infraestructuras críticas que proveen servicios esenciales a la Nación y desarrollar una cultura de Ciberseguridad.” De esta forma, el decreto 577/2017 muestra que la realidad es clara y contundente. El país es vulnerable a un ciberataque y las infraestructuras críticas no están exentas. Y esto puede suceder en un ámbito nacional como por ejemplo en una central Nuclear o en una transportadora eléctrica, como en ámbitos locales en una empresa prestadora del servicio de agua potable de una ciudad. La protección de estas nace debido a la consciencia que adquieren los gobiernos y las legislaciones que generan para garantizar el funcionamiento de los servicios esenciales para los países.

Si bien se están realizando una serie de acciones, como la creación del Comité de Ciberseguridad, integrado por representantes de los ministerios de Modernización, Defensa y Seguridad, que tendrá el objetivo de desarrollar una estrategia nacional de seguridad informática y entre otras tareas deberá fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales [25] la información oficial indica que para el primer trimestre de 2018 solamente 6 entidades se adhirieron al Programa Nacional de Infraestructuras Críticas y se encuentran en proceso varias organizaciones más, alcanzándose un total de 94 miembros entre organizaciones públicas y empresas privadas. Esto es realmente muy poco, considerando la cantidad de organismos tanto públicos como privados, de índole nacional, provincial o local que podemos encontrar en la República Argentina. Imaginemos simplemente cuantos clínicas y hospitales hay en toda la Argentina o cuantas empresas potabilizadoras de agua podemos contabilizar a lo largo del territorio nacional.

Entendiendo que Argentina es uno de los países con la tasa de penetración de internet más alta de la región, considerando la cantidad de recursos naturales estratégicos como petróleo, gas, agua dulce, biodiversidad o minerales estratégicos que tenemos en nuestra extensión geográfica, podemos concluir que estamos muy lejos de estar

protegidos y que seremos un blanco cada vez más interesante para diversos actores mundiales dentro del marco de una ciberguerra.

La realidad también muestra que si una organización plantea una ciberguerra como el objetivo para el desarrollo de un plan de protección de su infraestructura critica, claramente fracasara. Tenemos que empezar desde niveles más bajos, pensando en primera medida en errores involuntarios de usuarios con desconocimiento que pueden propiciar un ciberataque no dirigido, para luego evolucionar hacia políticas y procedimientos relacionados a incidentes dirigidos de ciberseguridad, como una ciberguerra.

Lamentablemente, falta mucha legislación, evangelización, presupuesto, pero por sobre todas las cosas, concientización.

25 – Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm

**Lista de referencias**

Páginas webs:


http://nuclearenergy.ir

http://www.cefadigital.edu.ar

https://www.incibe-cert.es

https://www.ccn-cert.cni.es

https://www.congress.gov

https://manuelsanchez.com/

http://www.infoleg.gov.ar

http://www.digesto.unc.edu.ar

https://www.brainpickings.org

http://diccionario.raing.es

https://m.isaca.org

https://www.kaspersky.com

https://dialnet.unirioja.es

https://elpais.com

https://www.pandasecurity.com

https://www.genbeta.com

https://www.welivesecurity.com

https://revistaitnow.com

https://www.symantec.com

https://www.itu.int

https://www.argentina.gob.ar