Instituto IDEAS

INSTITUTO DE ECONOMÍA APLICADA Y SOCIEDAD

Seguridad y defensa

CIBERDEFENSA Y CIBERDELITO

Dalila Nuñez Fernandez – Leonardo Cabral – Claudio Fernandez

Enero 2021

CIBERDEFENSA Y CIBERDELITO

Ante una realidad cada vez más globalizada, los límites geográficos se desdibujan con una rapidez galopante, el mundo presencia un nuevo paradigma en términos de seguridad y defensa. La clara expansión de las telecomunicaciones y el rol de que juega el ciberespacio han proporcionado un nivel de desarrollo en el términos de circulación de información sin precedentes, como así también a agilizado la vida de la población mundial, sin embargo ha traído a la par nuevos desafíos tanto para los individuos que forman una sociedad y a su vez han marcada una nueva agenda a las Entidades Estatales encargadas de proteger los intereses Nacionales y de sus ciudadania.

La defensa Nacional se encuentra en un proceso de modernización frente a las nuevas formas de amenazas que se presentan en una coyuntura signada por los ataques cibernéticos, como los perpetrados en la Dirección Nacional de Migraciones en Agosto de este año y el cibercrimen que se encuentra en la Argentina con un marcado ascenso en el número víctimas de estos delitos lo cuales entran en esta categoría cualquier actividad criminal que implica un ordenador. Cada año, la economía mundial pierde miles de millones de dólares como resultado de la actividad cibercriminal y la privacidad de los usuarios es puesta en grave peligro.

En el presente informe nos abocaremos a analizar las formas de cibercrimen presentes en el país y cuáles son los instrumentos que se poseen para la lucha contra este tipo de ataques. Para ello se utilizará bibliografía acerca del tema y cifras de algunas organizaciones que se especializan en la materia, se contará con el análisis de una entrevista hecha al General Anibal Intini Comandante de ciberdefensa del Estado Mayor Conjunto de las FF.AA. Los objetivos de este este informe serán la realización de un diagnóstico tentativo acerca de los límites y

desafíos que el país presenta para el mediano y largo en lo que respecta a Ciberdefensa.

I) DEFINICIONES Y TIPOLOGÍAS

- **Bot** es un programa informático que está preparado para realizar tareas repetitivas por medio de internet, el sistema es capaz de llevar a cabo funciones y proporcionar respuestas de forma más rápida y efectiva que un humano.

- **Tecnologías de la Información y la Comunicación** (TICS) conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento y transmisión de información, como por ejemplo voz, datos, texto, video e imágenes, entre otros.

- **Tecnologías del Aprendizaje y del Conocimiento** (TAC) tratan de orientar a las tecnologías de la información y la comunicación (TIC) hacia usos más formativos, tanto para el estudiante como para el profesor, profundizando en los conocimientos y habilidades necesarios para saber seleccionar y usar adecuadamente las herramientas para la adquisición de información en función de sus necesidades. Es decir, son tecnologías enfocadas al servicio del aprendizaje y adquisición de conocimiento,

- **Software** es un conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas,

- **Software de sistema** son los encargados de dar al usuario la capacidad de relacionarse con el sistema, para entonces ejercer control por sobre el hardware. El software del sistema también se ofrece como soporte para otros programas. Ejemplos: sistemas operativos, servidores, etcétera,

- **Software de programación.** Programas directamente diseñados como herramientas que le permiten a un programador el desarrollo de programas informáticos. Influyen en su utilización diferentes técnicas utilizadas y lenguaje de programación específico. Ejemplos: compiladores, editores multimedia, etcétera,

- **Software de aplicación.** Programas diseñados para la realización de una o más tareas específicas a la vez, pudiendo ser automáticos o asistidos. Ejemplos: videojuegos, aplicaciones ofimáticas, etcétera,

- **Hardware** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático,

- **Ofimática** conjunto de herramientas de informática que se utilizan para optimizar, mejorar y automatizar los procedimientos que se realizan en una oficina,

- **Algoritmo** un grupo de órdenes consecutivas que presentan una solución a un problema o tarea,

- **Algoritmo Informático** es una serie compleja de algoritmos escritos en un lenguaje de programación que pueden ser ejecutados en un ordenador,

- **Base de datos** conjunto de datos personales que son objeto de tratamiento o procesamiento electrónico y con diferentes modalidades de su formación, almacenamiento, organización o acceso.

- **Vehículos Autónomos** Es todo aquel vehículo que dispone de la capacidad de percibir el medio que le rodea y navegar en consecuencia, sin la intervención humana en su desplazamiento.

- **Vehículo Aéreo No Tripulado** (VANT) vehículo aéreo destinado a volar sin piloto a bordo y pilotado desde una estación de pilotaje a distancia, siguiendo planes de vuelo ordenados por medio de un *software* o sistemas de posicionamiento por coordenadas.

Sistemas Autónomos Letales SAAL

Ciber Resiliencia , la capacidad del sistema de sobrellevar los problemas tras las pérdidas de un ciberataque.

Ciberataque intento organizado causado por una o varias personas para provocar daños a un sistema informático o red. Estos ataques informáticos se aprovechan de alguna debilidad o vulnerabilidad del software o hardware.

OSI en sus siglas en inglés: Open Systems Interconnection conceptualmente se refiere a la arquitectura general requerida para

establecer comunicación entre computadoras, OSI puede verse de dos formas:como un estándar o como un modelo de referencia.

Cibernética: Ciencia que estudia comparativamente los sistemas de comunicación y de regulación automática o control en los seres vivos y en las máquinas. Fundada en 1948 por Norbert Wiener. "*Cibernética o el Control y Comunicación en animales y máquinas.*"

Control de los espacios comunes, refiriéndose al multidominio, según la publicación norteamericana denominada Capstone Concept for Joint Operations (Concepto Fundamental para las Operaciones Conjuntas), como aquel compuesto por tres categorías de dominio: la categoría Física (que incluía Tierra, Mar, Aire y Espacio), la Virtual (que abarca el Ciberespacio y la Información) y la Humana (que engloba los dominios Social, Moral y Cognitivo).

Diferencia entre ciberdefensa y ciberseguridad

II) CIFRAS EN LA ARGENTINA Y EJEMPLOS DE CIBERATAQUES

- ESTADÍSTICAS A NIVEL NACIONAL AÑO 2020

Tipo de delito	Porcentaje
Cyberbullying	18,75%
Fraude	16,56%
Extorsión online	13,75%
Phishing	12,12%
Calumnias	11,09%
Usurpación de identidad	7,18%
Amenazas	6,71%

Otros	4,06%
Pornovenganza	3,75%
Pornografía infantil	2,81%
Grooming	2,18%

Cuadro comparativo

Se comparan los periodos entre el 1 de marzo al 1 de Julio de los años 2016, 2017 , 2018 , 2019 y 2020 . Se observa un considerable aumento de consultas en los meses comprendidos entre marzo y julio de 2020 coincidentes con la cuarentena por Covid-19

Delitos más consultados desde el 20/3/2020 al 1/7/2020

Tipo de delito	Denuncias
Ciberbullying	120
Fraude	106
Extorsión online	88
Phishing	84
Calumnias	71
Usurpación de identidad	46
Amenazas	43
Otros	26
Porno venganza	24
Pornografía infantil	18

Nota : la usurpación de identidad , el Ciberbullying (hostigamiento) y la publicación

ilegítima de imágenes , sin bien son acciones dolosas aún no están contempladas en el

Código penal argentino – a excepción de CABA que las considera una contravención -.

El phishing puede ser utilizado para el robo de datos y la misión de fraudes , comercialización ilegal de información y / o extorsión .

El 29.68% de las consultas realizadas a nuestro equipo durante la cuarentena

corresponden a conductas dolosas no tipificadas . El 42,43% de los delitos consultados

representan – en la mayoría de los casos- tienen una finalidad economía (Fraude ,

phishing, extorsión) pudiendo llegar a 54% si se considera el móvil del phishing como

herramienta para cometer delitos con fines económicos.

Análisis de delitos más denunciados primer semestre 2020: Ciberbullying / hostigamiento digital.

Metodología: molestias , burlas , acoso , accionar persistente de contacto , otras accionas

perturbadoras que no constituyen delito

Legislación : No está contemplado en el Código Penal , aunque desde el año 2013 hay

varios proyectos. Solo CABA lo considera como una contravención con penas de multa .

Se observa un incremento de consultas por hostigamiento de un 108% considerando el

periodo de cuarentena marzo-julio 2020 y que dicha conducta no está tipificada por lo

tanto no puede ser denunciada .

Provincia	Porcentaje
Buenos Aires	36,20%
CABA	15,54%
Córdoba	13,60%
Mendoza	8,14%
Santa Fe	7,40%
Santiago del Estero	4,44%
Otras provincias	4,44%
Tucumán	2,96%
La Rioja	2,22%
Catamarca	1,48%
Jujuy	1,40%
Neuquén	0,74%
San Juan	0,74%
Salta	0,70%

Fraudes

Se observa un considerable incremento de esta modalidad delictiva a partir del segundo

semestre de 2019 incrementándose con la cuarentena iniciada en marzo de 2020 .

En comparativa primer semestre de 2019 y primer semestre de 2020 se observa un

incremento de casi un 72% .

Representa el 16,56% de las consultas recibidas durante la cuarentena pudiendo

incrementarse un 12,45% en los casos de phishing utilizando para extraer datos y luego

cometer fraude .

En las comparativas entre el último semestre de observamos un crecimiento constante

pronunciandose en los meses de junio , mayo y abril de 2020 . En noviembre y diciembre

se da un crecimiento considerable de consultas debido a dos oleadas de phishing

bancarios que llegaron a Argentina en esos meses .

Comparativa entre los periodos 1/3 – 1/7/2019 y 1/3 al 1/7/2020

En la comparativa se observa un incremento de este tipo de delitos superior al 110%

Metodologías:

- Phishing bancario
- Phishing con tarjeta de crédito
- Compras en portales no validados
- Compras a través redes sociales
- Compras / validaciones de datos telefónicas

Extorsión on line

Es un delito tipificado en el Código Penal Argentino y uno de los mas denunciados.

La extorsión on line al igual que el fraude se puede configurar de diferentes formas :

- A través de robo de contraseñas (hackeo o phishing previo)

- Posterior a la práctica de Sexting (sextorsión)
- Ransoware (encriptación por archivo malicioso)
- Posterior al robo de información

Comparativa entre los periodos 1/3 – 1/7/2019 y 1/3 al 1/7/2020

En la comparativa entre ambos periodos observamos un crecimiento de un 32%

considerando que en el mes de junio de 2019 se observó actividad muy constante de la

modalidad sextorsión.

Se observa un incremento constante desde el año 2016 de esta modalidad delictiva .

Como lo indica el gráfico los picos de consultas coinciden con oleadas masivas de emails extorsivos y/o casos de sextorsión conocida como "costa de marfil " .

En el inicio de la cuarentena , durante los primeros días de abril de 2020 se observa una

oleada masiva de emails en cuyo asunto figuraba una clave antigua del perfil de una red

social de la víctima . El contenido del email era claramente de contenido extorsivo

Durante el 2019 también se observó una oleada similar en el mes de junio como así

también una constante de sextorsión a gran escala. Este tipo de delitos por sus

características tiene un grado muy bajo de denuncia .

III) ANÁLISIS DE ENTREVISTA

Durante el desarrollo de la investigación tuvimos con una entrevista brindada por el General Anibal Intini Comandante comandante de ciberdefensa del Estado Mayor Conjunto de las FF.AA y nos proporcionó la perspectiva de la fuerzas de seguridad del Estado encargadas de proteger a la ciudadanía y puntualmente la información de los individuos parte de la sociedad argentina, como de la información sensible de país. Este encuentro mantuvo un diálogo fluido y una serie de temas que giraron en torno a las capacidades estatales en materia de Ciberdefensa y Cibercrimen, sobre la capacitación de las fuerzas de seguridad (sigue)-------

IV) DIAGNÓSTICO Y REFLEXIONES

Sobre el estado Argentino

Y su falta de política de ciberseguridad como política de estado.

Hay que leer las leyes de defensa nacional, ley de seguridad interior y ley de inteligencia nacional para hacer hincapié en que las FF.AA no pueden inmiscuirse en asuntos que son propios de fuerzas federales, no obstante, la falta de flexibilidad dentro del marco legal implica consecuencias.

Despenalización de la seguridad de la información, justamente para que los legisladores que trabajan de forma independiente, puedan hacer investigaciones sin ser acusados de ser delincuentes o atacantes.

¿Como es el "ciberdelincuente"?

Análisis V.I.C.A

Complejidad	Volatilidad
Capacidad material baja o pobre Desarrollo de las inteligencias artificiales Desarrollo de SAAL o sistemas autónomos letales	Incapacidad de negar ciberataques Falta de ciber resiliencia Múltiples ciberataques Escenario geopolítico con turbulencias

	Capacidades de inhabilitación remota de actores desconocidos.
Ambigüedad	Incertidumbre
Falta de decisión política e historial pésimo de ejecución de partidas presupuestarias. Ineficiencia	Economía inestable, sistema bimonetario quebradizo con moneda nacional débil El endeudamiento impide la compra de sistemas importantes al exterior.

Análisis FODA/SWOT

Fortalezas	Debilidades
Argentina no es un objetivo apetecible para ciberataques en comparación a otros estados con mayor relevancia en la arena internacional	Falta de presupuesto Carencias en el sistema educativo Carencias materiales Poca ciber resiliencia en las infraestructuras críticas Falta de concientización en la población tanto en su privacidad como en la protección de sus dispositivos y cuentas bancarias.
Oportunidades	Amenazas
Sanción del FONDEF y inversión pública en industria relacionada a la seguridad y el ámbito militar Capacidad técnica de empresas públicas y privadas asociadas a pymes para desarrollar nuevos sistemas. Coordinación y cooperación interministerial Innovación en la currícula militar de parte de las FFAA. Universidades destinadas a la defensa	Innovaciones de hackers en el ciberespacio Turbulencias en la geopolítica tras la pandemia

Ciberataques preventivos, y campañas de ataques simplemente para mostrar que tienen.

Recomendaciones a partir de la entrevista.

Fomento de dialogo entre técnicos y dirigentes

Con respecto a acuerdos con el sector privado.

Se debería instar al Ministerio de Educación de la Nación a incluir en la currícula escolar del nivel inicial, primario y secundario, materias teórico-prácticas obligatorias sobre programación, inteligencia artificial y robótica,

A través de la educación

Fomentar el estudio de carreras vinculadas a la programación e Inteligencia Artificial en las universidades nacionales y privadas. En otros niveles educativos, introducir de forma gradual información y/o asignaturas sobre Inteligencia Artificial, sus herramientas, investigaciones sobre el tema, desafíos, etc. Las escuelas y universidades deben incluir la ética, como el hacking etico y los temas relacionados en seguridad y privacidad, como parte integral de los planes de estudio sobre IA.

Generar acuerdos con empresas especializadas en el área de ciberseguridad y ciberdefensa en cuanto a las áreas del ministerio de defensa y ministerio de seguridad.

Fomentar acuerdos entre empresas privadas con ministerios provinciales de educación que busquen enseñar mediante cursos terciarios, diplomaturas o tecnicaturas programación, ciencia de datos o desarrollo web para que las comunidades educativas de enseñanza secundaria tengan en cuenta estas carreras.

El Estado nacional, las Provincias y CABA los municipios y las organizaciones no gubernamentales (ong) pueden actuar como agentes para el desarrollo y concientización contra ciberdelitos, el derecho a la privacidad, la autenticación de cuentas bancarias y billeteras virtuales, cada fuerza de

seguridad provincial debería de tener agentes especializados en ciberdelitos capaces de responder a las denuncias de la población.

Se debería de instar al Poder Ejecutivo Nacional a realizar las obras correspondientes conforme a lo establecido en la Ley 27.078 para lograr el objetivo de erradicar la brecha digital en la comunidad educativa y a su vez llevar a cabo campañas de concientización y aprendizaje en el uso de nuevas tecnologías, fomentar el aprendizajes de lenguajes de programación como C++, Python o Sharp.