Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Aportes de la cibercriminología a la ciberseguridad y prevención del cibercrimen

AUTOR: LIC. NAHUEL FERNANDO GRIFFA ZIMA

DIRECTOR: MG. ING. JORGE ESTEBAN ETEROVIC

POSGRADO: MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

SEPTIEMBRE 2024

Resumen

Este trabajo de investigación abordará la temática de cibercrímenes y delitos informáticos, incluyendo ciberataques técnicos por malwares y denegación de servicios (sabotaje informático), aquellos que no son técnicos y no requieren de conocimientos en informática y redes, como los delitos contra la integridad sexual (grooming y la -mal llamada- pornografía infantil), delitos contra la propiedad (estafas y otras defraudaciones a través de técnicas de ingeniería social), y también aquellas acciones maliciosas que no están tipificadas en el Código Penal Argentino, relacionadas con la violencia digital y de género que causan un verdadero tormento en la vida de las víctimas; desde una perspectiva criminológica, entendiendo el fenómeno social de las causas, consecuencias, factores endógenos y exógenos de los delincuentes y de las víctimas, así también sus aspectos socioeconómicos y psicológicos.

En Argentina, existe una falta de educación temprana en materia de Ciberseguridad, que desemboca en un incidente causado por la falta de concientización y la ausencia de elementos de protección. Acceder a los conocimientos relacionados con la Ciberseguridad es sólo para aquellas personas que deciden hacer un curso o estudiar carreras universitarias afines y no desde temprana edad en los colegios. Este trabajo propone incorporar en la educación primaria y secundaria las asignaturas correspondientes para formar niños y adolescentes conscientes de los riesgos que implica utilizar internet, y así mantener las protecciones en su vida adulta. Con educación temprana, herramientas y conceptos de seguridad, se puede reducir considerablemente el número de víctimas por ciberataques, tanto usuarios comunes como empleados de la industria IT. Además, la reducción del número de víctimas implica, consecuentemente, la reducción de los gastos en investigaciones forenses posteriores.

La Criminología y la Ciberseguridad son dos ciencias multidisciplinarias, es decir que se componen de varias disciplinas. La primera tiene como objetivo la prevención del delito mediante la aplicación de políticas públicas, mientras que la segunda tiene como objetivo el resguardo de la información, en cualquier medio de almacenamiento (físico, digital o mental). Ambas, en conjunto, pueden explotar la prevención del cibercrimen. La Cibercriminología, como área emergente de la Criminología, está enfocada a la prevención de los delitos informáticos o del cibercrimen, explicando distintos fenómenos con un lenguaje llano, no técnico, estudiando a los distintos tipos de cibercrímenes, las teorías criminológicas, los perfiles psicológicos criminales, los tipos de criminales existentes y

aún no categorizados, los distintos modus operandi cibercriminales según los objetivos; y la Cibervictimología.

En este trabajo, se analizarán las causas de los incidentes de ciberseguridad mediante estudios bibliográficos y análisis de casos para comprender las motivaciones de los cibercriminales, se ilustrarán todas las acciones maliciosas con el uso de internet y de las tecnologías de la información y la comunicación, para hacer un claro foco en la prevención y en un plan de educación temprana en materia de ciberseguridad, brindando la información necesaria para implementar ciertas medidas de seguridad que protejan nuestra información, datos, dispositivos, dinero, libertad, propiedad, honor e integridad.

Palabras claves:
Cibercriminología, Ciberseguridad, Criminología, Cibercrimen, Delitos informáticos.

Abstract:

This research will address the topic of cybercrime and computer crimes, including technical cyberattacks by malware and denial of service (computer sabotage), those that are not technical and do not require knowledge of computers and networks, such as crimes against sexual integrity (grooming and the -misnamed- child pornography), crimes against property (scams and other frauds through social engineering techniques), and also those malicious actions that are not classified in the Argentine Penal Code, related to digital and gender violence that cause true torment in the lives of victims; from a criminological perspective, understanding the social phenomenon of the causes, consequences, endogenous and exogenous factors of criminals and victims, as well as their socioeconomic and psychological aspects.

In Argentina, there is a lack of early education in Cybersecurity, which leads to an incident caused by the lack of awareness and the absence of protective elements. Access to knowledge related to Cybersecurity is only for those people who decide to take a course or study related university courses and not from an early age in schools. This work proposes incorporating the corresponding subjects in primary and secondary education to educate children and adolescents who are aware of the risks involved in using the Internet, and thus maintain protections in their adult life. With early education, tools and security concepts, the number of victims of cyberattacks can be considerably reduced, both common users and employees of the IT industry. In addition, the reduction in the number of

victims consequently implies the reduction of expenses in subsequent forensic investigations.

Criminology and Cybersecurity are two multidisciplinary sciences, that is, they are made up of several disciplines. The first aims at preventing crime through the application of public policies, while the second aims at safeguarding information, in any storage medium (physical, digital or mental). Both, together, can exploit the prevention of cybercrime. Cybercriminology, as an emerging area of Criminology, is focused on the prevention of computer crimes or cybercrime, explaining different phenomena in plain, non-technical language, studying the different types of cybercrimes, criminological theories, criminal psychological profiles, existing and yet-to-be-categorized types of criminals, the different modus operandi of cybercriminals according to their objectives; and Cybervictimology.

In this work, the causes of cybersecurity incidents will be analyzed through bibliographic studies and case analysis to understand the motivations of cybercriminals, all the negative aspects of the use of the Internet and information and communication technologies will be illustrated, to make a clear focus on prevention and an early education plan on cybersecurity, providing the necessary information to implement certain security measures that protect our information, data, devices, money, freedom, property, honor and integrity.

Agradecimientos

A Pablo Biderman, docente del curso “Seguridad de la Información” de mi trabajo en Presidencia de la Nación, quien me abrió la cabeza a un nuevo paradigma de pensamiento a nivel preventivo en mis dispositivos móviles; a Claudio Caracciolo, docente de la materia Ciberseguridad en la Especialización en Cibercrimen y Evidencia Digital de la Facultad de Derecho en la Universidad de Buenos Aires, quien enseñó los fundamentos de la Ciberseguridad de una manera práctica y quien me ayudó a decidir sobre la elección de seguir creciendo profesionalmente en este campo; a Cristian Borghello, docente de las materias Malware I y Malware II de la Maestría en Ciberdefensa y Ciberseguridad de la Facultad de Ciencias Económicas en la Universidad de Buenos Aires, quien nos ha brindado un sinfín de conocimientos teóricos y técnicos de primerísima calidad en materia de cibercrimen y ciberseguridad; a Stella Mary Ortega, psicóloga forense, criminóloga, mentora y amiga, con quien compartí mi voluntariado en Grooming Argentina en el Área de

Investigación Forense y me dio a conocer el concepto de la Cibercriminología; a Julián Reale, coordinador de la carrera de Especialización en Cibercrimen y Evidencia Digital de la Facultad de Derecho en la Universidad de Buenos Aires, por su gran acompañamiento durante mi elaboración de anterior tesis de posgrado; a Víctor Aquino, profesor de la materia "Informática Forense" en la Licenciatura en Criminalística en el Instituto Universitario de la Policía Federal Argentina, quien, en su momento, advertía sobre los nuevos usos de la informática, las problemáticas y los desafíos a nivel investigativo, pericial, penal y comunicacional; a los directivos de la Maestría, Carlos Amaya y Roberto Uzal, quienes motivaron a diario el compromiso de formarme como magíster; y a mi familia, principalmente a Victoria Sol Salamino, por su incondicional amor, compañía, apoyo y ánimo para seguir creciendo como profesional.

ÍNDICE

RESUMEN **2**

Abstrac 3

Agradecimientos 4

PRIMERA PARTE

INTRODUCCIÓN

CAPÍTULO I: INTRODUCCIÓN, PROBLEMA, SOLUCIÓN Y SUSTENTO **8**

I.I) Presentación 8

I.II) Hipótesis 9

I.III) Objetivos 9

I.IV) Motivación 9

I.V) Estado del arte 11

I.VI) Contribuciones de este trabajo 13

I.VII) Estructura de la tesis 13

I.VIII) Planteamiento del problema 14

I.IX) Contexto histórico 15

I.X) Situación actual 15

I.XI) Solución propuesta 16

I.XII) Sustento de la solución planteada 16

SEGUNDA PARTE

MARCO TEÓRICO

CAPÍTULO II: INTRODUCCIÓN A LA INFORMÁTICA **17**

II.I) La Informática y sus aplicaciones 17

II.II) Hardware y software 21

II.III) Redes informáticas 24

II.IV) Dirección IP, dominios y anonimato 28

II.V) Seguridad en redes 31

CAPÍTULO III: INTRODUCCIÓN A LA CRIMINOLOGÍA 36

III.I) La Criminología 36

III.II) Criminogénesis de la delincuencia 39

III.III) Victimología 41

III.IV) Perfilación Criminal 42

III.V) El sistema penal 43

III.VI) Delitos informáticos 45

TERCERA PARTE

CIBERCRIMINOLOGÍA

CAPÍTULO IV: CIBERSEGURIDAD 55

IV.I) Ciberseguridad 55

IV.II) Modelo OSI y la "capa 8" 57

IV.III) Ciberataques 59

IV.IV) Grupos cibercriminales 66

IV.V) Ingeniería social 69

IV.VI) Inteligencia artificial y nuevos desafíos 71

CAPÍTULO V: ASPECTOS CRIMINOLÓGICOS DEL CIBERCRIMEN 78

V.I) Cibercriminología 78

V.II) El ciberespacio 79

V.III) Cibercrimen 80

V.IV) Tipos de cibercrímenes 83

V.V) Ciberguerra 87

V.VI) Violencia digital 90

V.VII) Perfiles cibercriminales 94

V.VIII) Cibervictimología 100

CONCLUSIONES 103

BIBLIOGRAFÍA 109

PRIMERA PARTE

INTRODUCCIÓN

CAPÍTULO I: "INTRODUCCIÓN, PROBLEMA, SOLUCIÓN Y SUSTENTO"

I.I) Presentación

En cada evento de ciberseguridad, tenemos 3 elementos de interés criminológico: un victimario o grupo criminal, un blanco (víctima humana u objetivo informático) y la ausencia de elementos de protección o de un guardián. La convergencia de estos 3 elementos, constituyen un ciberdelito.

En este escrito abordaremos temas relacionados con algunos aspectos criminológicos del cibercrimen, para entender el porqué de las conductas cibercriminales, por qué se elige a ciertas víctimas y por qué el ciberespacio es una oportunidad propicia para los delitos informáticos. Entre estos temas, veremos los distintos tipos de cibercrímenes que existen (puros, réplicas o físicos y de contenido), los elementos necesarios para que pueda ocurrir un ciberdelito (según teorías criminológicas), los perfiles psicológicos criminales de los victimarios, los perfiles de las víctimas y los distintos métodos y técnicas de ciberataques según motivación de los actores. Además, veremos algunas acciones maliciosas relacionadas con la violencia digital y violencia de género digital, que no son delitos y generan un verdadero tormento en la vida de las víctimas.

Si bien el término Cibercriminología es relativamente nuevo y no hay muchos autores que traten la materia, Jahankhani (2018) dice que es una ciencia multidisciplinaria que abarca diversas disciplinas, tales como la Criminología, la Victimología, la Sociología, la Ciencia de Internet y las Ciencias de la computación. Es por ello que, para abordar esta tesina, necesito de un marco teórico extenso que trate diversos temas, desde el uso de la informática en nuestra vida diaria y las redes de comunicación entre dispositivos electrónicos; conceptos básicos de la Criminología, entender los delitos informáticos tipificados en nuestro Código Penal de la Nación y nociones de Ciberseguridad que hacen a la prevención de los ciberataques.

Al ser una ciencia multidisciplinaria, necesito de un marco teórico extenso que trate diversos temas, desde el uso de la informática en nuestra vida diaria y las redes de comunicación entre dispositivos electrónicos; conceptos básicos de la Criminología, la perfilación criminal como disciplina; los delitos informáticos tipificados en nuestro Código Penal de la Nación; las acciones maliciosas que no son delitos y generan un tormento para

la víctima, como por ejemplo la difusión no consentida de imágenes o videos íntimos o el ciberbullying; distintas temáticas relacionadas con la Ciberseguridad, incluyendo los distintos tipos de ciberataques, ciberestafas; y mucho más.

Todo este trabajo está escrito en un lenguaje llano que pueda ser entendido por todas aquellas personas que no tienen conocimientos técnicos.

I.II) Hipótesis

Aplicar la Cibercriminología brindará las herramientas necesarias a los usuarios de internet para reducir el número de víctimas de ciberdelitos, formando una adecuada concientización y preparación para la prevención del cibercrimen en la sociedad, integrando programas de educación temprana en ciberseguridad en el sistema educativo argentino, desde la educación primaria hasta la secundaria.

I.III) Objetivos

- Objetivos generales**:** Analizar los elementos de la Cibercriminología que permitan determinar el porqué de la conducta delictiva en el ciberespacio, el porqué de la elección de víctimas y la implementación de herramientas de prevención necesarias que reducirán el número de víctimas de ciberdelitos.

- Objetivos específicos:

  - Investigar las distintas acciones y herramientas maliciosas que existen en el ciberespacio;
  - Estudiar las características de los ciberdelincuentes;
  - Estudiar las características de las víctimas de ciberdelitos y;
  - Determinar las herramientas de prevención necesarias;

I.IV) Motivación

Este trabajo tiene la finalidad de hacer un claro foco en la prevención del cibercrimen, desde la perspectiva de cualquier persona que utilice alguna TIC (tecnología de la información y comunicación), brindando la información necesaria que permita implementar ciertas medidas de seguridad para reducir, eventualmente, el número de víctimas futuras y para resguardar nuestra información, datos, dispositivos, dinero, libertad, honor e integridad.

En la última década, los avances tecnológicos y la llegada del Covid-19, que nos obligó a aislarnos, permitieron que la mayoría de las personas en el mundo estemos conectadas a través de nuestros dispositivos electrónicos (celular, tablet, computadora, consola de video juegos) con conexión a internet. De esta manera, hoy en día podemos chatear, hablar y jugar con cualquier persona en cualquier parte del mundo, realizar operaciones bancarias y comerciales, como inversiones, compras y también estudiar o trabajar desde nuestra casa con nuestra computadora o teléfono.

Esta migración hacia el plano online no sólo permitió realizar de manera positiva todas estas acciones, sino que también trajo consigo una serie de acciones maliciosas. Antes, si una banda de ladrones iba a robar un comercio, debía planear la llegada, utilizar la violencia con armas, reducir personas, robar el dinero y planear la huida para escapar de la policía. Hoy, un ciberdelincuente puede trabajar completamente solo, robando el dinero de tu cuenta bancaria con sólo un clic o toque, en cualquier parte del mundo y casi sin darnos cuenta. Antes, cuando un ladrón tenía que ir y robarle a una persona, hoy nos pueden robar por alguna técnica de manipulación o estafa (ingeniería social, el famoso "cuento del tío", pero con internet), por ingresar a una página web falsa y escribir nuestros datos bancarios o contraseñas, o incluso por tener instalado en nuestro dispositivo un programa malicioso que le esté enviando la información de todo lo que hacemos, vemos o escribimos a un ciberdelincuente, que puede estar en cualquier parte del mundo.

Ante el eventual crecimiento exponencial de los distintos ciberataques y delitos informáticos, las distintas empresas en el mundo también se vieron obligadas a revolucionarse a sí mismas y a sus sistemas de seguridad. Por ejemplo, la plataforma de videollamadas Zoom, antes de la pandemia, era totalmente desconocida por el popular de la gente. Una vez comenzado el aislamiento obligatorio, las clases tuvieron que migrar a Zoom, pero la plataforma carecía de sistemas de seguridad fuertes y era blanco de múltiples ciberataques. Era frecuente ver en las noticias que personas ajenas a las clases podían ingresar a la sala.

Por otro lado, navegamos por la aplicación Telegram y descubrimos que existen decenas de grupos de barrios de compra y venta de drogas, entre otras cosas, tan libremente. Anonimato, venta de drogas, pornografía, servicios sexuales y hasta material de abuso sexual contra las infancias (mal llamada "pornografía infantil") son algunas de las acciones que más se encuentran en Telegram. ¿Por qué Telegram y no otra aplicación? Básicamente, porque prevalece el anonimato.

Así como existen delitos que atentan conta nuestro patrimonio, existen otros que pueden alterar o destruir nuestros archivos o todo nuestro dispositivo electrónico; y también los delitos contra la integridad sexual, como lo es el grooming (abuso sexual hacia niños, niñas y adolescentes a través de dispositivos electrónicos) y la mal llamada "pornografía infantil", donde esa foto o ese video es la clara evidencia del abuso sexual físico que recibió esa víctima y la viralización de ese contenido multimedia genera la revictimización constante de ella.

Pensemos que, mientras la gran mayoría de nosotros creció sin computadoras y recién empezamos a utilizarlas de adolescentes o adultos, hoy en día y desde hace más de una década, los niños, niñas y adolescentes juegan desde su dispositivo electrónico, teniendo la posibilidad de hablar con quién sea en cualquier parte del mundo. Entonces, si nosotros no entendemos cómo funciona internet y qué problemas puede generar, ¿cómo podemos protegerlos/as de pedófilos y pederastas digitales?

A modo de analogía, la educación vial aparece en los últimos años de la educación media y consta de una charla corta y muy esporádica. En Argentina, tenemos una cantidad muy numerosa de siniestros viales, por lo que estas premisas nos dan la conclusión de que este tipo de educación no sirve.

I.V) Estado del arte

No existen autores argentinos que hablen de Cibercriminología y no se escucha con frecuencia en nuestro país este término. Es por ello que los antecedentes de libros que hablan sobre esta disciplina son, principalmente, de autores españoles. Sí podemos afirmar que, si bien no utilizan el término "Cibercriminología" varios autores argentinos han escrito obras pilares sobre la criminología de los delitos informáticos (Gustavo Saín, Marcelo Riquert, Pablo Palazzi, Daniela Dupuy, entre otros).

El más relevante, para mí, es El Cibercrimen[1], de Fernando Miró Llinares, publicado en 2012, pero el autor nunca utiliza la palabra "cibercriminología", sino que habla siempre de la criminología de la ciberdelincuencia. El problema que radica con este libro es la antigüedad que presenta. Si bien los conceptos criminológicos y la base técnica informática son los mismos, la tecnología, los usos, los ciberataques y la disponibilidad de herramientas maliciosas han avanzado mucho en 10 años.

[1] Miró Llinares, Fernando: *El cibercrimen*, Marcial Pons, Madrid, 2012

Por otro lado, también hay un artículo escrito por Sergio Cámara Arroyo[2], publicado en una revista llamada Derecho y Cambio Social, titulado "Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente" en el 2020. Si bien este artículo es reciente, recopila información de distintas fuentes que no son contemporáneas, repite conceptos de Miró Llinares del 2012 y hace una clasificación de perfiles cibercriminales que, a mi parecer, no sólo está enfocada a perfiles técnicos, sino también que utiliza nombres de nomenclatura antigua y en inglés, extraída de otros autores. Lo que es destacable de este artículo es que traduce al español algunas definiciones de cibercriminología de autores como Kyung-Shick Choi (estadounidense) y Jahankhani (inglés).

Otro libro muy interesante es "Cibercriminología y victimización online"[3] (2020). Escrito por José R. Agustina, Irene Montiel Juan y Manuel Gámez-Guadix. Este libro está focalizado en lo que llamamos cibercrimen físico con motivación social, es decir, en acciones y delitos donde el objetivo es afectar directamente a la víctima, como grooming, el material de explotación sexual infantil, ciberacoso, la violencia digital, cyberbullying, cyberstalking y discurso de odio. Los autores hacen hincapié en los problemas que la víctima enfrenta.

Abel Gonzales García es un criminólogo español y profesor de Criminología de la Universidad a Distancia de Madrid. Él fue un estudioso de los postulados de Miró Llinares y ha escrito algunos artículos de revista relacionados. Además, ha realizado colaboraciones en obras colectivas en la escritura de algunos capítulos de ciertos libros sobre Criminología y Cibercriminolgía. Durante el trascurso de este trabajo, citaré algunas frases de este autor.

Por último, cabe mencionar la existencia de un libro muy interesante, un poco más actual y enfocado bastante en ciberataques, pero no logré tener acceso y poder leerlo. Este libro[4] está titulado "Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Seguridad Digital" (2018). Escrito por Marlon Mike Toro Álvarez y Kyung-shick Choi, de la Editorial Universidad Antonio Nariño.

---

[2] Arroyo, Sergio Cámara: "La Cibercriminología y el perfil del ciberdelincuente" en *Derecho y cambio social;* 60, Lima, 2020.

[3] Agustina, José R.; Montiel Juan, Irene, y Gámez-Guadix, Manuel: *Cibercriminología y victimización online,* Síntesis, Madrid, 2020.

[4] Kyung-Shick, Choi y Toro Álvarez Mike, Marlon Mike: *Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital,* Universidad Antonio Nariño, Bogotá, 2018.

I.VI) Contribuciones de este trabajo

Los conocimientos de ciberseguridad generarían en la gente una gran concientización en materia de protección personal. Ya sea que apliquen configuraciones de seguridad y privacidad o limiten el uso de redes sociales, cambiando a un perfil privado, filtrando las solicitudes de amistad o la información que se decide compartir. Está comprobado que la primera capacitación en materia de ciberseguridad o seguridad de la información abre muchísimo la cabeza de las personas y abre un nuevo paradigma de pensamiento.

El problema radica en que no todas las personas pueden acceder a una capacitación de esta índole, ya sea por ignorancia total de estos temas, desinterés, falta de dinero, falta de tiempo, miedo a no entender nada "por ser técnico", por falta de oportunidad, por considerarse que no son idóneos en la materia, por miedo a pensar que tienen que estudiar, entre otras razones.

Este trabajo no sólo contribuye a concientizar a los lectores, sino que además propone que la concientización comience a temprana edad. Si logramos implementar la ciberseguridad en la educación primaria y secundaria, tendríamos un futuro altamente capacitado y concientizado sobre los buenos usos y protecciones de los dispositivos electrónicos e internet. Así, lograríamos reducir el número de víctimas por ciberataques y, por consiguiente, reducir el volumen y los costos de las investigaciones forenses posteriores.

I.VII) Estructura del trabajo

Este trabajo de investigación consiste en la revisión y análisis del material bibliográfico sobre Cibercriminología y casos de uso basados en notas periodísticas e informes oficiales, junto con los conocimientos adquiridos y trabajos realizados durante la cursada en la Maestría en Ciberdefensa y Ciberseguridad, para poder estudiar y clasificar a los distintos tipos de cibercriminales, con un enfoque exploratorio descriptivo no experimental.

Primero, se considera importante construir un marco teórico relacionado con la Informática y la Criminología, para introducir al lector en temas generales. Luego, es importante abordar temáticas relacionadas con la Ciberseguridad y las acciones maliciosas existentes en el ciberespacio. Posteriormente, reunir y analizar material bibliográfico que trate sobre Cibercriminología y perfiles cibercriminales para escribir una tesina original y amoldada a los problemas actuales. Por último, realizar una conclusión a partir de toda la información reunida y analizada, para responder a los objetivos de este trabajo.

Este trabajo presenta distintos temas relacionados principalmente con la Informática y con la Criminología. Como el objetivo es prevenir ser víctimas de ciberdelitos, se ilustrarán distintos temas que acompañen a un lector que no tenga conocimientos técnicos, en un lenguaje llano. Hay muchos aspectos técnicos y profundos que no se abordarán, porque podrían confundir al lector. Por otro lado, si bien la Criminología tiene muchísima relación con el Derecho Penal, este trabajo no hará foco en los delitos informáticos tipificados en el Código Penal Argentino, sino que hablaremos de las acciones maliciosas en el ciberespacio en relación con las motivaciones (el por qué) de los atacantes.

I.VIII) Planteamiento del problema

Navegar por internet es como salir de nuestras casas, dejando la puerta abierta (un puerto) y confiarse de que nadie va a entrar a nuestro hogar (nuestro dispositivo). Esta analogía con la realidad se entiende claramente cuando pensamos que, en el pasado, las personas vivían dejando la puerta abierta de sus domicilios, ya que no había delincuencia. Hoy en día, casi nadie tiene el lujo de vivir en un lugar sin cerrar la puerta y sin ponerle seguro (cerrar con llave). Lo mismo sucedió con internet y aún más con la llegada del Covid y el aislamiento, donde los delincuentes tuvieron que adaptarse al mundo digital. En el pasado, los pocos cibercriminales tenían un gran conocimiento técnico en redes y programación. Hoy en día, cualquier persona sin estudios ni conocimientos técnicos puede ser un potencial ciberdelincuente.

A pesar de los avances tecnológicos, la cantidad de normas y las numerosas capacitaciones en materia de ciberseguridad, los ciberincidentes siguen sucediendo a diario y de manera catastrófica. En su mayoría, las empresas u organismos del Estado son ciberatacadas por un software malicioso de tipo ransomware. Esto significa que un empleado realizó un mal uso de los recursos del establecimiento laboral, es decir, básicamente, que ingresó a un sitio web o hizo click en un link malicioso. Esto denota cierta confianza de los usuarios al manipular dispositivos electrónicos sin los recaudos necesarios. Si las grandes empresas y organismos estatales están siendo víctimas de ciberataques exitosos frecuentemente, imaginar a las personas comunes que sólo tienen un celular.

Nuestros padres o abuelos nos enseñaron que no debemos hablar con desconocidos en la calle, y probablemente hemos transmitido esa enseñanza. De la misma manera, ustedes ¿enseñaron que no se debe hablar con desconocidos en internet?

I.IX) Contexto histórico

Si el lector de este trabajo tiene más de 25 años de edad, seguramente se haya criado en un hogar sin computadoras ni smartphones. Esto significa que, la mayoría de nosotros, tuvimos que adaptarnos a las nuevas tecnologías, sin saber nada sobre ellas. Sólo unas pocas personas idóneas en las ciencias de la computación tenían conocimientos técnicos den programación, sistema binario o el uso de BIOS para un mayor uso de las computadoras.

Los primeros "hackers" fueron estas pocas personas con conocimientos técnicos. Sus objetivos podían ser jugar, molestar y/o ganar prestigio. Además, la falta de leyes y desconocimientos sobre informática en el Derecho los amparaba para realizar cualquier acción maliciosa y causar daño. Sin embargo, no tenían una motivación económica; y la justificación es clara. Dañar un sistema o dejarlo inutilizable, no genera dinero. Contrario a eso es robar datos para venderlos en la dark web, secuestrar archivos para exigir rescate, los troyanos bancarios o spywares que recolectan credenciales, la ingeniería social, el phishing y la suplantación de identidad, entre otros.

I.X) Situación actual

Según un reporte realizado por el Ministerio Público Fiscal de la Nación Argentina, entre los meses de mayo y junio del 2023, hubo 3003 investigaciones de ciberdelitos, de los cuales el 58% representan las estafas por medios digitales, un 12,3% a robo de credenciales, un 8,8% a robo de credenciales con impedimento de acceso, un 4,3% a MASI (material de abuso sexual contra las infancias), un 2,5% de grooming (abuso sexual online) y un 14,1% de otros. Esto significa que, a pesar de los grandes incidentes técnicos a las grandes organizaciones, las personas comunes representamos la mayor cifra de víctimas por ciberdelitos. Cualquiera puede ser víctima de alguna estafa, un cuento del tío o cualquier técnica de ingeniería social.

El párrafo anterior nos ilustra que un 64,8% de los ciberdelitos no son técnicos. No requieren ningún tipo de conocimiento en redes o programación. Sólo se basan en engaños y en saber usar un celular con redes sociales. También, hay que tener en cuenta que el robo de credenciales también puede suceder por técnicas de ingeniería social. Suponiendo ese caso, la cifra de ciberdelitos no técnicos sería del 85,9%.

El problema está explícito. Existe una clara numerosa cantidad de ciberincidentes, gracias a una falta de seguridad, provocada por la falta de educación general en materia

de ciberseguridad. Es por ello que la aparición de la Cibercriminología ayudaría a proponer soluciones de concientización, formación y educación en materia de ciberseguridad, para cualquier persona, frente a cualquier actividad maliciosa en el ciberespacio y desde temprana edad. La solución ideal para reducir la cantidad de víctimas de ciberdelitos sería la implementación de educación sobre ciberseguridad en escuelas.

I.XI) Solución propuesta

Resulta evidente la ausencia de educación digital a nivel nacional en todos los niveles académicos. Sólo quienes tuvieron la suerte de estudiar alguna carrera relacionada a la informática saben algunos concejos de seguridad, o quienes en su trabajo tuvieron la posibilidad de asistir a algún curso relacionado. En mi caso, como Licenciado en Criminalística, ni en la materia Informática Forense estudié conceptos de ciberseguridad o de prevención.

Por lo expuesto en el párrafo anterior, lo que se propone en este trabajo es una concientización a nivel general de todas las acciones maliciosas en el ciberespacio (delitos y no delitos) para crear campañas de concientización que sean entendidas por toda la sociedad en general. Esto implica hablar en un lenguaje llano y bajar a tierra los conceptos técnicos, para que cualquier persona pueda entender los riesgos que existen en internet.

Además, exponer la ausencia total de educación digital a temprana edad, supondría la toma de consciencia en colegios y demás instituciones educativas o clubes, mínimamente frente a los riesgos más frecuentes a los que los chicos y chicas pueden estar expuestos, como el grooming.

Si bien este trabajo tiene como finalidad una presentación de concientización, sería un éxito lograr la implementación de la educación digital en algún colegio.

I.XII) Sustento de la solución planteada

Tal como expusimos en el apartado anterior, la principal solución propuesta es la de armar una presentación de concientización a nivel general, para toda la sociedad, con y sin estudios. Para ello, al final de este trabajo se enumerarán las principales soluciones que les permitirán a las generaciones futuras generar herramientas de seguridad que la "educación digital" podría implementar en las escuelas.

SEGUNDA PARTE

MARCO TEÓRICO

CAPÍTULO II: "INTRODUCCIÓN A LA INFORMÁTICA"

II.I) La Informática y sus aplicaciones

Si vemos a nuestro alrededor, necesariamente nos damos cuenta de que la informática forma parte de nuestras vidas. Se confía a sistemas computarizados innumerables situaciones críticas, se confían datos críticos, datos personales, etc. En cualquier ambiente en el que pensemos, tenemos la hoy por hoy necesaria intromisión de los sistemas informáticos. Vemos informática, en hospitales, en comercios, en la educación, en registros de nuestras propiedades y bienes, en los sistemas bancarios y hasta en nuestra propia casa. Por otro lado, la velocidad en la que se están dando los cambios, es una característica que no se puede dejar de lado. En los 70, no se pensaba que la evolución de los sistemas informáticos sería tan masiva, no era imaginable la cantidad de celulares de hoy en día, ni sus capacidades de comunicación, de almacenamientos y de interconexiones con otros dispositivos de datos. Tampoco se pensó en la enorme capacidad de almacenamiento ni velocidad de proceso alcanzado hoy en día. Entre otras innumerables realidades, la incorporación de soluciones informáticas a situaciones sencillas y cotidianas de la vida social humana (redes sociales, electrodomésticos inteligentes que almacenan datos, GPS, control de acceso, etcétera) han realizado (y realizan constantemente) un cambio profundo en las relaciones y en las estructuras tradicionales, que nos llevan a transitar un camino nuevo.

Entre las definiciones para informática podemos encontrar:

- Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras.[5]

- Es la ciencia que estudia el tratamiento automático y racional de la información." Se dice que el tratamiento es automático por ser máquinas las que realizan los trabajos de captura, proceso y presentación de la información, y se habla de racional por estar todo el proceso definido a través de programas que siguen el razonamiento humano.[6]

- Disciplina que estudia la gestión de la información, generalmente, pero no de manera exclusiva por medio de elementos computacionales. No obstante, su aplicación

[5] Diccionario de la Real Academia Española.
[6] Alcalde, Eduardo: *Informática Básica*, McGraw-Hill, Madrid, 1994, p.1.

como herramienta es abarcativa de toda ciencia humana, cualquiera sea la teoría de conocimiento que se considere cierta.[7]

La palabra computación proviene del inglés computing, cálculo. Término de uso general para referirse a cualquier tipo de operación aritmética realizada en forma automática, según conjunto de reglas. La Real academia Española, define "computación" como sinónimo de cálculo. En el Manual de Informática Forense de Arellano Gonzalez-Darahuge, define como "…el empleo particular pero no exclusivo de la computación de datos, como instrumento de la gestión de los activos informáticos. No obstante, es más un medio que una disciplina propia." Literalmente, computación es el conocimiento de sistemas computarizados.

Las computadoras son esenciales para enfrentar el reto de la competencia global, donde los negocios deben ser eficientes y sensibles a las necesidades y producir bienes y servicios de alta calidad a un costo siempre más bajo. Sin las computadoras, que proveen información precisa y actualizada necesaria para tomar decisiones estratégicas y administrar los procesos de producción, muchas compañías no podrían sobrevivir. Las computadoras utilizan información almacenada para construir simulaciones que van desde un simple análisis hasta ilustraciones realistas y animadas de nuevos productos. Esto permite predecir el efecto de las múltiples decisiones de negocios. Las computadoras ayudan a la gente a comunicarse, tanto directa como indirectamente.

El mundo industrial no podrá vivir mucho tiempo sin computadores, está sometido a una sobrecarga de información y no podrá manejarlos sin ellos. Teniéndose en cuenta que los avances de la sociedad humana desde la aparición del alfabeto se han debido a su capacidad de registrar y conservar la información.

Actualmente la informática tiene tantas aplicaciones que prácticamente es inconcebible pensar que exista un campo o área donde la informática no esté presente.

En el área Administrativa: El manejo de la información es actualmente una de las actividades más importantes de la sociedad moderna. Esto se puede observar por el alto porcentaje del trabajo cotidiano que se dedica al procesamiento y comunicación de la información. Por otra parte, los Sistemas Gerenciales están basados en la integración de las diferentes áreas funcionales de una organización como son: Mercadeo, Finanzas, Contabilidad, Producción, Presupuesto, Recursos Humanos, Alta gerencia.

[7] Darahuge y Arellano Gonzalez: *Manual de Informática Forense*, Errepar, Buenos Aires, 2011, p. 19

En la toma de decisiones: son de gran utilidad los programas que pueden generar gráficos de uso administrativos como son: barras, torta, línea y área entre muchos otros. De esta manera, un empresario puede tener una idea rápida, por ejemplo, de los ingresos versus egresos en una misma gráfica y comprobar si en realidad obtiene buenas ganancias o si sus egresos son tantos que casi alcanzan a esas ganancias, y en vista de esto elaborar estudios y tomar medidas al respecto.

En la educación: el surgimiento del microcomputador es de vital importancia en el área educativa, gracias a la disponibilidad de equipos a costos accesibles y la facilidad del manejo del mismo, actualmente están siendo muy utilizados en la casa, las escuelas, universidades, centros de enseñanzas y empresas. Debido a su capacidad para almacenar gran cantidad de datos, los computadores pueden ser usados como instrumentos de estudios y consulta de cualquier materia a cualquier nivel: otorgando al estudiante especial atención individual. La informática ofrece una gran cantidad de medios para lograr un aprendizaje eficaz como lo son el uso de gráficos, dibujos, caracteres de distintos formatos, color sonido. Superando las limitaciones de la enseñanza clásica la informática permite un dialogo dinámico hombre-máquina para adecuar este proceso a las necesidades particulares de cada persona de acuerdo a su velocidad de aprendizaje.

En la Navegación: en el área marítima los computadores controlan la fijación de posiciones o situaciones geográficas mediante satélites. En los puertos, una gran parte de las operaciones de carga y descarga se realizan de acuerdo a un programa establecido por el computador.

En la Aeronáutica: el computador realiza funciones tales como: controlar el tráfico aéreo, presentar la posición y altura de los aviones a través de las pantallas de radar, simular operaciones de vuelos especiales.

En la Ciencia: el computador es de gran ayuda para analizar los datos, almacenar y recuperar información, simplificar expresiones, controlar experimentos, identificar moléculas, medir áreas de figuras específicas, llevar información estadística de procesos, etcétera.

En el transporte urbano: hay sistemas que permiten controlar el servicio de autobuses, según la demanda del servicio, determinando nuevas rutas si no hay pasajero en espera.

En la industria: tareas tales como la soldadura por puntos en la carrocería de automóviles o la pintura de pistola, son ideales para los robots industriales.

En la vigilancia: los computadores ofrecen información instantánea acerca de automóviles robados, falsificación de documentos, valores y análisis de pruebas. En algunos países, los patrulleros de la policía están equipados con terminales y por teclado o micrófono se formulan las preguntas concernientes a algún hecho sospechoso, recibiendo la respuesta en segundos.

En el campo de la medicina: es posible hacer diagnósticos médicos, pudiendo detectar, por ejemplo, cuando el paciente ha sufrido un ataque cardíaco.

Automatización de oficinas: Puede ser definida como el concepto que envuelve la interacción de personas en una oficina que usa tecnología para alcanzar sus objetivos. La tecnología de la oficina involucra equipos como computadores, procesadores de palabras, impresoras, copiadoras, sistemas de telecomunicación, etc. Con estos equipos, las actividades de las oficinas tales como el procesamiento de datos, procesamiento de palabras, correo electrónico, gráficos, y computación personal son apoyados. Con el uso de sistemas automatizados, el personal de oficina está en mejor posición para contribuir a los objetivos de la organización.

La automatización de oficinas nos brindas algunas ventajas como:

- Ayuda al logro de los objetivos organizacionales: contribuye al esfuerzo de las personas que quieren lograr los objetivos empresariales.
- Incrementa la productividad: incrementa la producción de los trabajadores con relación a las horas trabajadas.
- Incremento en las ganancias: si la productividad aumenta, los gastos disminuyen, entonces incrementan las ganancias.
- Optimización del equipo de trabajo: la automatización mejora las capacidades humanas y compensa las limitaciones laborales.
- Mejora en la velocidad de la producción de la oficina: el tiempo para crear, procesar, almacenar y distribuir información es reducido.
- Mejora la calidad de la producción de la oficina: la información mejora su apariencia, exactitud y es suministrada a tiempo.
- Mejora la toma de decisiones: los gerentes reciben rápidamente información importante que puede reflejar alternativas para la solución a problemas.
- Mejora el control sobre el trabajo de oficina: los gerentes pueden tener información más detallada de la eficiencia del trabajador de oficina, frecuentemente evaluada por equipos computarizados.

- La conexión de sistemas de oficina: los usuarios pueden ser conectados con otros trabajadores para lograr una comunicación más eficiente.
- Mejora la calidad del ambiente de trabajo: el trabajo puede ser más interesante, satisfactorio debido a la eliminación de rutinas y tareas repetitivas.
- Provisión de nuevos servicios: la organización puede ofrecer a sus clientes nuevos servicios tales como la conexión a través de redes para agilizar las órdenes de entrada o para hacer seguimiento a sus órdenes.

Ahora bien, también tiene desventajas como:

- Naturaleza de la automatización de oficina: sin conocimiento del valor de la automatización de oficina, los gerentes pueden resistirse al cambio, lo que traduce en un mal uso de la tecnología, causando efectos contrarios a los diseñados.
- Justificación de los costos: muchos beneficios de la automatización de oficina son intangibles lo que hace difícil justificar los costos a la gerencia.
- Procedimientos organizacionales: nuevos sistemas tecnológicos frecuentemente desplazan procedimientos tradicionales.
- Personas: entrenamiento, despidos, pueden ocurrir cuando la automatización es implementada.
- Vendedores: incompatibilidad de equipos, obsolescencia de modelos, vendedores ineficientes hacen de la selección de equipos una tarea dura.
- Software: algunos paquetes son inapropiados, difíciles de aprender y necesitan muchas modificaciones para satisfacer las necesidades de la organización.
- Seguridad: como más miembros de la organización tienen acceso a los computadores, hay más acceso a archivos de la organización.
- Legalidad: el crecimiento del uso de computadoras presenta un incremento en las oportunidades de crimen basado en computadoras, tales como transferencia ilegal de fondos o robo de datos computarizados.

II.II) Hardware y software

a) Hardware

Es el elemento físico de un sistema informático, es decir, todos los materiales que lo componen, como la propia computadora, los dispositivos externos, los cables, los

soportes de la información y en definitiva todos aquellos elementos que tienen entidad física.[8]

Básicamente, el hardware son todos los componentes físicos de un dispositivo electrónico, lo tangible, lo que se puede tocar. Algunos ejemplos son: monitor, teclado, mouse, CPU, microprocesador, memoria RAM, disco duro, discos externos, pendrives, impresora, etcétera.

Los dispositivos utilizados en informática son innumerables, se crean y desechan a diario. Dentro de lo básico, los dispositivos internos de un ordenador:

- Unidad central de proceso (C.P.U.): es el verdadero cerebro de la computadora. Su misión consiste en controlar y coordinar o realizar todas las operaciones del sistema. Para ello extrae, una a una, las instrucciones del programa que se tiene alojado en la memoria central, las analiza y emite las órdenes necesarias para su completa realización. Físicamente está formado por circuitos de naturaleza electrónica que en una microcomputadora se encuentran integrados en una pastilla o chip denominada microprocesador. La Unidad Central de Proceso está compuesta por las dos siguientes unidades. La Unidad de Control o UC (de ella se controlan y gobiernan todas las operaciones como ser obtener una información de memoria principal, examinarla y codificarla) y La Unidad Aritmético Lógica o UAL (Esta unidad es la encargada de realizar las operaciones elementales de tipo aritmético y de tipo lógico(comparaciones).

- Memoria principal: La memoria central, principal o interna es la unidad donde están almacenadas las instrucciones y los datos necesarios para poder realizar un determinado proceso. Está constituida por multitud de celdas o posiciones de memoria, numeradas de forma consecutiva, capaces de retener, mientras la computadora esté conectada, a información depositada en ella. A la numeración de las celdas se denomina dirección de memoria y mediante esta dirección se puede acceder de forma directa a cualquiera de ellas, independientemente de su posición; se dice por ello, que la memoria central es un soporte de información de acceso directo. Además, el tiempo de acceso a la memoria central es notablemente inferior al necesario para acceder a las memorias auxiliares.

- Memoria RAM: Random Access Memory (memoria de acceso aleatorio). Es el almacenamiento primario interno. Puede acceder directamente cualquier punto aleatoriamente seleccionado en la misma cantidad de tiempo. La ventaja del almacenamiento

[8] Alcalde, Eduardo: *Informática Básica*, McGraw-Hill, Madrid, 1994, p.6.

de información electrónica es la capacidad de almacenar información en un punto conocido con precisión de la memoria y recuperarlo de esta misma posición con la consiguiente mejor performance en velocidad de acceso.

- Memoria ROM: (read-only memory), Chips de memoria con base a semiconductores que contienen instrucciones de programación. Estos chips pueden ser únicamente leídos, no pueden recibir información. Memoria de solo lectura. Es un dispositivo electrónico donde se almacena una información fija en forma binaria que ha sido grabada en el proceso de fabricación del circuito integrado. Es de sólo lectura y la información que contiene no se borra al perder el suministro de energía eléctrica. Es de acceso aleatorio. Se puede accesar en forma arbitraria a los bits almacenados en una dirección cualquiera. Se emplea para almacenar programas o rutinas standard de aplicación específica y su principal aplicación es, guardar los programas de arranque.
- Memoria Secundaria: son los dispositivos de almacenamiento masivo de información que se utilizan para guardar datos y programas en el tiempo para su posterior utilización. La característica principal de los soportes que manejan estos dispositivos es la de retener la información a lo largo del tiempo mientras se desee, recuperándola cuando sea requerida y sin que se pierda, aunque el dispositivo quede desconectado de la red eléctrica (disquetes, discos duros, discos ópticos, cintas, pen drives, etcétera).

b) Software

Es el conjunto de instrucciones detalladas que controlan la operación de un sistema de cómputo. Sin el software, el hardware de las computadoras no podría realizar las tareas que se asocian con las computadoras. Las funciones del software son:

1) Administrar los recursos de cómputo de la instrucción.

2) Proporcionar las herramientas a los seres humanos para que aprovechen estos recursos.

3) Actuar como intermediario entre las instituciones y la información almacenada.

Tipos principales de software:

• Software de Sistema: Sistema operativo. Es un conjunto de programas generalizados que administran los recursos de la computadora, como la CPU, los dispositivos de comunicaciones y los dispositivos periféricos. Coordina las distintas partes del sistema de cómputo y sirve como mediación entre el software de aplicación y el hardware de la computadora.

• Software de Aplicación: Se refieren a los programas que son escritos para o por usuarios para aplicar la computadora a una tarea específica. Se pueden citar los lenguajes de programación, controladores de sistemas externos, programas contables, programas de uso en medicina, etc.

• Software de Usuario: Tienen relación con programas que ayudan al usuario en sus tareas diarias como ser los programas de ofimática (Word, Excel, etc.), juegos, entretenimiento, antivirus, etc.

El sistema operativo (SO) es un programa de control principal almacenado en forma permanente en la memoria, que interpreta los comandos del usuario que solicita diversos servicios: visualización, impresión o copia de un archivo de datos, presenta una lista de todos los archivos existentes en un directorio o ejecuta un determinado programa. Las funciones del sistema operativo son:

- Administración de trabajos: el sistema operativo determina el orden en el que se procesan los programas y define la secuencia de ejecución de determinados trabajos. Se crea la cola de trabajo atendiendo a: trabajos que se procesan actualmente, cuáles recursos se están utilizando, qué recursos se van a necesitar, la prioridad de cada trabajo.
- Administración de recursos: establece una tabla en la que se relacionan los programas con los dispositivos que están trabajando o que se van a usar. El SO consulta esta tabla para aprobar o negar el empleo de un dispositivo específico.
- Control de operaciones: crea un directorio de los programas que se están ejecutando y de los dispositivos que necesitan para efectuar las operaciones. El SO identifica cada uno de los trabajos con un número que se le asigna cuando entra a la cola de trabajos.
- Recuperación de errores: el SO trata de señalar los errores y le avisa al usuario. Cancelará el procesamiento del programa erróneo lo sacará de la cola de trabajos y seguirá con el siguiente programa en la cola.
- Administración de memoria: el SO debe asignar eficientemente almacenamiento primario a las tareas que se están ejecutando dentro del sistema.

II.III) Redes informáticas

Consiste en la conexión de dos o más computadoras a través de uno o varios canales de transmisión (par trenzado, cable coaxial, fibra óptica, microondas, satélites y transmisión inalámbricos como ondas de alta y baja frecuencia de radio, o infrarrojos) con el

objeto de intercambiar datos, información o recursos. El Ingeniero Gustavo Vázquez (2022) definió los distintos canales de transmisión:

- Par trenzado: consiste en dos hilos conductores de cobre envueltos cada uno de ellos en un aislante y trenzado el uno alrededor del otro para evitar que se separen físicamente, y para conseguir una impedancia característica bien definida. Al trenzar los cables, se incrementa la inmunidad frente a interferencias electromagnéticas (interferencias y diafonía). La distancia de transmisión en redes de datos esta condicionada por el protocolo empleado. Desde el punto de vista de la seguridad, físicamente es muy seguro sin embargo en instalaciones criticas es conveniente su instalación dentro de caños metálicos.

- Cable coaxil: consiste en dos conductores cilíndricos concéntricos, entre los cuales se coloca generalmente algún tipo de material dieléctrico (polietileno, PVC). Lleva una cubierta protectora que lo aísla eléctricamente y de la humedad. Los dos conductores del coaxial se mantienen concéntricos mediante unos pequeños discos o el polietileno. La funcionalidad del conductor externo es hacer de pantalla para que el coaxial sea muy poco sensible a interferencias y a la diafonía. Se utilizan para transmisión de datos a alta velocidad a distancias de varios kilómetros, es decir, se cubren grandes distancias, con mayores velocidades de transmisión y ancho de banda que el par trenzado.

- Fibra óptica: es una fibra flexible, extremadamente fina, capaz de conducir energía óptica (luz). Para su construcción se pueden usar diversos tipos de cristal; las de mayor calidad son de sílice, con una disposición de capas concéntricas, donde se pueden distinguir tres partes básicas: núcleo, cubierta y revestimiento. El diámetro de la cubierta suele ser de centenas de µm (valor típico: 125 µm), el núcleo suele medir entre 2 y10 µm, mientras que el revestimiento es algo mayor: decenas de milímetros. Para darle mayor protección a la fibra se emplean fibras de Kevlar. La transmisión por fibra óptica se basa en la diferencia de índice de refracción entre el núcleo y la cubierta que tiene un índice de refracción menor. El núcleo transmite la luz y el cambio que experimenta el índice de refracción en la superficie de separación provoca la reflexión total de la luz, de forma que sólo abandona la fibra una mínima parte de la luz transmitida. Los núcleos de los cables de fibra óptica pueden ser de vidrio o de plástico (polímero). La fibra óptica con núcleo de plástico es más flexible y los conectores pueden adaptarse mejor sin necesidad de pulir los extremos o de utilizar resinas epóxicas. Un cable con núcleo de plástico no precisa elementos adicionales para alcanzar la rigidez que necesita, como tiras de Kevlar, por lo que es más barato que los de vidrio. La desventaja de los cables con núcleo de plástico es

que presentan una atenuación mucho mayor, lo que limita la longitud del enlace. Las fibras con núcleo de vidrio tipo monomodo requieren el desarrollo de empalmes por fusión para minimizar perdidas. En cuanto a las características de la fibra óptica, se pueden enumerar: la gran capacidad de transmisión, permitiendo elevados anchos de banda; la muy alta inmunidad al ruido eléctrico; el radio de curvatura de la instalación de los cables de fibra óptica es limitado, a fin de evitar interrumpir el haz; permite transmitir señales a grandes distancias; requiere dispositivos terminales activos para conectarse a las redes de datos (Media converters); emplea distinto tipo de conectores especiales; y, desde el punto de vista de la seguridad, constituye uno de los medios de transmisión más seguro.

- Radioenlaces terrestres: la transmisión está sujeta a los principios de la óptica, sufriendo los fenómenos de reflexión, refracción, difracción y absorción. A frecuencias más altas, la señal se propaga en forma más directa, restringiendo su alcance a la línea del horizonte. A mayores frecuencias, se puede disponer de un mayor ancho de banda de transmisión. Existen bandas de frecuencias licenciadas y no licenciadas. La asignación de frecuencias licenciadas está regulada por el ente fiscalizador de cada país. (ENACOM). Desde el punto de vista de la seguridad, la direccionalidad restringe las posibles escuchas y puede estar sujeto a interferencias.

- Enlaces satelitales: el satélite se comporta como un elemento repetidor ubicado a gran distancia de la tierra. Permite establecer enlaces de grandes distancias, posee latencia en las comunicaciones por la distancia entre el satélite y la tierra y emplea métodos de acceso al medio tendientes a ahorrar el ancho de banda. Normalmente, requieren de instalaciones centrales que poseen la inteligencia de la red (Hub) y estaciones terminales de pequeña amplitud que interconectan a los corresponsales (VSAT). La disponibilidad de satélites de comunicaciones en órbita y sus bandas de frecuencias, esta reglada por la UIT. Desde el punto de vista de la seguridad, es necesario el cifrado de los enlaces en razón que pueden estar sujetos a escuchas. Para enlaces críticos es conveniente la redundancia de los enlaces.

- Redes celulares: optimiza el empleo del espectro electromagnético a través del reúso de frecuencias y distintos métodos de acceso (Frecuencia - Tiempo - Código). La red se planifica sobre la base de su diseño en celdas. El tamaño de cada celda depende de la densidad de usuarios. El reúso de frecuencias entre distintas celdas puede generar interferencia cocanal. Las distintas generaciones de telefonía celular fueron ampliando su capacidad de servicios y el ancho de banda transmisión para los usuarios. Desde el punto

de vista de la seguridad los sistemas que acceden por CDMA son los más seguros. La transmisión de datos se realiza a través de los protocolos de Internet. La transmisión de datos es más segura que la transmisión por voz. Hoy, aún a través de los sistemas que operan por transmisión de datos pueden ser vulnerables, a través de procesos de clonación.

La importancia de las redes es que permiten unir la información, ya fragmentada en empresas muy computarizadas; compartir el uso de los recursos y el valor que agregan las redes a las organizaciones. De la información que maneja la red, depende en gran parte el progreso de la empresa. La comunicación con sucursales a través de la conexión de redes de computadoras permite obtener la información de las transacciones y operaciones que se realizan en las mismas.

La topología de redes es el cómo se conectan las máquinas para permitir que funcione la red. Los cuatro mayores tipos de topología son:

- Redes en Anillo (Ring): contiene computadores y dispositivos de computador ubicados en círculo. En este tipo de topología no hay un computador coordinador central. Los mensajes son enviados a lo largo del anillo de un computador o dispositivo a otro hasta llegar a destino. Constituye físicamente una red circular, donde cada terminal se conecta a dos nodos cercanos adyacentes. La transmisión es unidireccional alrededor del anillo y posee el sentido de transmisión de las gujas del reloj. Utiliza como medio de transmisión pares trenzados o fibra óptica. El mal funcionamiento de una estación de trabajo puede deshabilitar la red. No es muy flexible o escalable. Constituye una topología activa, ya que las estaciones de trabajo participan en la entrega de los datos. Los datos van de estación en estación y se detienen cuando arriban al destino.

- Redes Bus: es un cable o línea de telecomunicaciones con dispositivos conectados a este. Este tipo de redes es el más popular (Un ordenador envía datos a otro transmitiendo a través del bus la dirección del receptor y los datos). El medio físico de transmisión es el cable coaxil y todos los terminales de datos se conectan al cable coaxil. No intervienen dispositivos de conectividad, el canal de comunicaciones es compartido por todos los dispositivos y la señal viaja entre los dos extremos de la red. Utiliza un extremo puesto a tierra para evitar la estática. Velocidad de transmisión 10 Mbps (megabytes por segundo). Constituye una topología pasiva, los nodos escuchan y aceptan los datos que le corresponden. Usa el método de transmisión de broadcast.

- Redes jerárquicas: usa una estructura de árbol. Los mensajes son pasados a través de las ramas de la jerarquía hasta que llegan a su destino. Este tipo de topología no requiere de un computador central que controle la comunicación.
- Red estrella: este tipo de red tiene un computador central de donde salen líneas en las que se conectan otros computadores. El computador central controla y dirige los mensajes. Si esta falla, toda la red falla (los ordenadores están conectados con un elemento integrador llamado hub). Las computadoras de la red envían la dirección del receptor y los datos al hub, que conecta directamente los ordenadores emisor y receptor. Una red en estrella permite enviar simultáneamente múltiples mensajes, pero es más costosa porque emplea un dispositivo adicional -el hub- para dirigir los datos. Emplea como medio físico de transmisión el par trenzado o cableado de fibra óptica. Un solo cable conecta el dispositivo terminal con el dispositivo central. Posee una buena tolerancia a fallos. Es flexible en cuanto a su diseño y a la ampliación de terminales e interconexión de redes Estrella. Las redes Ethernet modernas están basadas en esta topología.
- Red Híbrida: es una combinación de una o más topologías.

Dependiendo de la distancia de las comunicaciones, las redes pueden ser clasificadas en:

- Red de área local o LAN (conecta computadores y dispositivos en una misma área geográfica, abarcan una distancia limitada, en general un edificio o varios próximos).
- Red de área amplia (WAN): son redes de largas distancias. En general pertenecientes a grandes compañías u organismos oficiales, abiertas a la comunicación de cualquier usuario que se conecte a ellas (normalmente mediante un contrato de alquiler, asignándosele un identificativo que le permite ser recibido el paquete es transformados en los mensajes y datos originales. Por su eficiencia, este tipo de red es usado por organizaciones con una alta necesidad de comunicación.

II.IV) Dirección IP, dominios y anonimato

IP es la abreviatura de Internet Protocol. Los protocolos de red son una descripción formal de un conjunto de reglas y convenciones que gobiernan el modo en que se comunican los dispositivos de una red. Son reglas comunes para que los equipos puedan enviar mensajes en un lenguaje entendido por quien recibe el mensaje. El modelo de referencia TCP/IP explica la posible comunicación de datos entre dos computadoras de cualquier parte del mundo. Es la unidad básica para la transferencia de datos, selección de rutas

(ruteo) y conjunto de reglas para la entrega de paquetes. Toma los datos del nivel superior (TCP o UDP) y los inserta en datagramas. Se basa en servicio no orientado a la conexión y no confiable (sin validación). No se garantiza que el datagrama llegue a destino. Es un servicio de entrega con el mejor esfuerzo (best effort). Los datagramas son independientes, no hay relación entre ellos y viajan por distintas redes (ethernet, fddi, frame relay, x.25, token ring, etcétera).

La versión IPv6 mantiene las buenas características del IPv4 y descarta las malas. No es compatible con IPv4, pero sí lo es con todos los demás protocolos de Internet. Tiene direcciones más grandes que IPv4 (16 Bytes de longitud), representa una cantidad ilimitada de direcciones. Simplifica la cabecera del datagrama (pasa de 13 campos IPv4 a 7 campos IPv6), lo que representa una mayor velocidad de procesamiento. Posee mayor apoyo a las opciones simplificando su uso para los routers y brinda mayor velocidad de procesamiento. Incrementa considerablemente la seguridad (autenticación y confidencialidad) y amplia la cantidad de servicios que puede atender atento a los servicios multimediales.

El Domain Name System (DNS) es el dominio (nombre) usado para identificar una red o sitio de Internet. Es un sistema de nombre de dominio que asocia un nombre con una dirección IP. Es un sistema organizado de servidores con bases de datos que permiten la asociación. Es jerárquico y distribuido. Desde el punto de vista de seguridad, puede ser vulnerado redireccionando la asociación hacia lugares maliciosos. DNSSEC modifica el protocolo para asegurar respuestas firmadas criptográficamente. La diferencia entre una URL (Uniform Resource Locator) y un nombre de dominio es que una URL puede ser http://www.example.net/index.html y un nombre de dominio www.example.net. Un nombre de dominio registrado puede ser example.net, mientras que la dirección IP es http://192.0.32.10.

Estructura jerárquica de dominios:

1. Raíz(.)

2. Dominios de nivel superior: Códigos Genéricos – Abiertos (.com, .net, .org, .biz, .info) –Restringidos (.edu, .gov, .mil, .int, .arpa, .museum, .aero). Códigos Territoriales Tradicionales (.ar, .br, .cl, .co, .do, .fr, .kr, .jp, .hn, .mx, .uk, .us) –Comerciales (.as, .cc, .la, .md, .nu, .sr, .to, .tv)

3. Dominio de Segundo nivel: Es la palabra "subdominio" sufijo de un nombre que se le va a dar a la dirección numérica (Facebook, Gmail, Hotmail).

4. Dominio de Tercer Nivel: Resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida.

El DNS tiene tres componentes:

Clientes: Programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (¿Qué dirección IP corresponde a nombre.dominio?).

Servidores DNS: Contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada. (100.56.24.12)

Zonas de autoridad: Parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. (subdominio.COM)

Los proveedores de servicios de internet (ISP) son los encargados de bridar el servicio de internet. La asignación de una conexión a internet implica darle una dirección de IP al cliente que la solicitó, a través de un módem conectado a un domicilio físico. Este tipo de IP es de real importancia en las investigaciones criminales, ya que el ISP tiene los datos del abonado de alguna IP relacionada con algún hecho cibercriminal.

Existen dos tipos de direcciones IP, la pública y la privada. La primera es la que tiene establecida cualquier dispositivo conectado a internet. Son siempre únicas y no se pueden repetir. La IP privada se utiliza para individualizar dispositivos dentro de una red privada o doméstica.

Anonimato

Lejos de hablar en lenguaje técnico, voy a exponer 2 formas de ocultar la dirección IP, maniobra que motiva a los delincuentes a ocultar su identidad y cometer ciberdelitos. Las direcciones IP se pueden ocultar con una VPN o con el navegador Tor, o bien ambas herramientas en simultáneo.

Una VPN (Virtual Private Network) es una red privada que usa una red pública (generalmente Internet) para conectar sitios o usuarios remotos de forma segura. Funciona ocultando la verdadera IP, redireccionando la red a un servidor remoto especial alojado por el proveedor de la VPN, cifrando los datos para que no se pueda interpretar la información, en caso de que alguien intercepte la comunicación. Disfraza la identidad en internet, estableciendo una conexión protegida. Funciona como un túnel entre el usuario e

internet. El ISP y otros terceros no pueden detectar este túnel. Una VPN ofrece garantizar que los datos se originen en la fuente de la que afirman venir, restringir el ingreso de usuarios no autorizados a la red con un control de acceso, confidencialidad que evita que cualquier persona lea o copie datos mientras viajan por Internet y la integridad de los datos, que garantiza que nadie manipule los datos mientras viajan por Internet

El navegador Tor funciona cifrando en capas la dirección IP y que el tráfico de red viaje a través de distintos servidores del mundo, antes de salir a internet. Es decir que, cuando se sale a internet con el navegador, el tráfico se reenvía y cifra tres veces. La red está comprendida por miles de servidores, ejecutados por voluntarios, conocidos como repetidores Tor. Este navegador es el utilizado para navegar por la darkweb. La darkweb es la parte de internet donde se realizan la mayoría de las operaciones ilegales, como la venta y compra de drogas, armas, sicarios, material de explotación infantil, datos personales o bancarios robados, información confidencial obtenida de hackeos a empresas u organismos, entre otras operaciones.

II.V) Seguridad en redes

Los requisitos de la seguridad de la información dentro de una organización han sufrido dos cambios principales en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información valiosa para la organización se proporcionaba fundamentalmente por medios físicos y administrativos. Como ejemplo del primer tipo de medios sirva el empleo de robustos archivadores con cerrojo de combinación para almacenar los documentos importantes. Un ejemplo del segundo es el uso de procedimientos de investigación del personal durante el proceso de contratación. Con la introducción de los computadores, se hizo evidente la necesidad de herramientas automáticas para proteger ficheros y otra información almacenada en el computador. Éste es especialmente el caso de los sistemas compartidos, como los sistemas multiusuario. Esta necesidad se acentúa en los sistemas a los que se pueda acceder desde redes de datos o redes de telefonía públicas. El término genérico del conjunto de herramientas diseñadas para proteger los datos y frustrar las actividades de los piratas de la computación es seguridad en computadores. El segundo cambio relevante que ha afectado a la seguridad es la introducción de sistemas distribuidos y la utilización de redes y servicios de comunicación para transportar datos entre terminales de usuario y computadores y de computador a computador. Las medidas de seguridad en red son

necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos. La tecnología esencial subyacente, virtualmente, en todas las aplicaciones de seguridad en redes y computadores es el cifrado. Se utilizan dos técnicas fundamentales: cifrado simétrico y cifrado de clave pública, también conocido como cifrado asimétrico.

William Stallings (2004) sostiene que las amenazas a la seguridad de la red se dividen en dos categorías: las amenazas pasivas, llamadas a veces escuchas, que suponen el intento de un atacante de obtener información relativa a una comunicación, y las amenazas activas, que suponen alguna modificación de los datos transmitidos o la creación de transmisiones falsas. Hasta ahora, la herramienta automática más importante para la seguridad en red y de las comunicaciones es el cifrado. En el cifrado simétrico, dos entidades comparten una sola clave de cifrado/descifrado. El principal reto del cifrado simétrico consiste en la distribución y protección de las claves. Un esquema de cifrado de clave pública admite el uso de dos claves, una para el cifrado y la otra para el descifrado. La parte que generó el par de claves mantiene privada una de ellas y difunde la otra. El cifrado simétrico y el de clave pública se suelen adoptar en aplicaciones de red seguras, donde no tengamos dudas de su seguridad. El cifrado simétrico se utiliza para cifrar los datos transmitidos, utilizando una clave de un solo uso o clave temporal de sesión. La capa de sockets segura (SSL), y el estándar de Internet posterior, conocido como capa de transporte segura (TLS), proporcionan servicios de seguridad para transacciones web. Una mejora en la seguridad empleada con IPv4 e IPv6, llamada IPSec, proporciona mecanismos de privacidad y autenticación.

La seguridad en computadores y en redes implica cuatro requisitos:

- Privacidad: se requiere que sólo entidades o sujetos autorizados puedan tener acceso a la información. Este tipo de acceso incluye la impresión, la visualización y otras formas de revelado, incluyendo el simple hecho de dar a conocer la existencia de un objeto.
- Integridad: se requiere que los datos sean modificados únicamente por personas autorizadas. La modificación incluye la escritura, la modificación, la modificación del estado, la supresión y la creación.
- Disponibilidad: se requiere que los datos estén disponibles para las partes autorizadas.

- Autenticidad: se requiere que un computador o servicio sea capaz de verificar la identidad de un usuario

Los ataques pasivos consisten en escuchas o monitorizaciones de las transmisiones. El objetivo del atacante es la de obtener la información que está siendo divulgada. La divulgación del contenido de un mensaje y el análisis de tráfico constituyen dos tipos de ataques pasivos. La divulgación del contenido de un mensaje se entiende fácilmente. Una conversación por teléfono o un mensaje de correo electrónico pueden contener información sensible o confidencial. Por ello, queremos imposibilitar que un atacante sepa el contenido de estas comunicaciones. Un segundo tipo de ataque pasivo, el análisis de tráfico, que es más sutil. Suponga que disponemos de un medio para enmascarar el contenido de los mensajes u otro tipo de tráfico de información, de forma que, aunque los oponentes capturasen el mensaje, no podrían extraer la información del mismo. La técnica más común para ocultar el contenido es el cifrado. Pero, incluso si utilizamos alguna protección criptográfica, el atacante podría, igualmente, observar el contenido de estos mensajes. El atacante podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información podría serle útil para averiguar la naturaleza de la comunicación que se está realizando. Los ataques pasivos son muy difíciles de detectar, ya que no suponen la alteración de los datos. Habitualmente, el tráfico de mensajes es enviado y recibido de forma supuestamente normal y ni el emisor ni el receptor son conscientes de que una persona externa haya leído los mensajes u analizado el tráfico de la red. Sin embargo, es factible impedir el éxito de estos ataques, usualmente mediante cifrado. De esta manera, el énfasis en la defensa contra estos ataques se centra en la prevención en lugar de en la detección.

Los ataques activos admiten alguna alteración del flujo de datos o la creación de flujos falsos. Los podemos clasificar en 4 categorías: enmascaramiento, retransmisión, modificación de mensajes y denegación de servicio. Un enmascaramiento tiene lugar cuando una entidad pretende ser otra entidad diferente. Un ataque por enmascaramiento normalmente incluye una de las otras formas de ataques activos. La retransmisión supone la captura pasiva de unidades de datos y su retransmisión posterior para producir un efecto no autorizado. La modificación de mensajes significa sencillamente que algún fragmento de un mensaje legítimo se modifica o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje con un significado «Permitir a Juan García leer el fichero confidencial de cuentas» se modifica para tener el significado

«Permitir a Alfredo Castaño leer el fichero confidencial de cuentas» La denegación de servicio impide o inhibe el normal uso o gestión de servicios de comunicación. Este ataque puede tener un objetivo específico. Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino concreto (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la interrupción de un servidor o de toda una red, bien deshabilitando el servidor o sobrecargándolo con mensajes con objeto de degradar su rendimiento. Los ataques activos presentan características opuestas a las de los ataques pasivos. Mientras que un ataque pasivo es difícil de detectar, existen medidas para impedir que tengan éxito. Por otro lado, es bastante difícil impedir ataques activos de forma absoluta, ya que para hacerlo se requeriría protección física permanente de todos los recursos y de todas las rutas de comunicación. En su lugar, la finalidad radica en detectarlos y recuperarse de cualquier obstáculo o demora causados por ellos. Ya que la detección tiene un efecto disuasorio, también puede contribuir a la prevención.

El cifrado simétrico, también denominado cifrado convencional o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los setenta. Innumerables individuos y grupos, desde Julio César, pasando por la fuerza alemana Uboat, hasta los actuales usuarios diplomáticos, militares y comerciales, han empleado el cifrado simétrico para la comunicación secreta. De los dos tipos de cifrado, es todavía el más utilizado. Un esquema de cifrado simétrico tiene cinco componentes:

- Texto nativo (plaintext): es el mensaje original o datos que se proporcionan como entrada del algoritmo.
- Algoritmo de cifrado: el algoritmo de cifrado lleva a cabo varias sustituciones y transformaciones sobre el texto nativo.
- Clave secreta: la clave secreta es también una entrada del algoritmo de cifrado. Las sustituciones y transformaciones concretas realizadas por el algoritmo dependen de la clave.
- Texto cifrado (ciphertext): es el mensaje alterado que se produce como salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- Algoritmo de descifrado: es el algoritmo de cifrado, pero ejecutado a la inversa. Toma como entradas el texto cifrado y la clave secreta y produce como salida el texto nativo original.

Existen dos requisitos para la utilización segura del cifrado simétrico:

1. Se necesita un algoritmo de cifrado fuerte. Como mínimo, es de desear que el algoritmo cumpla que, aunque un oponente conozca el algoritmo y tenga acceso a uno o más textos cifrados, sea incapaz de descifrar el texto o averiguar la clave. Este requisito se suele enunciar de una forma más estricta: el oponente debería ser incapaz de descifrar el texto o descubrir la clave incluso si él o ella tuviera varios textos cifrados junto a sus correspondientes textos originales.

2. El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, toda comunicación que utilice esta clave puede ser leída. Existen dos enfoques generales para atacar el esquema de cifrado simétrico. El primer ataque se conoce como criptoanálisis. Los ataques de criptoanálisis se basan en la naturaleza del algoritmo junto a algún posible conocimiento de las características generales del texto nativo o incluso de algunos pares de texto nativo y cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo concreto o deducir la clave que se esté utilizando. Si el ataque tiene éxito en la deducción de la clave, el efecto es catastrófico: todos los mensajes cifrados con esa clave, pasados y futuros, están comprometidos.

El segundo método, conocido como ataque por fuerza bruta, consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga una traducción inteligible de texto nativo. Con el uso de una masiva organización paralela de microprocesadores sería posible alcanzar tasas de procesamiento de varios órdenes de magnitud superiores.

El cifrado protege contra los ataques pasivos (escuchas). Proteger contra ataques activos (falsificación de datos y transacciones) constituye un requisito diferente. La protección contra tales ataques se conoce como autenticación de mensajes. Un mensaje, fichero, documento u otro conjunto de datos se dice estar autenticado cuando es genuino y proviene del origen pretendido. La autenticación de mensajes es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos son auténticos. Los dos aspectos importantes son verificar que el contenido del mensaje no se ha alterado y que el origen es auténtico. También podemos desear verificar la temporización de un mensaje (que no haya sido artificialmente retrasado y retransmitido) y verificar su secuencia relativa a los otros mensajes que se transmitan entre las dos partes. Es posible

llevar a cabo la autenticación simplemente mediante el uso del cifrado simétrico. Si suponemos que solamente el emisor y el receptor comparten una clave (que es lo que debe ocurrir), entonces solamente el emisor genuino sería capaz de cifrar un mensaje satisfactoriamente para el otro participante. Es más, si el mensaje incluye un código de detección de errores y un número de secuencia, se le asegura al receptor que no se han efectuado modificaciones y que la secuencia es la adecuada. Si el mensaje incluye también una marca de tiempo, el receptor tiene la seguridad de que el mensaje no se ha retrasado más de lo normalmente esperado en el tránsito por la red.

CAPÍTULO III: "INTRODUCCIÓN A LA CRIMINOLOGÍA"

III.I) La Criminología

La Criminología es una ciencia empírica e interdisciplinaria que se ocupa del estudio del crimen, de la persona del delincuente, la víctima y el control social del comportamiento delictivo, tratando de suministrar una información válida contrastada sobre la génesis, dinámica y variables principales del crimen -contemplado éste como un problema individual y como problema social-, así como de los programas de prevención eficaz del mismo y técnicas de intervención positivas en el delincuente. (Cuarezma Terán, S.J., 1996, p.297)

Antiguamente, se conocía a la Criminología como "el estudio del crimen", pero esa definición fue evolucionando y hoy está enfocada al fenómeno social de la criminalidad. Baratta (2004) sostiene que "En su origen, la criminología tiene como función específica, cognoscitiva y práctica, individualizar las causas de esta diversidad, los factores que determinan el comportamiento criminal, para combatirlos con una serie de medidas que tienden, sobre todo, a modificar al delincuente" (pp. 21-22). Hoy, es una ciencia multidisciplinaria, porque se nutre de ciencias como la Psicología, la Sociología, la Biología, la Antropología, el Derecho y la Criminalística. Hoy en día, luego de años de estudio y autores sobre las distintas escuelas criminológicas, se entiende a la Criminología como una ciencia que estudia al delito, a la víctima, al victimario y al entorno biopsicosocial. Esto es así, porque no es lo mismo una persona que nace con alguna discapacidad, que una persona totalmente sana (aspecto biológico); una persona que goza de total plenitud de sus facultades mentales, de una que desarrolla una enfermedad mental o traumas en la infancia (aspecto psicológico); o una persona que nace en una familia adinerada, de una

que nace en un barrio carenciado (aspecto social). También, algunos autores utilizan el término "control social".

Cabe hacer la distinción entre Criminología y Criminalística, que tanta confusión genera: La Criminalística es una ciencia multi e interdisciplinaria que se encarga de esclarecer hechos y previene que vuelvan a ocurrir. Decimos que esclarece hechos, ya sean delictivos o no, ya que un accidente automovilístico, un suicidio o una muerte accidental por inhalación de monóxido de carbono en época invernal, son algunos ejemplos de hechos que no son delitos y la Criminalística se encarga de esclarecerlos de igual manera y bajo los mismos procedimientos científicos. Mientras la Criminalística responde las preguntas de "cómo", "cuándo", "dónde", "quién" y "qué" mediante una investigación técnica experimental, la Criminología responde a la pregunta del "por qué" mediante una investigación lógica o intelectual. El "por qué" de las acciones significa el motivo, es decir, la motivación. La motivación es el motor que impulsa a alguien a hacer algo. Es anterior a la acción, porque primero viene el proceso mental de querer hacer eso. Es el porqué de la conducta. La motivación y la conducta son objetos de estudio de la Psicología.

Las escuelas criminológicas son diferentes corrientes de pensamiento que buscan entender y explicar el fenómeno del crimen desde diversas perspectivas. Las principales escuelas criminológicas se resumen en:

- *Clásica*: Nació en el siglo XVIII con filósofos como Jeremy Bentham y Cesare Beccaria. Se centra en la idea de libre albedrío y responsabilidad individual, abogando por penas proporcionales y predecibles para disuadir el crimen.
- *Positivista*: A finales del siglo XIX, Emile Durkheim y Cesare Lombroso fueron figuras clave. Se basa en la creencia de que factores biológicos, psicológicos y sociales influyen en la conducta delictiva. Busca identificar las causas subyacentes del crimen y aboga por intervenciones científicas y tratamientos.
- *Sociológica*: Se desarrolló en el siglo XX con figuras como Edwin Sutherland y Robert K. Merton. Examina cómo los factores sociales, como la desigualdad y la falta de oportunidades, contribuyen al crimen. Se enfoca en las estructuras sociales y en la relación entre individuos y sociedad.
- *Criminología crítica*: Surgió en la década de 1960 y cuestiona las estructuras de poder y la influencia del sistema legal en la creación y perpetuación de la criminalidad. Se centra en aspectos como la opresión, la desigualdad y la discriminación.

- *Control social*: Desarrollada por Travis Hirschi, se centra en los lazos sociales y la importancia del control social informal para prevenir el crimen. Propone que los vínculos afectivos y la integración social disminuyen la probabilidad de participar en conductas delictivas.
- *Etiquetamiento*: Esta escuela, influida por Howard Becker y Edwin Lemert, examina cómo las etiquetas sociales y las reacciones de la sociedad hacia los individuos pueden influir en la conducta delictiva. Se centra en el proceso de estigmatización y cómo afecta la identidad de las personas.
- *Cultural*: Se enfoca en cómo los valores, normas y subculturas influyen en el comportamiento delictivo. La teoría de la subcultura delincuente, por ejemplo, sugiere que ciertos grupos desarrollan normas y valores que favorecen la actividad criminal.

En la práctica, muchos criminólogos adoptan un enfoque interdisciplinario, combinando elementos de varias escuelas para obtener una comprensión más completa de la criminalidad. La criminología contemporánea tiende a incorporar múltiples perspectivas para abordar la complejidad de los factores que contribuyen al crimen. Cada una ofrece perspectivas únicas y aborda diferentes aspectos del crimen. La elección de la teoría o enfoque depende de la pregunta específica que se esté tratando de responder y de la complejidad del fenómeno delictivo en cuestión. La perspectiva dependerá de la naturaleza del problema de investigación y de la capacidad de la teoría para explicar y prever los fenómenos observados. Cada escuela criminológica aporta valiosas perspectivas, y la elección de la teoría adecuada dependerá de los objetivos específicos del estudio o del análisis. Si bien los criminólogos puedan llegar a tener una postura sobre alguna escuela, cabe destacar que este trabajo ilustra brevemente estas escuelas y que no se encasillará en un tipo en particular, sino que se adopta el enfoque multidisciplinario explicado anteriormente.

Un estudio multidisciplinario tiene importancia a la hora de investigar un delito, ya que varias disciplinas se centran en distintas cuestiones que están relacionadas. Si bien la Criminología castigaba al autor de un delito, el Derecho Penal castiga el acto en sí. En el Derecho Penal de Acto, el sistema legal se centra principalmente en el acto delictivo en sí mismo, es decir, en la conducta prohibida por la ley. La culpabilidad se atribuye al comportamiento ilegal y no necesariamente al individuo que lo lleva a cabo. La idea fundamental es que el derecho penal está diseñado para castigar acciones que la sociedad considera perjudiciales o inaceptables. En cambio, el Derecho Penal de Actor pone más

énfasis en la persona que comete el acto delictivo. La culpabilidad está vinculada directamente al autor del crimen, considerando sus intenciones, motivaciones y responsabilidad personal. Se busca castigar no solo la acción en sí, sino también al individuo que la realiza. En general, el derecho penal tiende a ser una combinación de ambos enfoques, pero la proporción puede variar según la jurisdicción y la filosofía legal predominante. En muchos sistemas legales, la responsabilidad penal se basa tanto en la acción como en la culpabilidad del individuo que realiza la acción. Es importante señalar que, en teoría, el derecho penal no debería castigar a una persona como tal, sino a la conducta delictiva que ha llevado a cabo. La responsabilidad penal implica demostrar que el individuo ha realizado conscientemente un acto prohibido por la ley y que es merecedor de sanción.

En este trabajo, los casos de estudio no tienen que ver con una marginalidad en sentido de barrios carenciados o de convivir con la delincuencia cruda en situación de calle, ya que estos delitos se suelen cometer dentro de una habitación, donde los variados objetivos van desde hacer plata fácil estafando gente, crear softwares maliciosos, utilizarlos, hasta neutralizar los servidores de una empresa. Por ello, podríamos abordar a la Cibercriminología desde una perspectiva de control social y cultural muy notoria. Las actividades que los chicos realizan en el ciberespacio son tan inmensas e innovadoras que los padres tienen un desconocimiento total de lo que sus hijos hacen con su celular o computadora. Esto genera que el control y la educación en materia digital sean prácticamente nula. Por más lazo social y familiar que el chico tenga, nunca sabrá qué está bien y qué está mal hacer con una computadora. De aquí nace la urgente necesidad de asignaturas en materia de ciberseguridad en la escuela primaria y secundaria. Por otro lado, desde el punto de vista cultural, el chico puede ir sumergiéndose más en el mundo de la informática profunda y/o en darkweb para mejorar sus aptitudes técnicas, y encontrarse con un mundo de chicos y chicas en su misma situación, creando lazos de amistad en el ciberespacio con ciberdelincuentes (actuales y futuros) de mismos intereses. La falta de control social y el sentido de pertenencia a un grupo podrían dar resultado a la criminogénesis de la ciberdelincuencia.

III.II) Criminogénesis de la delincuencia

Existe una multiplicidad de enfoques que intentan explicar el origen de la conducta criminal, que van desde la biología molecular hasta la antropología cultural, pasando por

la neurofisiología, la psicología y sociología. Cuanto más violento es el crimen, más intensas se vuelven las preguntas que tratan de lograr una explicación.

Según la "teoría de las actividades rutinarias" de Cohen y Felson[9], el origen de la conducta criminal se desencadena por la convergencia ocasional de tres elementos: un delincuente motivado, una víctima accesible y la ausencia de elementos de protección. De esta teoría nace el "triángulo del delito" que Fernando Miró Llinares utiliza para adaptarlo al entorno ciber en su libro "El Cibercrimen" en 2012[10].

Los sociólogos Gottfredson y Hirschi, en su teoría general de la Delincuencia[11], plantean que la pieza clave que explica la conducta delictiva radica en el grado de autocontrol de los individuos y cómo ello se vincula a la toma de decisión de cometer un delito.

David Farrington[12], profesor del Instituto de Criminología de Cambridge, plantea que el origen se encuentra en el período antisocial entre los 14 y 20 años en jóvenes de clase baja que fracasan en la escuela. Lipsey y Derzon, en un estudio de 1997[13], plantearon que el mejor predictor de delitos graves consistía en identificación de conductas transgresoras a edades muy tempranas.

Ningún genetista encontró una relación causal directa entre algún gen y comportamiento antisocial, pero es evidente que los genes codifican proteínas que dirigen en buena parte el diseño de nuestro sistema nervioso y endócrino que constituyen nuestro organismo, y cómo responde éste en su sensibilidad e intensidad de los estímulos (temperamento).

A su vez, nadie duda que ese organismo se desarrolla en un entorno de múltiples y complejas influencias familiares, sociales, culturales (experiencias de aprendizaje) y cómo interactúan, determinándose recíprocamente con las variables biológicas.

[9] Cohen, Lawrence E. Y Felson, Marcus: "Social change and crime rate trends: A rutine activity approach", en *American Sociological Review*, Vol. 44, Urbana, agosto 1979, pp. 588-608.
[10] Miró Llinares, Fernando: *El cibercrimen*, Marcial Pons, Madrid, 2012, pp. 168-170.
[11] Gottfredson, M. y Hirschi, T.: *A general theory of crime*. Stanford University Press, California, 1990.
[12] Farrington, David: "Childhood origins of antisocial behavior" en *Clinical Psychology & Psychotherapy*, 12. Cambridge, 2005, pp. 177-190.
[13] Lipsey, Mark W. y James H. Derzon: "Predictors of violent or serious delinquency in adolescence and early adulthood", en *Serious and Violent Juvenile Offenders: Risk Factors and Successful Interventions* (Edit. Loeber y Farrington). Sage Publications, Thousand Oaks, California, 1998, pp. 86-105.

III.III) Perfilación Criminal

Disciplina de la Criminología que emplea técnicas y métodos para determinar los posibles perfiles (rasgos) psicológicos de los criminales. Delimita las características probables del presunto autor del hecho para disminuir el rango de posibles culpables y ayudar a quienes llevan a cargo la causa. Es un estudio probabilístico.

Establece patrones de conducta en base al análisis de la escena del crimen, del estudio de la víctima y en análisis de datos policiales, para realizar una estimación acerca de las características biográficas, psicológicas y del estilo de vida de un criminal o de una serie de crímenes graves y que aún no ha sido identificado.

No es una ciencia exacta, ya que se trata de un estudio en donde no contamos con la presencia física del sujeto para aplicarle el proceso psicodiagnóstico. Parte de indicios o de actos delictivos ya consumados, más la información de diversas fuentes y deducir la personalidad del criminal para llegar a su individualización.

Existen 3 técnicas de perfilación: Perfil de agresores conocidos o Método Inductivo, Perfil de agresores desconocidos o Método Deductivo y Mixta, que es una técnica que integra las 2 anteriores. Veamos las 2 primeras:

Perfil de agresores conocidos o Método Inductivo: Parte de premisas particulares para arribar a conclusiones generales. Si hay un sospechoso, se lo evaluará y se determinará si hay coincidencia entre el perfil de éste con el "perfil típico o general" de otros criminales que han cometido delitos similares al que se le imputa. La información partió de entrevistas con criminales y análisis de casos.

El Crime Classification Manual (Manual de Clasificación Criminal, en 1992)[14] describe los perfiles psicológicos de los distintos tipos de criminales. Creado por Robert Ressler y John Douglas, miembros de la Unidad de Ciencias de la Conducta del FBI. Fueron los primeros en utilizar el término "serial killer" (asesino serial).

Perfil de agresores desconocidos o Método Deductivo: El método deductivo consiste en partir de premisas generales para arribar a conclusiones particulares. Se tienen en cuenta los datos aportados por el método inductivo. Se utiliza cuando se desconoce el autor de un determinado delito o un crimen, y no hay ningún sospechoso detectado. Las reflexiones sobre el perfil del criminal dependerán de la interpretación correcta de la sumatoria de informaciones parciales dejadas en la escena del crimen, más los aportes

[14] Douglas Je., Burgess Ag. y Ressler R.: *Crime Classification Manual*, Lexington Books, Lexington, 1992.

policiales. Se evalúa el contexto del escenario, el tipo de violencia ejercida, la disposición de las cosas, modus operandi, la zona geográfica y la víctima. Esto nos dará un patrón de personalidad.

III.IV) Victimología

La Corte Interamericana de Derechos Humanos, en un artículo realizado por Sergio I. Cuarezma Terá (1996) sostiene que el estudio de la víctima tiene su origen en el positivismo criminológico, que inicialmente concentró la explicación científica del comportamiento criminal alrededor del delincuente, ignorando en gran parte a la víctima, considerándola como un objeto indiferente, pasivo, estático, que nada aporta a la génesis, dinámica y control del hecho criminal. En este sentido Hassemer, expresa que "desde los más diversos ámbitos del saber se ha llamado la atención sobre el desmedido protagonismo del delincuente y el correlativo abandono de la víctima, se ha dedicado exclusivamente a la persona del delincuente todos los esfuerzos de elaboración científica, tiempo, dinero, hipótesis, investigaciones sin preocuparse apenas de la víctima de los delitos."[15]

La victimología fue la parte de la Criminología que se encargaba de estudiar a la víctima, pero, hace algunos años, se separó y se empezó a estudiar a parte y más en profundidad. Cuarezma Terán (1996) sostiene que “el estudio sobre las víctimas fue adquiriendo un progresivo interés, hasta conformar una nueva disciplina científica” (p. 302). La victimología como disciplina nace en respuesta a que tanto el Derecho, como la Criminología e incluso la Psicología Forense, se habían centrado solamente en el agresor o delincuente, sin prestarle atención a la parte que sufrió el delito. De allí, nace esta disciplina de la Criminología que tiene por objeto el estudio de la víctima de un delito, de su personalidad, de sus características biológicas, psicológicas, morales, sociales y culturales, de sus relaciones con el delincuente y del papel que ha desempeñado en la génesis del delito.

La victimología ha evolucionado a lo largo del tiempo, y se suele hacer una distinción entre la "victimología vieja" y la "victimología nueva" (Cuarezma Terán, 1996) para destacar las diferencias en sus enfoques y perspectivas. La victimología tradicional solía ver ca la víctima como un sujeto pasivo, enfocándose más en el comportamiento del delincuente que en las experiencias y necesidades de la víctima. Se centraba principalmente

[15] Citado por García Pablos de Molina, en: Manual de Criminología, 1988, pág. 43

en las víctimas de delitos violentos, como asaltos, homicidios y agresiones sexuales; y la atención se dirigía a la victimización secundaria, es decir, el sufrimiento adicional que la víctima podría experimentar durante el proceso legal y social, como la revictimización en el sistema de justicia. La victimología moderna reconoce la importancia de comprender la experiencia de la víctima y su impacto psicológico, emocional y social; se ha expandido para incluir una variedad de víctimas, no solo de delitos violentos, sino también de delitos económicos, ambientales y de derechos humanos; considera la posibilidad de que una persona pueda experimentar múltiples formas de victimización a lo largo de su vida, reconociendo la complejidad de las interacciones delictivas; se centra en la prevención del crimen y la promoción de la justicia restaurativa; y tiende a adoptar un enfoque multidisciplinario, integrando elementos de la criminología, la psicología, el trabajo social y otras disciplinas.

Cuarezma Terán (1996) sostiene que:

El surgimiento de esta nueva Victimología obedece a la justificación de una política de "ley y orden" y a la mayor rentabilidad de satisfacer a las víctimas que a los delincuentes, así como a la necesidad de establecer un contrapeso a la criminología crítica que, en su análisis, parecía eximir implícitamente al delincuente de la responsabilidad. (p. 305)

III.V) El sistema penal

El Dr. Raúl Zaffaroni en su Manual de Derecho Penal[16], dice que "El sistema penal es el conjunto de agencias que coinciden en la cuestión criminal. Algunas son exclusivamente penales (policías, servicio penitenciario, tribunales penales, órganos políticos de interior, seguridad, inteligencia, etc.). Otras, participan del poder punitivo, pero sus funciones son más amplias, como: las agencias políticas (ejecutivos, legislativos); las agencias de reproducción ideológica (universidades. facultades, academias); las cooperaciones internacionales (agencias de países acreedores que financian programas en países deudores); los organismos internacionales que organizan programas, conferencias, seminarios. etc. (ONU, OEA, etc.); y, por supuesto, el gran aparato de propaganda sin el que no podría subsistir, o sea, las agencias de comunicación masiva (de prensa, radio, televisión, etc.)."

[16] Zaffaroni, E. R., Alagia, A. y Slokar, A.: *Manual De Derecho Penal: Parte General*, Ediar, Buenos Aires, 2006, pp. 9-10.

Zaffaroni hace hincapié en que cada agencia funciona con intereses pertinentes a sus funciones, sin importarle mucho lo que sucede en las demás agencias. Es por ello por lo que se genera una criminalización a partir del poder punitivo ejercido por el Estado. Es más, en este manual, Zaffaroni dice "No es extraño que este sistema funcione como una empresa organizada por niños traviesos...", haciendo alusión en que el sistema penal funciona por una lucha contra el poder sobre las personas, en vez de trabajar sobre la integridad de ellas.

También, habla sobre los estereotipos criminales, que son prejuicios (racistas, clasistas, xenófobos, sexistas) que van configurando una fisionomía del delincuente en el imaginario colectivo, que es alimentado por los medios de comunicación, y que quienes padezcan algún rasgo de esos estereotipos corren riesgo de ser criminalizados, aunque no hayan cometido ningún delito. Por ejemplo, la gente de piel morena o negra, los que viven en la villa, los indigentes, etc.

Básicamente, la idea de ilustrar el sistema penal por Zaffaroni en el capítulo de Criminología nace por la necesidad de demostrar que existen causas en las que el Estado mismo es parte de cierta injusticia para algunas personas, que pueden causar cierta marginalidad y una mayor tasa de delincuencia en personas que no tengan la necesidad de delinquir.

El sociólogo Edward A. Ross (1866-1951), fue autor, en 1901, del libro Control Social, una expresión que asumiría gran triunfo en la Sociología, en la Criminología y en el Derecho Penal. La concepción de control social de Ross tuvo un significado clave, que remite a las ideas comunitarias antes que a las estatales. El control hacia los demás a través de la vergüenza y la censura resultaba mucho más seguro que las diferentes maneras experimentadas por el Estado. Tal distinción positivista sería especialmente significativa en las nuevas sociedades de masas de la ciudad, que es donde pretenderían introducir sistemas de relaciones que conservaran una alianza armoniosa y no violenta.

No sólo la investigación sociológica, teórica y materialista, ha ayudado al estudio del carácter truncado del derecho penal y de los aparatos selectivos del sistema, sino también un estudio de la relación entre derecho penal y desigualdad lleva a alterar el modo como los términos de ella aparecen en el plano. Es decir, no sólo las normas del derecho penal se establecen y se utilizan selectivamente, reflejando las relaciones de desigualdad existentes, sino que el derecho penal practica también una función activa, de reproducción y de producción, de las relaciones de desigualdad. Por un lado, la aplicación de las

sanciones penales estigmatizantes (en espacial, las de cárcel) son selectivas. Influyen negativamente sobre todo en el estatus social de las personas que pertenecen a las capas sociales más bajas. Esta aplicación selectiva ejerce de modo de problematizar y obstruir su ascenso social. Por otro lado, el hecho de penar ciertas conductas ilegales sirve para resguardar un número más ancho de conductas ilegales que subsisten exentas al proceso de criminalización. De esa forma, la aplicación selectiva del derecho penal tiene como resultado contiguo la tapadera ideológica de esta propia selectividad.

III.VII) Delitos informáticos

> El Código Penal argentino, en su versión vigente, fue elaborado a comienzos del siglo pasado y aprobado en la década del veinte. No es de extrañar, entonces, que los bienes jurídicos que ampara respondan a otra era tecnológica. La redacción de los tipos penales también intenta captar otra tecnología. A modo de ejemplo, en los tiempos de Google y Facebook, el art. 153, Cód. Penal, se refería al "despacho telegráfico o telefónico". El hurto del art. 162, Cód. Penal, era sólo de cosas muebles (aún sigue redactado igual). Lo mismo sucedía con el delito de daño. La estafa recaía únicamente sobre personas y no sobre máquinas (Palazzi, Pablo A. 2016, p.11).

Con esta introducción de Pablo Palazzi, entendemos que hablar de delitos informáticos es, básicamente, tratar de encuadrar acciones contemporáneas a tipos penales antiguos. Aunque en 2008 se sancionó en Argentina la Ley 26.388 de delitos informáticos, que ayudaba a tipificar y a adaptar nuevas acciones maliciosas en el ciberespacio, hoy, a 16 años más tarde, queda un poco obsoleta. Aún, tenemos acciones maliciosas que no están tipificadas y, por ende, no son delitos. Además, hay que tener en cuenta que, mientras la tecnología avanza (y no las leyes), la magnitud de los daños será mayor, así como también la facilidad para cometer los ciberdelitos en cualquier parte del mundo y, por ende, las investigaciones serán más difíciles. Ni hablar si nombramos a las criptomonedas.

Se define al delito como una acción típica antijurídica y culpable. Básicamente, la acción es la conducta humana que genera un resultado; es típica porque está tipificada (escrita) en el Código Penal; antijurídica, porque la acción debe ser en contra de la ley; y culpable por tener una pena o sanción. Los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros

dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o que tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos. Son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas atípicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento (medio) o como fin (concepto típico). Como medio será cuando el delito tiene repercusiones en el plano físico. Delitos contra la integridad sexual (grooming) o la pérdida de patrimonio (estafas informáticas) son ejemplos de la informática como herramienta media para cometer el delito, también conocidos como delitos informáticos impropios. Como fin o delitos informáticos propios serán cuando el objetivo es hacia computadoras, dispositivos electrónicos, servidores (hacking, daño Informático, inutilización de un sistema).

Por otro lado, Pablo Palazzi (2019) dice que:

> Se pueden considerar dos categorías: los delitos netamente informáticos o propios que constituyen todas las acciones típicas que, cometidas mediante el uso de un dispositivo informático, recaen sobre los sistemas informáticos, es decir, hechos ilícitos que afectan: a) la operatividad y el normal funcionamiento de un sistema informático; y b) las comunicaciones electrónicas o digitales y los datos informáticos que atentan contra la integridad, confidencialidad y disponibilidad de esas comunicaciones o datos informáticos; y los delitos informáticos impropios son delitos informáticos en un sentido más genérico porque el accionar disvalioso se consuma a través de un dispositivo electrónico conectado a Internet que, en definitiva, involucra la utilización de un medio informático para fines delictivos. En esta categoría se incluyen aquellas conductas típicas que preveía el código penal antes de la incorporación de la Ley N.º 26.388 y que requieren técnicas poco sofisticadas. (p.188)

Saín (2018) afirma que existen dos grandes grupos de delitos informáticos. Aquellos que requieren de conocimientos técnicos avanzados para su comisión, como la elaboración de programas maliciosos desarrollados por hackers que buscan atacar dispositivos o redes; y aquellos delitos que “adquieren una nueva vida en la nube y son intermediados por servicios y aplicaciones web como las amenazas, los fraudes, el grooming” y que muchos de ellos se comenten mediante la ingeniería social y la suplantación de identidad (p.11).

Marcelo Riquert (2011) sostiene que se opta por hablar de "delincuencia o criminalidad informática", como suerte de categoría criminológica, y que de lo que se trata es de la aparición de nuevos modos de agresión, pero no de nuevos delitos. En mi opinión, sí es cierto, pero para algunas figuras. En otras, no. Así como existen los delitos de homicidio y de lesiones por separado, no podemos encuadrar la utilización de un troyano spyware, un wiper, un virus o un ataque DoSS en un tipo penal no informático. ¿Y Stuxnet? Sí estoy de acuerdo con figuras como el abuso sexual. Si bien el objetivo de la ley de grooming fue evitar el abuso sexual presencial, no logró que niños y niñas dejen de ser abusados, sino todo lo contrario. Los casos de grooming aumentaron frente a una nueva modalidad de abuso sexual virtual.

Saín (2012) sostiene que, desde un punto de vista criminológico, existen dos enfoques para analizar este "nuevo" fenómeno criminal, y que ambos enfoques son válidos. El primero de ellos es que los delitos informáticos son delitos convencionales que utilizan a la informática como medio para cometer el delito, como por ejemplo una amenaza que se efectúa por medios electrónicos. La segunda perspectiva afirma que las tecnologías de la información y comunicación brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución malwares, ataques a sitios web y la ciberpiratería.

En cuanto a la materia legislativa, en el año 2000 se sanciona la Ley 25.390 que aprueba el Estatuto de Roma, que recién se implementa en el 2007, con la Ley 26.200. Este Estatuto crea una Corte Penal Internacional que la faculta para ejercer su jurisdicción sobre "personas respecto de los crímenes más graves de trascendencia internacional". El Estatuto encuadra a estos crímenes el crimen de genocidio, los crímenes de lesa humanidad, los crímenes de guerra y el crimen de agresión, de un país a otro. Si bien el Estatuto de Roma no amplía su jurisdicción al ciberespacio y no tiene artículos dedicados al crimen informático, las operaciones en el ciberespacio relacionadas con la ciberguerra o que encajen en algún tipo penal nombrado, podrían ser investigados por la Corte Penal Internacional, teniendo en cuenta la magnitud que podría causar un ciberataque a una infraestructura crítica.

En el año 2008, se sanciona la Ley 26.388 de Delitos Informáticos, la cual no constituye una ley especial, sino que modifica, sustituye, o incorpora tipos penales al texto del Código Penal de la Nación Argentina. Mantiene sin modificaciones sustanciales el esquema de márgenes punitivos de los delitos ya previstos. Incorpora a las nuevas tecnologías como formas comisivas de los delitos.

Por otra parte, en el 2017 se aprueba el Convenio Sobre Ciberdelito del Consejo De Europa, adoptado en la Ciudad de Budapest, Hungría (conocido como el "Convenio de Budapest"), el 23 de noviembre de 2001. El Convenio de Budapest es la primera herramienta internacional que trata de manera concreta aspectos afines con el cibercrimen, a nivel de cooperación internacional relacionada con la investigación penal y procesal con evidencia digital, es decir, con la recolección, obtención y el tratamiento de la prueba digital. Frente a la ausencia de normativa específica se han desarrollado protocolos o reglas de buenas prácticas. Entre las más importantes a nivel internacional se encuentra la ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence y la ISO/IEC 27042:2015 Information technology -- Security Techniques -- Guidelines for the Analysis and Interpretation of Digital Evidence. A pesar de que no son obligatorias suelen ser seguidas por diversas fuerzas encargadas de recolectar prueba digital.

Si bien el análisis de las terminologías delito/crimen informático o cibercrimen lo desarrollo en el apartado sobre Cibercrimen, cabe destacar el texto de Gustavo Saín (2015) donde dice:

> El cibercrimen no es cometido únicamente por hackers o personas con altos conocimientos en informática y sistemas en la actualidad. Cualquier usuario de computadoras e Internet puede cometer un crimen informático en la actualidad. Asimismo los delitos informáticos en su generalidad no pueden considerarse como parte del crimen organizado, ya que los mismos no se cometen en su mayoría por varias personas que actúan concertadamente ni insume una complejidad propia de este tipo de ilícitos. Si bien el cibercrimen surge como un tipo de delito ocupacional de tipo profesional más que como un delito de cuello blanco, esa definición queda obsoleta en la actualidad a la luz de los avances tecnológicos y el uso masivo y cotidiano de Internet a nivel global. Por último, los delitos informáticos no establecen un tipo de criminalidad específica con características particulares, sino que adquieren ese nombre a partir del rol que ocupa la tecnología en la comisión de hechos ilícitos, tanto como medio para llegar al delito en sí como también fin o blanco del delito mismo.

A continuación, se detallarán las modificaciones mencionadas de los delitos tipificados en el Código Penal de la Nación, la incorporación de nuevos vocablos tecnológicos y se comentará cada artículo según mi propio análisis.

Ley 26.388 de Delitos Informáticos

No constituye una ley especial, sino que modifica, sustituye, o incorpora tipos penales al texto del Código Penal. Mantiene sin modificaciones sustanciales el esquema de márgenes punitivos de los delitos ya previstos. Incorpora a las nuevas tecnologías como formas comisivas de los delitos. Se destaca seguidamente algunas de las modificaciones relacionadas delitos ya planteados en el código y la incorporación de nuevos vocablos tecnológicos (se hace referencia a los artículos del Código Penal de la Nación).

Material de abuso sexual contra las infancias ("pornografía infantil")

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.

Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

Tal como expresa el Código Penal, el artículo 128 castiga la producción, distribución, facilitación, comercialización, divulgación y/o tenencia de material de explotación sexual infantil. Cabe aclarar que la tenencia simple es penada desde el 2018. Antes, la tenencia de material de abuso sexual contra las infancias no era delito, salvo que constituya un inequívoco indicio de comercialización (por ejemplo, la tenencia de varios CD's con contenido).

Daniela Duput (2018) define a la situación como “incontrolable”. La realidad es que hablar de este tema requiere de varias páginas, y no podría cumplir con los requisitos de este trabajo. La problemática con la mal llamada “pornografía infantil” pareciera no tener freno. Como investigador del cibercrimen, basta con navegar en internet por las redes sociales. Hoy en día, existen muchas mujeres menores que utilizan las redes sociales para venden contenido pornográfico. Es para reflexionar, porque, más allá de un supuesto problema económico que pueda tener su familia para que la menor se “prostituya”, hay una clara ausencia total del control y educación familiar. Por otro lado, si hay venta, hay alguien que compra. Ese comprador, si es mayor, incurriría en el delito por tenencia. Lo que más indignación nos genera, es que estas mujeres encuentran la manera para que Instagram no identifique la venta de material pornográfico, ni siquiera reportando la cuenta. La práctica más común es cambiar letras o tacharlas, para que Instagram no pueda leer las palabras “venta” y “contenido” (por ejemplo, escriben “v3nt4 de c0nt3nid0”. Hay una falta muy grave por parte de la red social de Meta al utilizar sólo inteligencia artificial para evaluar los reportes, sin la intervención humana. Cabe destacar que el eje de este análisis no es encasillar a las mujeres como sujetos activos del delito, ya que, por su condición de menores, serían inimputables; sino reflexionar sobre una enorme problemática social que va más allá del Derecho Penal.

Para terminar con este artículo, es importante hacer hincapié en la terminología. Quienes nos dedicamos a la prevención, militamos por la erradicación del término “pornografía infantil”, ya que la pornografía no tiene nada de infantil. Ese video o esa foto de un menor de edad en representaciones sexuales es la clara evidencia de un abuso sexual. Ahora bien, en el supuesto caso del párrafo anterior, ¿sería correcto decirle “pornografía infantil”? ¿Cómo debería llamarse?

Grooming

Ley de Grooming (26.904/2013) incorpora el art. 131 CP: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

El grooming, al ser un delito tan grave para los niños, niños y adolescentes, se analizará más adelante en este trabajo; pero cabe destacar que también es una

problemática que pareciera no tener freno. En realidad, la ley de grooming nace como cierta manera de prevenir la antesala al abuso sexual físico presencial, cuando los abusadores contactan a sus víctimas por medios informáticos y logran tener un encuentro físico con ellas. El problema radica en que esta figura penal pareciera no lograr ponerles freno a los pederastas digitales. Si bien se ha logrado bajar el número de casos de abuso sexual presencial con grooming como antesala, hoy en día existe muchísimo más grooming solo en internet y no hay muchas denuncias, ya que no sólo suelen ser casos aislados, donde el groomer busca una gratificación sexual personal y momentánea, sino que la víctima no sabe que es víctima ni se siente como tal. Esto es, en parte, por la creciente práctica de sexting entre menores de edad. El sexting es la producción y envío de material pornográfico de manera consensuada por los participantes. Muchos menores de edad (sobre todo adolescentes) están en búsqueda de esta práctica, sin importar mucho quién está del otro lado de la pantalla. Muchas veces, no les interesa preguntar edad ni verificar la identidad de la otra persona, a la hora de chatear con alguien e intercambiar material. Cabe destacar que esta práctica es sumamente peligrosa para la difusión de ese contenido.

Por último, cierro este delito con una frase de Daniela Dupuy (2018) sobre la tenencia simple de pornografía infantil: "no es lo mismo tener material de pornografía infantil que tener estupefacientes para consumo propio. Quien decide consumir drogas, afecta su propia salud; quien consume pornografía infantil, afecta la integridad sexual de los niños" (p.97).

Comunicaciones Electrónicas

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra

naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Los artículos 153 y 155 fueron modificados para actualizar e incorporar las figuras informáticas de las comunicaciones, con relación a las "antiguas" comunicaciones (cartas, pliegos cerrados, despachos telegráficos y comunicación telefónica). Con esta nueva salvedad, el Derecho Penal puede entender este delito en múltiples plataformas donde se pueda llevar a cabo, como correos electrónicos, conversaciones de WhatsApp, Instagram, Facebook o por cualquier otra red social o comunicación privada por internet.

Hacking

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese a un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Se crea el artículo 153 bis, que pena el hacking no ético, con fines maliciosos. Tengamos en cuenta que el hacking es un conjunto de técnicas utilizadas para acceder a un sistema informático, vulnerando las medidas de seguridad de este. Cabe aclarar que un hacker es un profesional de la informática y, por sí solo, no puede ser considerado cibercriminal. Un hacker será un cibercriminal, cuando la finalidad sea ilegal (conocidos como hackers de "sombrero negro").

Ahora bien, el Derecho Penal deja en claro que la acción típica es el acceso a un sistema informático "sin autorización o excediendo la que se posea". Esto significa que no sólo puede llevarse a cabo a través de herramientas informáticas (malwares, man in the middle, exploits), sino también entrando en el Facebook de una persona, sin que sepa o simplemente desbloqueando el teléfono de otra persona, sin su autorización. También, por fuerza bruta (adivinando contraseñas).

Base de Datos

Artículo 157 bis CP: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Se crea el artículo 157 bis. Si bien este artículo tiene cierta relación con el 153 bis (porque no deja de ser una técnica de hacking y acceder a un sistema informático), el hecho de que esté enfocado sólo en bases de datos hace la diferencia y podríamos entender a la inyección SQL como técnica maliciosa para llevar a cabo este delito.

Estafa Informática

Artículo 172 CP: Será reprimido con prisión de un mes a seis años, el que defraudare a otro (...)

Artículo 173 CP (Defraudaciones especiales) - Se agrega el Inciso 16: El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Con este nuevo inciso, el Derecho Penal da la oportunidad de penar cualquier acción de estafa mediante internet, como engaños, simulaciones, estafas de inversión, piramidales, de lotería, ventas online defraudatorias, ofertas fraudulentas, cualquier técnica de ingeniería social (cuento del tío, phishing, vishing, smishing) y suplantación de identidad (sin figura penal) que robe el patrimonio de la víctima. También, se entiende la utilización de malwares utilizados para robar información financiera, como los troyanos bancarios o los spywares (en concurso real con el delito de daño o sabotaje informático).

Daño y Sabotaje

Artículo 183 (párrafo agregado): “En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.”

Como segundo párrafo del artículo 183, y con su misma pena (15 días a 1 año de prisión) se agrega la alteración, inutilización o destrucción de datos, documentos,

programas o sistemas informáticos. También se establece la venta, distribución o introducción en un sistema informático de cualquier programa destinado a causar daños (virus, gusanos, troyanos, etc.). En el art. 184 (agravantes del daño, con 3 meses a 4 años de prisión), se prevé que el daño recaiga sobre datos, documentos, programas o sistemas informáticos públicos, o si se ejecuta en sistemas destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte, u otro servicio público.

En estos artículos, se habla particularmente de los malwares (primer párrafo) y de los ataques de denegación de servicios (segundo párrafo). Además, la figura de la venta hace referencia a lo que se conoce como MaaS (malware as a service), RaaS (ransomware as a service), TaaS (trojan as a service) y demás servicios de venta de software malicioso, teniendo en cuenta que muchos ciberdelincuentes no son expertos en informática y programación, por lo que deciden comprar los malwares que fueron creados por un profesional cibercriminal.

Interrupción de Telecomunicaciones

Artículo 197 CP: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

En el Título Delitos contra la Seguridad Pública, ya se encontraba este tipo penal, destinado a proteger las telecomunicaciones. Con el agregado de "o de otra naturaleza" han quedado a cubierto toda clase de comunicaciones.

Supresión o Alteración de Prueba Digital

Artículo 255 CP: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Claramente, el artículo 255 no hace referencia a un tipo de criminalidad informática, sino a la responsabilidad penal de los funcionarios públicos encargados del resguardo de la evidencia digital y su debida cadena de custodia.

TERCERA PARTE

CIBERCRIMINOLOGÍA

CAPÍTULO IV: "CIBERSEGURIDAD"

IV.I) Ciberseguridad

Analizar la Ciberseguridad desde el punto de vista de la Cibercriminología es fundamental para comprender la relación entre los ciberdelincuentes y sus víctimas. El factor humano (la "capa 8") como principal elemento. Esto es así, ya que se requiere entender qué técnicas utilizan los atacantes (herramientas técnicas o engaños) y qué herramientas y acciones preventivas utilizan (o no) las víctimas o cuáles podrían implementar. En definitiva, analizar la Ciberseguridad desde la Cibercriminología no sólo nos ayuda a comprender el por qué, sino también el cómo se producen los ciberdelitos. En la página 15 del presente trabajo, afirmé que la Criminología se nutre de muchas ciencias. La Criminalística (en especial, la Informática Forense) es fundamental. Primero, se consume un delito; luego, se analiza el cómo, mediante una secuencia fáctica (Criminalística); y, por último, el por qué (Criminología) para crear políticas de prevención que eviten que vuelvan a cometerse delitos.

Claudio Caracciolo, profesor de la materia Ciberseguridad de la Especialización en Cibercrimen y Evidencia Digital, define a la Ciberseguridad como un concepto madre que contempla la seguridad informática y la seguridad de la información, ya sea en medio digital, físico o en la cabeza de las personas (2020, campus de Facultad de Derecho). Esto último es importante, porque en la mayoría de los casos se engaña a la víctima. Si bien veremos más adelante la ingeniería social, es importante aclarar que, ya sea que estemos hablando de una estafa por WhatsApp, un ataque ransomware, un troyano bancario o un phishing, casi siempre se recurre a la ingeniería social como técnica para inducir al error humano o a la divulgación de información.

La Jefatura De Gabinete De Ministros de la Presidencia de la Nación, dependiente de la Secretaría De Gobierno De Modernización, mediante el Anexo II (Glosario de Términos de Ciberseguridad) de la Resolución 1523/2019, define a la Ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

William Stallings, un experto en criptografía y seguridad informática, define la ciberseguridad como "la protección de sistemas informáticos y redes contra diversos tipos

de ataques y daños, asegurando que los datos y las operaciones se mantengan seguros y accesibles solo para usuarios autorizados". William Stallings es conocido por su extenso trabajo en el campo de la seguridad informática y criptografía, y su definición refleja la comprensión técnica y aplicada de la ciberseguridad.

La Ciberseguridad abarca la protección de la información y de las personas, tanto desde dentro de nuestros sistemas, como desde afuera, en cualquier medio. La seguridad informática es la protección de la infraestructura computacional y todo lo vinculado a ella, como la información, los datos, la arquitectura, los sistemas, las aplicaciones que están en una computadora o circulan por las redes informáticas. La seguridad de la información es un concepto más amplio que incluye la seguridad informática, pero que está dedicado a la protección de los datos o la información como un todo, más allá de lo tecnológico, en cualquier medio donde se puedan encontrar.

Los pilares de la ciberseguridad que resguardan la información y la mayoría de los ciberataques van a intentar romper, son:

Integridad: Mantener la información íntegra significa que ésta no se altere. Aquí es de vital importancia el número hash para las investigaciones forenses, que asegura la correcta cadena de custodia, sin contaminar la evidencia digital.

Confidencialidad: Implica que sólo el destinatario de la información pueda leerla o poseerla, sin intervenciones ni intromisiones en la comunicación. Algunos ejemplos son los ataques MITM (man in the middle) o el uso de spywares.

Disponibilidad: Que la información se encuentre disponible hace referencia a que sólo pueda ser leída o accesible por la persona autorizada a recibirla y que no haya ningún problema en ello. Aquí entran en juego dos cuestiones relacionadas con la ciberseguridad, por un lado más criminal, los ataques por ransomware que secuestran la información y permanece inaccesible, y los ataques DDos que tumban un servidor o servicio. Por otro lado más organizacional de la ciberseguridad, los controles de acceso y la robustez de las contraseñas; donde, en muchas organizaciones, cualquier persona puede acceder a los ordenadores de sus superiores, o que las contraseñas sean débiles.

Para terminar, cito el texto de un paper realizado por el Ing. Santiago Trigo, el Ing. Gonzalo Ruíz De Ángeli y la Lic. Sandra Cirimelo (2022), para la Universidad FASTA, Facultad de Ingeniería, llamado "Seguridad en el ecosistema digital: ciberseguridad, ciberespacio y las personas":

La ciberseguridad no se reduce a una cuestión técnica de la informática, ni es sinónimo de "seguridad informática". En concreto, la gran mayoría de las denuncias de delitos que se producen en el ciberespacio en la actualidad tienen que ver con la seguridad de las personas. En la investigación de estos delitos informáticos aparecen cuestiones de la criminalística y del derecho que son imprescindibles tenerlos en cuenta. En la prevención, incluso, aparecen cuestiones de la psicología y sociología que considerar. Todos estos aspectos hacen a la ciberseguridad y nada tienen que ver con la seguridad informática, aunque la seguridad informática pueda ayudar a prevenirlos y la informática forense pueda ayudar a esclarecerlos. Cuestiones tan elementales como la educación o concientización de las personas de una organización (y de ciudadanos en general) sobre los riesgos y cómo "cuidarse" en el ciberespacio hacen a la ciberseguridad y no son cuestiones de la seguridad informática. Claramente, la ciberseguridad va más allá de la informática y no es una cuestión de ingenieros, aunque éstos sean partícipes fundamentales, junto a otros profesionales. Una política de ciberseguridad, en síntesis, es una política criminológica, que recurre en algunos aspectos a la informática en general y en algunos temas puntuales a la seguridad informática o informática forense como instrumentos. (p.2)

IV.II) Modelo OSI y la "capa 8"

El modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés) desarrolla un sistema de siete capas de referencia que se aplica en los protocolos de la red de arquitectura en capas. Este modelo fue creado por ISO en 1980 y se aplica como estándar desde 1983. Las 7 capas son:

1. Física: Se refiere al medio físico o de transporte, como son los cables o las ondas.

2. Enlace de datos: Se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

3. Red: Se encarga de los enrutadores o routers y/o la saturación de la red o paquete, se encarga de la comunicación, independientemente del medio de transporte de la información.

4. Transporte: Capa encargada de dividir la información en paquetes para ser transportados por la Capa 3, asegurando que los datos lleguen en el mismo orden en que han sido enviados, y sin errores.

5. Sesión: Se encarga de mantener y controlar el diálogo establecido entre los dos computadores que están transmitiendo datos de cualquier índole.

6. Presentación: Se encarga principalmente de la representación de la información, de manera que, aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, números, sonidos o imágenes, los datos lleguen de manera reconocible.

7. Aplicación: Son los protocolos de comunicación como HTTP, SSH, POP, HTTPS, TCP, etc. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que, a su vez, interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente (interfaz).

Pero, si el modelo tiene siete capas, ¿por qué hablamos de la capa número 8? El error está entre la silla y el teclado. La "capa 8" somos nosotros, los usuarios, los cuales nos encontramos frente al mayor riesgo debido a que somos factibles de caer en engaños, inaplicar políticas de seguridad vigentes, o bien, realizar un uso inadecuado del software. Somos un factor de riesgo, porque, al navegar en internet, estamos dejando un puerto abierto y estamos expuestos a distintos escenarios probables de encontrarnos con una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un malware o una estafa. Por ello, es importante saber cuáles son estas amenazas y estos ciberataques, para prevenir riesgos en la capa 8, o sea, en nosotros.

El riesgo depende de la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El fruto de estos componentes representa el riesgo. Una vulnerabilidad es una debilidad o fallo en un sistema informático que pone en riesgo la seguridad de dispositivos o de la información, permitiendo que un atacante logre comprometer la integridad, disponibilidad o confidencialidad, por lo que es obligatorio localizarlas y eliminarlas cuanto antes. Estos "agujeros" pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos. Vulnerabilidades pueden ser también negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Por su parte, una amenaza, en términos generales, es todo aquello que puede producir daños. Sin embargo, en el ámbito de protección de activos, es toda persona u organización que posee la intención,

la capacidad y la oportunidad de producir uno o más daños. En tal sentido, resulta primordial que cada organización identifique, describa y caracterice a las amenazas dentro del contexto, de la realidad y de la situación que incluya a esa organización. Asimismo, de ser posible, la identificación, la descripción y la caracterización siempre debe ser creada durante la evaluación de riesgos y se debe elaborar un conocimiento específico sobre cada amenaza. Sin embargo, existen ocasiones en las que pudieran emerger nuevas amenazas posteriormente a la evaluación debido a cambios tecnológicos y avances científicos de la vida humana, amenazando a los sistemas de protección física. Una amenaza, entonces, podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, malware) o sucesos físicos (incendios, inundaciones). Desde el punto de vista de una organización pueden ser tanto internas, externas, o externas coludidas con internas (incluyen a amenazas externas que se asocian con miembros de la organización, que pasan a ser internas; y amenazas internas que se asocian con personas o grupos externos para dañar a los activos de la organización).

IV.III) Ciberataques

Claudio Caracciolo (2020) define al ciberataque como un intento malicioso y deliberado de un individuo o una organización de exponer, alterar, deshabilitar, destruir, robar, obtener acceso no autorizado o indebido de la información o de un sistema informático. Recordemos que un sistema informático se compone de hardware, software y un operador (persona, capa 8) que interactúa con éstos.

Existen 2 tipos de ciberataques: los masivos y los dirigidos. Los ciberataques masivos se envían a gran número de personas, sin importar quién es la víctima y "el que cae, cae" o "el que pica, pica". Uno de los ejemplos más claros son los emails raros que nos llegan a la carpeta spam y en otro idioma, diciéndonos que ganamos algo. Los ciberataques dirigidos son más complejos, porque, por alguna razón en particular, una persona es el blanco de un ciberatacante. Ya sea por el tipo de trabajo que tenga, posición política o económica, por religión, por exposición o cualquier otro tema de interés, esa persona está siendo el objetivo de alguien y los ciberataques van dirigidos hacia esa persona en particular, donde sí tiene interés la víctima.

Por otro lado, hay que tener en cuenta que hay ciertos ciberataques que no necesitan de un entendimiento tecnológico para llevarse a cabo, sobre todo cuando el objetivo es

atacar a una persona, ya sea para estafarla, para atentar contra su integridad sexual, su intimidad o su honor.

Ahora veremos algunas modalidades de ciberataques en particular y las relacionaremos con los delitos tipificados en nuestro Código Penal.

Malwares (art. 183): El término malware nace de la unión de dos palabras en inglés "malicious software" (software malicioso) diseñado para infiltrarse en un dispositivo sin su conocimiento (computadora o en un dispositivo móvil). Una vez instalado, el malware infecta el dispositivo y comienza a trabajar para efectuar los objetivos del atacante. El usuario descarga o instala involuntariamente el malware, que infecta el dispositivo. Hay muchos tipos de malwares y cada uno busca sus objetivos de un modo diferente. Algunos más conocidos son:

- Adwares: Dispersa publicidad que suele surgir en ventanas emergentes o en barras de herramientas, simulando ofrecer distintos servicios o productor. El mayor cuidado que se debe tener con este software malicioso es en no hacer clic en ningún anuncio.
- Virus: El objetivo es de infectar archivos del sistema para modificarlo o dañarlo. La técnica radica en alojar su código malicioso en el interior del archivo "víctima", para que ese archivo pase a ser portador del virus y, por lo tanto, una nueva fuente de infección.
- Gusanos: Están diseñados para propagarse automáticamente a través de cualquier medio, como dispositivos de almacenamiento, (pendrives, discos externos, duros), redes sociales, entre otros. A diferencia de los virus, no necesitan de un archivo "víctima".
- Keyloggers: Software malicioso o hardware que registra todas las teclas que se pulsan para operar la computadora o celular, sin permiso o conocimiento. Almacena esa información y la envía al atacante.
- Spywares: Se oculta en el dispositivo, controla la actividad y roba información confidencial, como datos bancarios o contraseñas. Recopila información privada y la transmite al atacante.
- Troyanos: Siguiendo con el concepto del caballo de Troya de la historia, estos malwares destruyen y permiten el ingreso al sistema, haciéndose pasar por una aplicación auténtica. A diferencia de los virus y gusanos, los troyanos no pueden multiplicarse. Existen de muchos tipos y, hoy en día, según un informe de ESET Latinoamérica, Argentina lidera el ranking con más casos de troyanos bancarios. Este tipo de troyano puede activarse al ingresar a determinadas páginas web bancarias. Puede ser tipo

spyware/keylogger, puede hacer aparecer un banner o ventana emergente similar al banco, pidiendo ingresar credenciales allí, además de desconectar mouse y teclado (o tildar). En Android, puede desplegar una interfaz que enmascara la aplicación real de homebanking, pero en realidad se trataría de un colector de datos bancarios.

- Ransomwares: Secuestro de archivos para extorsionar y exigir un pago de dinero para recuperarlos o para evitar su divulgación. Los ciberataques por ransomware han crecido enormemente estos últimos años, por lo que se han convertido en una verdadera problemática. Este software malicioso se encarga de cifrar archivos y, cuando se intenta abrirlo, aparece un cartel informando el ataque y exigiendo un pago de dinero en bitcoin para la obtención de la clave que sirve para descifrar. Además, muchas veces se extorsiona a la víctima, amenazándola con la divulgación de la información. Lógicamente y a diferencia de los demás malwares, éste funciona con el conocimiento de la víctima.
- Rootkits: Paquete (kit) de malwares diseñados para infiltrarse sin conocimiento y permitir el acceso a un sistema e interceptar sus funciones, permitiendo también ocultar procesos, manipular el dispositivo y robar información.

Hacking (art. 153 bis): Entendido como un delito, el hacking es el acceso a un sistema informático sin autorización o excediendo la que se posea. Puede darse a través de herramientas informáticas (por ejemplo, a través de malwares) o entrando en el Facebook de mi pareja sin que sepa o simplemente desbloqueando el teléfono de otra persona, sin su autorización. En la mayoría de los casos, la víctima no se da cuenta de la intrusión ilegal. Una vez ingresado al sistema, el delincuente puede realizar más acciones maliciosas, como robo de credenciales, robo o destrucción de información, instalación de software malicioso, etc.

En el ámbito de la Informática, se denomina hacking a la exploración permanente sobre sistemas informáticos, tanto de sus medidas de seguridad como de sus vulnerabilidades y la forma de sacar ventaja de estas. Por ende, un hacker es aquella persona que tiene vastos conocimientos sobre computadoras y redes informáticas, con amplias capacidades de investigación y en la búsqueda constante de perfeccionar sus técnicas.

Existen 3 tipos de hackers distintos. Los “buenos” (hackers de sombrero blanco), los “malos” (de sombrero negro) y los “híbridos” (sombrero gris). Los hackers buenos o de sombrero blanco son aquellos que tienen un trabajo legal, donde su propósito no es malo. Suelen encargarse de realizar pentesting (pruebas de penetración) y escaneo de

vulnerabilidades de sus sistemas de trabajo, con previa autorización. Los hackers de sombrero negro sí son malignos y abarcar distintos objetivos que perjudican el normal funcionamiento de un servidor o comprometer la información. Por último, los hackers de sombrero gris son aquellos que acceden ilegalmente a un sistema informático, pero que avisan sobre el problema de seguridad y no realizan acciones malignas dentro del sistema. Por lo general, buscan una recompensa económica o ser contratados. Cabe aclarar que hay más "colores de sombreros" de los hackers, que hacen alusión a tu trabajo, si es de defensa u ofensa.

Si bien en el capítulo sobre perfiles cibercriminales volveré a mencionar a los hackers, hay que tener en cuenta que un hacker no es un delincuente, sino un profesional. Un ejemplo claro es un policía bueno y un policía que hace abuso de sus facultades, es decir, un policía que mata indebidamente a una persona es un delincuente. Del mismo modo, un hacker que irrumpe ilegalmente pasa a ser ciberdelincuente.

Botnet, ataque DoS y DDoS

- Botnet (arts. 153bis y 183): También llamada máquina zombi, ya que se infecta un dispositivo con el objetivo de manipularlo. El atacante tiene acceso y control de una computadora remota.
- Ataque DoS (art. 183): Denial of Service. El ataque de denegación de servicio es un ataque a un sistema de computadoras o red de dispositivos infectados con una variedad de malwares que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, siendo controlado por el atacante. Impide que un servidor preste su servicio, saturándolo y generando una sobrecarga.
- Ataque DDoS (Distributed Denial of Service): El ataque de denegación de servicios distribuido tiene el mismo concepto que el anterior, pero con la diferencia que comprende una red de botnets o máquinas zombis que, en conjunto, atacan a un servidor. Múltiples computadoras en distintas ubicaciones del mundo envían múltiples ataques a un solo objetivo.

Exploit (arts. 153 bis y 183): Herramienta o programa que aprovecha las vulnerabilidades (puntos débiles o defectos de seguridad) de las aplicaciones, las redes, los sistemas operativos o el hardware. Los atacantes pueden instalar software malicioso

(malware), prender cámara o micrófono, robar archivos, o manipular completamente un sistema.

Man In The Middle (MITM) (arts. 153 y 153 bis): "Hombre en el medio". Se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y el dispositivo. Por ejemplo, simplemente por tener el dispositivo conectado a una red WiFi. Una entidad externa intercepta una comunicación entre el dispositivo y su conexión a internet, pudiendo ver y acceder al correo electrónico, redes sociales, navegación web.

En un ataque MITM frecuente, se utiliza un router WiFi para interceptar las comunicaciones del usuario. El atacante configura su dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería). Después, el usuario se conecta al "router" y navega por internet, capturando el criminal los datos de la víctima o infectando el dispositivo. En un ataque MITM menos frecuente y más complejo, el hacker ataca y logra acceder directamente el módem o router de la víctima.

Grooming (art. 131): Abuso sexual hacia niños, niñas y adolescentes a través de internet y dispositivos electrónicos (computadoras, celulares, consolas de videojuegos). El groomer chatea y se gana la confianza de la víctima con fines sexuales, tales como el envío de fotos o videos íntimos. El groomer (atacante) elabora lazos emocionales (de amistad) con el NNA. Utiliza tácticas como la seducción, provocación y el envío de imágenes de contenido pornográfico, consiguiendo trasgredir la intimidad de su víctima. Es así como se va ganando la confianza y logra el objetivo de que su víctima se desnude o cometa actos de naturaleza sexual.

Según el objetivo, los groomers pueden atacar solos por simple autosatisfacción, ser parte de una organización de MASI (material de abuso sexual contra las infancias o mal llamada "pornografía infantil", art. 128) o lograr producir un abuso sexual físico presencial (hasta incluso, matar a su víctima, como el caso de Micaela Ortega). También, se genera un problema mayor cuando el groomer amenaza a su víctima con publicar ese material, exigiéndole así más material pornográfico. Es ahí cuando el menor comienza a desarrollar ciertos problemas psicológicos.

Se considera que es abuso, ya que es una acción o conducta de naturaleza sexual en contra de la libertad sexual de una persona que es incapaz de consentir esa acción, en la que no se emplea violencia física o intimidación directas. Las víctimas son menores de

edad por su inmadurez sexual y la incapacidad de discernir entre lo que está bien y lo que está mal.

Spoofing: Es el robo y suplantación de identidad para la utilización o explicación de los datos de identificación personal u otro tipo de información de la persona como el nombre, el número de DNI, etc., para cometer fraude o participar en otras actividades ilegales. Si bien no constituye un ciberataque dirigido hacia alguna persona, puede generarle problemas a la persona a la que se le robó la identidad. Por ejemplo, pueden realizar compras a mi nombre o cometer un delito y la justicia vendría por mí. En Argentina, no constituye un delito.

> No se legisló por ejemplo sobre robo de identidad porque esa figura estaba cubierta en forma abarcativa por la estafa y la falsedad de documentos. Sin embargo queda más que claro que en materia de robo de identidad existe un enorme vacío de parte del Estado en prevención y educación de usuarios de Internet y una real toma de conciencia de entidades financieras (Palazzi, Pablo A. 2016, p.24).

Ciberespionaje (arts. 153, 153 bis, 183 y 184): Según el Manual de Tallin (OTAN, Estonia, 2013), se lo define como un acto emprendido clandestinamente o bajo falsas pretensiones que utiliza capacidades cibernéticas para recopilar información con la intención de comunicarla a la parte contraria. Aquí, los spywares tienen mayor protagonismo. El malware Flame y el grupo APT1 son claros ejemplos de operaciones de ciberespionaje. El objetivo es el robo de información confidencial y sin conocimiento de la víctima, por parte de un Estado o empresa. Es raro y no tendría mucho sentido entre particulares. Aunque, en realidad, cualquiera que sea el objetivo, casi siempre un hacker termina espiando a su víctima.

Flame fue la ciberarma más poderosa, junto con el gusano Stuxnet (que el objetivo del gusano no era robar información, sino alterar el funcionamiento de las bombas centrífugas de una planta nuclear) y se relacionaros directamente con los gobiernos de Estados Unidos e Israel. Por su parte, el grupo de ciberespionaje APT1 fue por parte del estado militar chino hacia empresas. APT significa Advanced Persistent Threat, o amenazas avanzadas persistentes, que son un conjunto de técnicas informáticas discretas guiadas por un tercero (organización, grupo delictivo, una empresa, un estado) con la finalidad y

la capacidad de atacar de forma avanzada y prolongada en el tiempo, un objetivo definitivo (empresa competidora, estado, etc.) a través de múltiples líneas de ataque, utilizando ingeniería social, malwares y exploits.

Técnicas de ingeniería social: Previamente, definí a la ingeniería social como una técnica de manipulación psicológica que tiene por objetivo inducir al error humano o a la divulgación de información. Frente a esta definición, cualquier estafa es una técnica de ingeniería social, ya que, principalmente, se engaña a la víctima, haciendo que ésta no sea consciente de estar siendo víctima. Más adelante, veremos que la estafa para robar dinero (art. 173) no es el único objetivo de un criminal para utilizar ingeniería social, sino que también puede utilizarse para ataques ransomware, troyanos (art. 183), hacking (art. 153 bis) y ciberespionaje (art. 153). Ahora, veremos las técnicas de ingeniería social aplicadas al ciberespacio:

- Phishing: Al igual que la traducción al español, "pescar". Se envía un correo electrónico a una o gran número de personas y "el que pica, pica". Un tercero se hace pasar por una entidad (un banco, Netflix, Mercado Libre, Mercado Pago, etcétera) enviando un email que simula ser la entidad real, pero que no lo es. Suelen notificar un bloqueo de la cuenta y dejando un link que dirige a una página web idéntica a la original (pero que no lo es), solicitando datos bancarios, usuarios, contraseñas o tarjetas de crédito/débito para "validar la cuenta". Otra modalidad de phishing implica hacer clic en un enlace que automáticamente nos descarga un malware que infecta nuestro dispositivo, o con un archivo adjunto malicioso. Esta modalidad es muy frecuente en organismos estatales o empresas, donde la seguridad es muy grande y siempre se intenta atacar a la inocencia humana. En este caso, hablamos de un ataque de spear-phishing, donde el ciberataque es plenamente dirigido hacia esa persona. Luego de tareas de inteligencia e ingeniería social, se diseña un correo phishing personalizado directamente a una víctima en particular.
- Vishing: El término suele referir únicamente a las realizadas por llamado telefónico, pero muchos expertos en Ciberseguridad encuadran también a cualquier tipo de estafa informática que no sea por email (llamadas y redes sociales, como WhatsApp, Telegram, Facebook, Instagram) que además pueda robarnos datos sensibles (personales). Engaños, simulaciones, cuentas falsas, estafas de inversión, piramidales, ofertas

fraudulentas de ventas o de trabajo, de lotería y demás. Veamos algunos ejemplos de modalidades delictivas por redes sociales:

Por Instagram: Una persona quiere sacar pasajes para irse de vacaciones, entonces busca por Instagram el nombre de una empresa de venta de pasajes y les habla para poder comprar uno. Ellos con gusto atienden su consulta. Sin saberlo, esa persona se contactó con una cuenta falsa, fraudulenta, que simulaba ser la original, pero no lo era.

Por WhatsApp: Al ser la red social más utilizada, los casos son numerosos y muy peligrosos. Uno de ellos son los enlaces maliciosos que se difunden por esta aplicación, donde un contacto conocido envía una supuesta promoción de una empresa y al hacer clic o tocar ese enlace, automáticamente se descarga un malware que infecta nuestro dispositivo. Otra modalidad es la mencionada anteriormente, donde una persona se hace pasar por una entidad (por ejemplo, el gobierno) y avisa que le va a llegar un código que debe pasarle para "validar datos". En realidad, ese código es de acceso a WhatsApp y no hay que dárselo a nadie. El criminal ingresa los datos de nuestro WhatsApp muy fácilmente en otro dispositivo, inicia sesión y tiene acceso a nuestros contactos. Ya sea por una modalidad o por la otra, el cibercriminal, al tener acceso al dispositivo y a los contactos, envía mensajes a todos los contactos con el mismo enlace o simulan ser nosotros mismos, manifestando necesitar dinero, donde el CBU o CVU es distinto del titular.

Considero importante diferenciar a los estafadores activos de los pasivos. En los últimos tiempos, entendí que un estafador activo busca contactarse con potenciales víctimas y realiza ataques de ingeniería social y suplantación de identidad. El pasivo se crea una cuenta falsa y espera a que las víctimas vayan a él. Por ejemplo, una cuenta fraudulenta de venta de indumentaria, donde una persona, que se encuentra navegando por las redes sociales, ve esta cuenta, le llama la atención, le gustó un producto, se contacta con el criminal para comprarle algún producto y le realiza una transferencia, sin recibir ningún producto.

IV.IV) Organizaciones cibercriminales

Si bien la mayoría de los cibercriminales actúan en bandas delictivas con una clara división de tareas, cuando se habla de las grandes organizaciones cibercriminales se suele hacer referencia a los grupos que crean, venden y distribuyen ransomwares. La banda de ransomware LockBit es uno de los sindicatos organizados de delitos cibernéticos más notorios que existen en la actualidad. La pandilla está detrás de ataques dirigidos a

corporaciones del sector privado y otras industrias de alto perfil en todo el mundo. Los medios de comunicación y las noticias han documentado muchos ataques de LockBit, mientras que los proveedores de seguridad ofrecen evaluaciones técnicas que explican cómo ocurrió cada uno. Aunque estos proporcionan información sobre los ataques, quería saber más sobre el lado humano de la operación para conocer las percepciones, motivaciones y comportamientos de las personas al otro lado del teclado.

Como ocurre con cualquier habilidad u oficio, llegar a ser competente en lo que hace requiere práctica y experiencia. Por ejemplo, sé que grupos de ransomware como DarkSide y REvil comenzaron como afiliados que respaldaban programas de ransomware como servicio (RaaS) más maduros antes de expandirse de forma independiente. De manera similar, los criminales detrás de la pandilla LockBit probablemente comenzaron sus carreras ilícitas antes de que comenzara la operación LockBit. La nueva campaña RaaS tenía varias características atractivas para tentar a los afiliados a unirse a la operación. La banda LockBit afirmó que su carga útil de ransomware tenía capacidades de cifrado rápidas y podía autopropagarse dentro del entorno de la víctima.

En términos de ataques de ransomware, las víctimas casi siempre son objetivos de oportunidad, no de diseño. Recordemos que el atacante quiere que le paguen y busca acceso a cualquier víctima que considere lo suficientemente rentable como para pagar el rescate. Además, muchas bandas de ransomware con sede en Rusia, como LockBit, tienen relaciones sólidas con otras bandas, que a veces comparten recursos e incluso datos de las víctimas. Por lo tanto, el uso de objetivos e industrias observados en múltiples operaciones de ransomware generalmente no es lo suficientemente convincente como para respaldar una atribución sólida. Además, en noviembre de 2021, Europol arrestó a doce hombres por apoyar la operación de ransomware Gogalocker. Ninguno de los hombres arrestados afirmó tener alguna asociación con LockBit. Si lo hubieran hecho, probablemente habrían utilizado la información como moneda de cambio para minimizar la sentencia que enfrentaban.

Jon DiMaggio, un estratega jefe de seguridad, logró infiltrarse en foros criminales y grupos de chat privados utilizados por delincuentes de ransomware y obtuvo conocimientos internos sobre la propia pandilla LockBit. Identificó las cuentas y la infraestructura utilizada por la pandilla y los delincuentes con los que interactuaban. Pudo ver las herramientas y recursos utilizados para gestionar y realizar ataques desde la perspectiva del adversario. Más importante aún, aprendió sobre las opiniones, hábitos personales,

motivaciones e inseguridades de los criminales humanos detrás de la operación. DiMaggio dice que el individuo que actualmente lidera y dirige la operación de ransomware LockBit, que a menudo utiliza el personaje en línea "LockBitSupp", está demostrando rasgos narcisistas que alimentan su ego en constante crecimiento. En los últimos meses, ha habido un sentimiento cada vez más negativo hacia la personalidad "LockBitSupp". El disgusto surge de los comentarios arrogantes que hace en foros criminales y entrevistas con los medios. Muchos delincuentes no aprecian el enfoque de "mírame" que adopta LockBit para promocionar su programa de ransomware. Además, muchos delincuentes están cansados de los trucos publicitarios de LockBit para llamar la atención, como pagar a personas para que se hagan tatuajes con el tema "LockBit" y publicar las imágenes en las redes sociales. Durante los últimos seis meses, el personaje de LockBitSupp ha llevado a cabo varias “campañas de desprestigio” basadas en propaganda contra pandillas rivales. LockBit utiliza información y programas legítimos, que presenta con mensajes en foros escondidos para defiende una historia que beneficia sus propios intereses al tiempo que intenta perjudicar la reputación de otras bandas. El líder de LockBit afirma que almacena las claves PGP, las carteras Crypto, los archivos de claves y otros datos confidenciales en dos unidades de disco. Las unidades se almacenan por separado unas de otras para evitar que alguien obtenga acceso. Mantiene una unidad flash en un collar que siempre usa, y otra está guardada en una unidad guardada por un tercero en una ubicación remota para su custodia. El liderazgo de LockBit afirma que accede a su infraestructura de back-end a través de Starlink, un servicio de Internet satelital estadounidense propiedad de SpaceX y afirma que depende principalmente de los intercambios de Bitcoin en Hong Kong y China para lavar su dinero. Cree que la relación de confrontación de China con Estados Unidos hace que sea más seguro y más fácil realizar operaciones de lavado.

Según el líder de LockBit, el desarrollador del ransomware DarkSide es el mismo individuo que desarrolló el ransomware BlackMatter y LockBit Black y anteriormente desarrolló malware para Fin7, otro grupo de cibercrimen. Este individuo está vinculado a muchos ciberdelincuentes de alto nivel y debería ser un objetivo para las operaciones gubernamentales y policiales. Además, el desarrollador puede tener conocimiento de primera mano de las identidades de miembros clave de varios sindicatos de delitos cibernéticos. LockBit interactúa y se comunica con otras bandas de ransomware, DarkSide/BlackMatter, BlackCat, REvil, Hive y BlackBasta. Las relaciones son de confrontación, pero los individuos detrás de estas pandillas parecen conocerse y tener líneas directas de

comunicación entre sí. LockBit cree que Conti y ahora BlackBasta trabajan y apoyan en secreto al gobierno ruso y cree que la pandilla brinda apoyo directo al FSB. En 2020, LockBit patrocinó un "concurso de trabajos de verano" en el que los solicitantes presentarían trabajos de estilo académico relacionados con técnicas de piratería y explotación. LockBit seleccionaría el mejor artículo y otorgaría al autor un premio monetario. Este fue uno de sus primeros intentos de ganar reconocimiento entre los ciberdelincuentes y demuestra su enfoque innovador para identificar y reclutar futuros delincuentes inteligentes.

IV.V) Ingeniería social

Si buscamos en internet "ingeniería social", vamos a observar que las definiciones son afines a la seguridad informática y mencionan a los cibercriminales. Esto no es así, ya que, en realidad, la ingeniería social es una práctica tan antigua que existe desde mucho antes que exista internet.

Para las ciencias sociales, el término ingeniería social se remonta al siglo XIX y refiere al objetivo de influir sobre el comportamiento de una población determinada, ya sea para bien o para mal. Esto requiere un esfuerzo por los gobiernos, medios de comunicación o entidades privadas. Tal vez les pueda aclarar este concepto con un simple ejemplo: la dictadura militar argentina (1976 – 1983) que se caracterizó por implementar un terrorismo de Estado (infundir terror), el mundial de 1978 como coartada y la guerra de Malvinas en 1982, donde las noticias eran distintas a la realidad.

Hoy en día, el término ingeniería social refiere al ámbito de la ciberseguridad y comprende una de las principales modalidades delictivas que hacen al cibercrimen. Se entiende a la ingeniería social como una técnica de manipulación psicológica basada en engaños, en la que un delincuente busca conseguir que su víctima realice determinadas acciones que lo beneficien, sin que la otra persona pueda darse cuenta de que está siendo víctima de un delito. Induce al error humano o a la divulgación de información. Es por ello por lo que se plantea decirle "ciberinfluencia" o "influencia social".

En Argentina, conocemos a "el cuento del tío" como una modalidad delictiva antigua, en la que un par de delincuentes toca timbre en un domicilio, se hace pasar por personal de alguna empresa (agua, luz, gas) y pide permiso para ingresar al domicilio, con alguna excusa de realizar alguna medición interna, usar el baño o el teléfono, para luego lograr que su víctima (generalmente, personas mayores) le permita ingresar a su casa. Muchas veces, no sólo utilizan indumentaria de alguna empresa, sino que simulaban

trabajar varias horas, para lograr engañar aún más a su víctima. Una vez adentro, los delincuentes se identifican como tales, reducen a sus víctimas y roban las pertenencias y el dinero que puedan encontrar. Muchas veces, los delincuentes ejercen violencia para que la víctima confiese dónde se encuentra el dinero y muchas veces "desvalijan" la casa, dejando el domicilio vacío.

Cuando hablamos de manipulación o engaños, no sólo nos referimos al cuento del tío presencial. También cabe mencionar aquellos famosos casos de engaños telefónicos o “cuento del tío telefónico”, donde suena el teléfono, una persona atiende y escucha del otro lado la voz de un niño o una niña, diciéndole “Mamá, soy yo. Me tienen secuestrado. Dicen que, si no llevás toda la plata a un lugar, me van a matar”. O también, “Abuela, soy yo. Tuve un accidente y necesito plata. Va a ir un amigo a buscarla”. Esto también es ingeniería social.

Hoy en día, existen decenas de delitos producidos por engaños, con o sin internet: por el cuento del tío, por llamadas telefónicas, por correos electrónicos falsos (phishing), ofertas fraudulentas, las estafas piramidales, ofertas de empleo etcétera. Es por ello por lo que, “el cuento del tío digital” será aquella actividad delictiva en la que un delincuente se hace pasar por personal de una entidad (empresa, banco o gobierno), contacte a una persona a través de dispositivos electrónicos y logre engañar a su víctima para que ésta le brinde alguna información que pueda darle acceso a su dispositivo o a su cuenta bancaria, para robarle información o el dinero de su cuenta.

Ahora bien, sólo he expuesto casos donde el riesgo es patrimonial, es decir, que nos roben dinero. Me parece crucial no dejar de mencionar los delitos contra la integridad sexual hacia niños, niñas y adolescentes. Muchas veces, los casos de abuso sexual infantil no se dan con violencia ni con personas desconocidas, sino todo lo contrario. El abuso sexual contra las infancias requiere del engaño del agresor hacia la víctima, haciéndole creer que es un juego, que es normal, que no tiene nada de malo. Este engaño es un abuso de poder hacia la mentalidad inocente y de la inmadurez sexual del niño o de la niña; y, lo peor de todo, es que, mayormente, los agresores son personas conocidas de la víctima (padre, tío, abuelo, hermano, primo, etc.) y el niño o la niña no tienen noción de estar siendo víctimas de un delito.

De la misma manera, trasladamos el abuso sexual infantil hacia internet y nos encontramos con la definición de grooming, donde acá no sólo el agresor puede ser una persona conocida de la víctima, sino que la hiperconectividad y el anonimato que permite

internet generan que el agresor pueda ser cualquier persona en cualquier parte del mundo, diciendo ser quien quiera y con la edad que quiera. Si bien no tenemos un abuso sexual físico, el abuso está, el engaño está y muchas veces se logra concretar un encuentro real con un abuso sexual físico. Muchas veces, el groomer (agresor) vía internet, convence a su víctima menor de edad de masturbarse frente a una cámara web; y esta práctica ha sido entendida por jueces como un verdadero abuso sexual físico.

Veamos algunos ejemplos de modalidades delictivas.

Por correo electrónico (email): cualquier persona puede recibir un correo de phishing, ya sea porque el ciberataque sea masivo, donde se envía a gran número de personas sin importar quién es la víctima; o porque el ciberataque sea dirigido, cuando, por alguna razón específica (política, económica, trabajo, forma de pensar, etcétera) somos el blanco de un cibercriminal. En organizaciones empresariales importantes o estatales, muchas veces se logran infectar con un malware a través de un link malicioso al que alguien hizo clic.

Por redes sociales: Hay que tener en cuenta y concientizarnos acerca del peligro que implica dejar nuestros datos personales y nuestras fotos en redes sociales a la vista y merced de todos, que facilita al ciberdelincuente a obtener información nuestra, cuando tenemos un perfil público o aceptamos a cualquier persona. Por otro lado, hoy en día ya no es meramente necesario que un tercero se haga pasar por una entidad (por ejemplo, por el gobierno para saca turno para la vacuna contra el Covid-19), sino que, como vimos anteriormente, uno mismo se dirige hacia cibercriminales.

IV.VI) Inteligencia artificial y nuevos desafíos

La inteligencia artificial abre en la historia de la humanidad un sendero inexplorado y radicalmente excepcional, que sin lugar a duda constituirá un punto de inflexión en nuestra evolución como especie. Desde el surgimiento mismo del universo, hace 13.800 millones de años, la conformación de nuestro sistema solar, hace 4500 millones de años, y posteriormente el surgimiento de la vida en nuestro planeta; el advenimiento de la inteligencia en la especie humana ha constituido un punto de ruptura en la evolución. El surgimiento de vida inteligente en este planeta constituye una maravilla sin precedentes hasta la fecha. El astrofísico y científico Stephen Hawking, dice:

> Todo lo que la civilización tiene para ofrecer, es producto de la inteligencia humana. El ADN transmite los planos de la vida entre generaciones. Formas de vida

> cada vez más complejas captaron información mediante sensores como ojos y oídos y la procesan en cerebros u otros sistemas para descubrir cómo reacciona el mundo, ... En algún momento durante nuestros 13.800 millones de años de historia cósmica, algo maravilloso sucedió. Este procesamiento de información devino tan inteligente que las formas de vida llegaron a ser conscientes. El universo ha despertado y ha tomado consciencia de sí mismo. (Hawking, Stephen, "Breves respuestas a las grandes preguntas", Título original Brief Answers to the Big Questions. Traducción de David Jou Mirabent, Ed. Paidós, Buenos Aires, 2018, 1ª ed., p. 227)

A comienzos del siglo XXI, la evolución tecnológica, y la convergencia de seis factores ha ayudado a la Inteligencia Artificial "a pasar del medio in vitro (los laboratorios de investigación) al in vivo (la vida cotidiana)"[17]. La evolución exponencial y su auge actual se debe esencialmente a la convergencia de estos seis factores, que son: macrodatos o big data, poder de procesamiento, un mundo interconectado, software y datos de dominio público, mejores algoritmos y rendimientos acelerados. Por este motivo, la convergencia de estos seis factores a través del "establecimiento de marcos teóricos compartidos, combinado con la disponibilidad de datos y poder de procesamiento, ha producido éxitos notables en diversas tareas de componentes, tales como reconocimiento de voz, clasificación de imágenes, vehículos autónomos, traducción automática, locomoción articulada y sistemas de preguntas y respuestas" (Stephen Hawking, 2018).

En las últimas dos décadas el empleo de inteligencia artificial, y en particular la incorporación de robots en el mercado laboral se ha incrementado significativamente, a fin de abaratar costos de investigación, desarrollo y producción, incrementar la producción, reducir los plazos de producción, como así también de entrega del productor, y mejorar su calidad. Tal es así, que al año 2016 existían ya, 1.800.000 robots empleados en la manufactura de productos. Actualmente, más de 20 países están en manos de la inteligencia artificial y empleo de robots para su perfeccionamiento industrial. Stephen Hawking (2018) sostiene que "usada como una herramienta, la inteligencia artificial podría aumentar nuestra inteligencia actual y abrir avances en cada área de la ciencia y la sociedad. Sin embargo, también conllevará peligros... La preocupación estriba en que la inteligencia artificial se perfeccionaría y se rediseñaría a sí misma a un ritmo cada vez mayor.

[17] RAO, Anand S., "Una nueva etapa de la globalización", publicado en AA.VV., Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina, Integración & Comercio #44, Julio 2018, Ed. Planeta, Buenos Aires 2018, 1ª ed., ps. 51-52.

Los humanos que estamos limitados por la lenta evolución biológica, no podríamos competir con ella, y seríamos superados". El autor Anand S. Rao[18] cree que la Inteligencia Artificial presenta seis factores de riesgos bien claros y definidos, siendo estos: riesgos de rendimiento, riesgo de seguridad, riesgos del control, riesgos económicos, riesgos sociales y riesgos éticos. Establece un riesgo de rendimiento, porque los sistemas de IA requieren ser verificados y validados utilizando técnicas pautadas. Por ejemplo, el manejo autónomo, previo a ser seguro para su introducción fuerte, demandará variadas operaciones de verificación y validación. Por su parte, el riesgo de seguridad emana del uso inapropiado de la Inteligencia Artificial por parte de piratas informáticos, ya que, muchos algoritmos desarrollados con buenas intenciones (los vehículos autónomos) pueden ser repensados para hacer daño (para obtener armamentos autónomos). A su vez, también se genera un riesgo de control de los organismos con inteligencia artificial, por parte de los seres humanos, debido a que "algunos sistemas de IA trabajan de manera autónoma, e interactúan entre sí generando mecanismos de retroalimentación entre las máquinas que pueden provocar resultados inesperados" (Rao, Anand S). A ello, debe adicionarse riegos económicos, debido a que a medida que las empresas transnacionales que adopten Inteligencia Artificial en su producción crezcan en forma exponencial, pueden alterar significativamente las reglas actuales del mercado. Estos riegos económicos se encuentran emparentados con riesgos sociales tales como el hecho de que la automatización a gran escala amenaza con reducir el empleo en el transporte, la industria manufacturera, la agricultura y el sector de servicios entre otros. Incluso más preocupante de todos los riesgos sociales es el empleo de IA para el desarrollo de armamento autónomo. Una vez desatado el desarrollo de armamento autónomo, estos pueden a su vez provocar daños de gran magnitud en el medioambiente, un escenario apocalíptico, donde una IA militarizada supondría un riesgo existencial para la humanidad. Los ejércitos de las grandes potencias ya han empezado con la producción de prototipos de técnicas autónomas de armas. El ejemplo más representativo es el de Corea del Sur, con el caso del SGR-A1, diseñado por grupo surcoreano Samsung. Desde 2013, este “robot centinela” vigila día y noche la frontera de las dos Coreas, gracias a cámaras de alta definición y sensores que pueden distinguir un blanco en movimiento a una distancia de cuatro kilómetros. También reconoce voces y contraseñas, distingue un hombre de un animal y lanza la orden de rendirse cuando

[18] RAO, Anand S., "Una nueva etapa de la globalización", ob. cit., p. 56

alguien atraviesa la línea de demarcación. Si el sospechoso levanta los brazos, este "Robocop" no tira. Si no lo hace, puede usar su ametralladora Daewoo K3 de calibre 5,56 mm o un lanzagranadas de 40 mm. La autorización de abrir fuego sigue dependiendo del ser humano (oficial de mando), pero el dispositivo posee un modo "automático" que le permite desenvolverse solo.[19]

Otros estados como los Estados Unidos de América, la Federación de Rusia, la República Popular de China, el Reino Unido de Gran Bretaña e Irlanda del Norte, e Israel, también han comenzado con el desarrollo de sistemas autónomos de armas. Esto despertó cierta inquietud internacional. En ocasión de la Conferencia Internacional sobre inteligencia artificial del 28/07/2015, miles de personalidades, entre las que se encontraban el astrofísico británico Stephen Hawking, el lingüista Noam Chomsky o empresarios como Elon Musk (SpaceX) y Steve Wozniak (Apple), lanzaron un llamado para prohibir los sistemas de armas autónomas letales (SAAD). Incluso las Naciones Unidas busca dictar un Tratado que prohíba la proliferación de armas autónomas y la magnitud de los avances recientes en inteligencia artificial han suscitado un llamamiento al Parlamento Europeo para redacte un conjunto de regulaciones que rija la creación de robots con IA. Por último, la inteligencia artificial también conlleva un claro riesgo ético. Carlos Sueiro (2020) sostiene que "el empleo masivo y cotidiano de inteligencia artificial, implica la utilización de macrodatos; la creciente dependencia de algoritmos para llevar adelante tareas, diseñar alternativas y tomar decisiones; y la reducción gradual de la participación humana en muchos procesos". Además, sostiene que la disminución paulatina de la intervención humana en labores tales como toma de decisiones, plantea graves complicaciones en cuestiones vinculadas y relacionadas con la justicia, la igualdad y el respeto por los derechos humanos.

La IA tiene sus raíces en la década de 1950, cuando los primeros investigadores comenzaron a explorar la posibilidad de crear máquinas que pudieran pensar y aprender. Desde entonces, la IA ha evolucionado significativamente, pasando de simples programas de computadora a sistemas complejos que pueden aprender y adaptarse. Ha evolucionado de la lógica simbólica a la inteligencia artificial basada en el aprendizaje automático, lo que ha permitido una mayor capacidad de análisis y toma de decisiones. La evolución de

[19] PFLIMLIN, Édouard, "La urgencia por prohibir los robots asesinos. Tercera revolución de las técnicas de guerra", artículo publicado en el Periódico Le Monde Diplomatique, 213, año XVIII, marzo de 2017, pp. 34-35.

la IA ha sido impulsada por avances en campos como el procesamiento de lenguaje natural, la visión por computadora y el aprendizaje profundo.

La inteligencia artificial es un campo en constante evolución que busca desarrollar sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. También, ha revolucionado la forma en que se abordan las amenazas cibernéticas. Es una herramienta fundamental para la detección de amenazas cibernéticas, ya que puede analizar grandes cantidades de datos e identificar patrones que no serían visibles para los humanos. La IA se ha convertido en un componente clave en la lucha contra las amenazas cibernéticas, desde la detección de malware hasta la identificación de vulnerabilidades en los sistemas.

En la ciberseguridad, la IA se ha convertido en una herramienta fundamental, con aplicaciones que van desde la detección de malware hasta la identificación de vulnerabilidades en los sistemas. La IA puede ser utilizada para analizar grandes cantidades de datos e identificar patrones que pueden indicar una amenaza cibernética. Sin embargo, también plantea desafíos en cuanto a la privacidad y la seguridad de los datos. la IA también puede ser empleada negativamente para la creación de malware y ransomware más sofisticados, ataques de phishing y engaño más efectivos, análisis de vulnerabilidades y explotación de debilidades en los sistemas y más. Hoy en día, se utiliza mucho Chat GPT para la redacción de textos sin errores gramaticales ni de ortografía. Esta herramienta permite crear correos electrónicos fraudulentos más difíciles de detectar. Además, herramientas de IA como FakeYou y DeepFake son utilizadas para aumentar el engaño hacia la víctima. Estos programas crean videos o audios alterados digitalmente para que simulen ser reales. Pueden utilizarse para engañar a las personas (ingeniería social) haciéndoles creer que están interactuando con algún conocido, que no es. Estos deepfakes pueden ser utilizados para realizar estafas, influir en la opinión pública u operar el mercado de valores, ya que también se han creado videos alterados con la imagen de los grandes magnates de la política, tecnología y economía.

Aplicando la inteligencia artificial, se le preguntó a Chat GPT qué es Chat GPT. La respuesta automática fue: “ChatGPT es un modelo de lenguaje desarrollado por OpenAI, basado en la arquitectura GPT (Generative Pre-trained Transformer). Su función principal es entender y generar texto de manera coherente y útil en función de las preguntas y comentarios que recibe. El modelo ha sido entrenado con una amplia variedad de textos y puede realizar tareas como responder preguntas, mantener conversaciones, proporcionar

explicaciones sobre diversos temas, ayudar con la redacción de textos y mucho más. Aunque es bastante avanzado en la comprensión y generación de texto, no tiene consciencia ni emociones, y sus respuestas se basan en patrones aprendidos durante su entrenamiento".

Sol Gonzales, Ingeniera en Informática que ha desarrollado un escrito para la empresa de seguridad ESET, sostiene 6 usos maliciosos con Chat GPT que incluyen la creación de noticias falsas o *fake news*, ataques de phishing, robo de identidad, desarrollo de malware, automatización de procesos ofensivos y chats ofensivos. Además, dice que "Investigaciones ya han demostrado que los cibercriminales ya comenzaron a utilizar Chat GPT para utilizarlo como herramienta para desarrollar código malicioso y realizar otro tipo de acciones fraudulentas" (welivesecurity.com, 2023). Ante esta creciente amenaza, la prevención de ciberataques con IA y la implementación de ciberseguridad contra la IA se han transformado en prioridades para algunas empresas y organismos públicos de los gobiernos. Estas medidas buscan no sólo proteger los datos sensibles y a las infraestructuras críticas, sino también defender la confianza en las tecnologías que se utilizan en nuestra moderna sociedad.

La ciberseguridad y la IA están estrechamente relacionadas, y existen tanto desafíos como oportunidades en su intersección. Algunas de las aplicaciones más comunes de la IA en la ciberseguridad incluyen detección de malwares, análisis de tráfico de red para detectar patrones anormales, identificación de vulnerabilidades en los sistemas y redes, detección de phishing y ataques de ingeniería social y mejorar la respuesta a incidentes y la gestión de riesgos, entre otros. La IA es fundamental para analizar las amenazas cibernéticas e identificar patrones que pueden indicar una amenaza. Puede ser utilizada para analizar grandes cantidades de datos e identificar patrones que no serían visibles para los humanos. Algunas de las técnicas de análisis de amenazas cibernéticas que utilizan IA incluyen análisis de comportamiento de malware, análisis de tráfico de red para detectar patrones anormales, análisis de vulnerabilidades en los sistemas y redes, análisis de inteligencia de amenazas para identificar patrones y tendencias y más. La IA puede ser utilizada para mejorar la ciberseguridad, pero también plantea desafíos en cuanto a la privacidad y la seguridad de los sistemas. La IA plantea desafíos significativos en cuanto a la privacidad en la era digital. Puede ser utilizada para analizar grandes cantidades de datos personales e identificar patrones que pueden ser utilizados para violar la privacidad de los individuos. Algunos de los desafíos de privacidad que plantea la IA incluyen el uso de

datos personales para entrenar algoritmos de IA, riesgo de violación de la privacidad debido a la capacidad de la IA para analizar grandes cantidades de datos o la dificultad para controlar el uso de datos personales en entornos de IA. La detección de malware y ransomware es un desafío constante en la ciberseguridad. La IA puede ser utilizada para mejorar la detección de malwares mediante el análisis de patrones de comportamiento y la identificación de anomalías. La IA puede ser utilizada para analizar el comportamiento de los programas e identificar patrones que pueden indicar la presencia de malware.

El uso de IA en ciberdelincuencia ha dado lugar a varios incidentes de casos reales de fraude y ataques de IA notables, manifestando la creatividad y la peligrosidad. Uno de los ejemplos más impresionante de estafas impulsadas por IA fue por el uso de voz sintetizada (alterada) para imitar la voz del CEO de una empresa, solicitándole a un empleado que transfiriera dinero urgente. La cuenta también era fraudulenta.

El futuro de la IA en la ciberseguridad es prometedor, con avances en tecnologías como el aprendizaje automático y el procesamiento de lenguaje natural. Jugará un papel fundamental en la ciberseguridad en el futuro, permitiendo una detección y respuesta más efectivas a las amenazas cibernéticas. Es fundamental desarrollar estrategias para proteger la privacidad en la era de la IA, como el uso de técnicas de anonimización de datos y el desarrollo de algoritmos de IA que respeten la privacidad. En algún futuro cercano, habrá un mayor uso de algoritmos de aprendizaje automático para detectar y responder a amenazas cibernéticas, mayor desarrollo de sistemas de IA que puedan aprender y adaptarse a nuevas amenazas y un mayor enfoque en la privacidad y la seguridad de los datos en entornos de IA. Es fundamental continuar investigando y desarrollando la IA para mejorar la ciberseguridad y proteger contra amenazas cibernéticas. Frente a la sofisticación progresiva de los ciberataques con IA por ciberdelincuentes, es fundamental implementar estrategias de defensa. La ciberseguridad contra IA no solo debe ser reactiva, sino también proactiva, anticipándose a las amenazas antes de que ocurran. La implementación de tecnologías avanzadas y modernas, la educación en ciberseguridad de IA y una cultura de seguridad robusta son cruciales en este esfuerzo por detener la ciberdelincuencia.

CAPÍTULO V: "ASPECTOS CRIMINOLÓGICOS DEL CIBERCRIMEN"

V.I) Cibercriminología

El Dr. Kyung-Shick Choi[20] define a la Cibercriminología como la ciencia que busca estudiar las causas, factores y escenarios que permitan la realización del ciberdelito, o ciberdelito, cuyo objetivo es prevenir los delitos cometidos en el ciberespacio, o con la acción de las tecnologías de la información y la comunicación. Se refiere al uso extensivo de medios tecnológicos (informática) y comportamientos antisociales que se dan por el uso de un sistema electrónico como medio de comunicación, los cuales se configuran en Delitos Informáticos. Dentro de esta definición Cibercriminología, algunos autores proponen la criminología ciborg o cyborg criminology, entendido como un híbrido organismo y máquina (Arroyo, 2020) y entendido como "la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio" (Miró, 2012, p. 37).

Otros autores han definido a la Cibercriminología como el estudio de la causa de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico. En esencia, la Cibercriminología implica el examen del comportamiento criminal y la victimización en el ciberespacio desde una perspectiva teórica y criminológica (Jaishankar, 2011[21] y Jahankhani 2018[22]).

El profesor Abel González García (2020) dice:

> La criminología se ocupa del estudio de la delincuencia en todas sus vertientes y su fin primordial es ofrecer información científica para la prevención de este fenómeno. Además, en los últimos años, el campo de acción de esta ciencia se ha incrementado empujado por el avance tecnológico y por la propia dinámica en la que se encuentra la sociedad en la actualidad, inmersa en una revolución tecnológica como nunca antes se ha visto en la historia de la humanidad. Teniendo en cuenta estas premisas nace la Cibercriminología, como la parte de la criminología que se ocupa del estudio de la delincuencia en el ciberespacio y su relación con el mundo físico, la explicación de estos problemas y la propuesta de medidas preventivas eficaces. (p. 517)

Saín (2018) sostiene que las dos disciplinas que estudian los delitos informáticos son el Derecho Penal, que sanciona las acciones, y la Seguridad Informática, para

[20] Kyung-Shick, C.: *Cybercriminology and digital investigation*. LFB Scholarly Publishing, 2015.
[21] Jaishankar, K.: *Cyber Criminology: Exploring internet crimes and criminal behavior*. CRC Press, Taylor and Francis, Florida, 2011.
[22] Jahankhani, H.: *Cyber Criminoloy*, Springer, Londres, 2018.

prevenir. Si bien este punto de vista es válido, la realidad es que la Seguridad Informática sólo está presente en grandes empresas u organismos potencialmente blancos para cibercriminales. No existe, al día de la fecha, una Seguridad Informática que prevenga de todos los delitos informáticos para el común de todas las personas. Bajo este concepto, Pablo Palazzi (2000) sostiene que "cabe resaltar la magnitud de los daños, la cada vez más frecuente naturaleza global e internacional de esta clase de delitos; la facilidad para cometerlos".

De aquí debe, necesariamente, surgir la Cibercriminología para bajar a la Seguridad Informática, o Ciberseguridad, a todas las personas comunes que usen un celular, una consola de videojuegos, una computadora, en todo rango etario. Antes, es importante metemos en las distintas temáticas que hacen a la Cibercriminología, para entender el espacio propicio donde se encuentra la ciberdelincuencia.

V.II) El ciberespacio

Si bien es lógico pensar que el ciberespacio no es otra cosa que internet, existe una diferencia a la hora de utilizar estos términos. Hablamos de internet cuando nos referimos al componente físico a nivel de redes computacionales. En cambio, cuando hablamos de ciberespacio nos referimos a un quinto dominio que se suma a los otros (marítimo, aéreo, terrestre y electromagnético). Si bien este concepto del quinto dominio tiene un origen militar dentro de la incumbencia de la Defensa Nacional, tiene sentido hablar de este nuevo dominio donde las personas se relacionan y se cometen nuevas modalidades delictivas.

Se define al ciberespacio como un espacio de relaciones virtualizado a través de dispositivos electrónicos con conexión a internet. Esto es así, ya que es un espacio de comunicación social donde el alcance es global, que puede darse desde y hacia cualquier parte del mundo; es trasnacional, porque no existen barreras para la comunicación; es universal y popular, al ser utilizado en casi todo el mundo por la mayoría de las personas; se encuentra en permanente revolución tecnológica y, como característica más problemática, prevalece el anonimato. El anonimato permite que cualquier persona pueda ser quien quiera ser en internet.

A diferencia del espacio físico, donde tenemos un espacio y un tiempo determinado, el ciberespacio puede darse desde y hacia cualquier parte del mundo; y en cualquier momento del tiempo. Por ejemplo, hoy se puede programar un ataque informático para

que sea efectivo en 3 meses, desde Alemania hacia España. En el ciberespacio no hay espacio. No tiene espacio físico y, al mismo tiempo, está en todos lados.

En un espacio de relaciones físico, nuestros recuerdos almacenados en nuestra memoria se alteran o se pierden con el tiempo. En el ciberespacio, los datos no se borran. Son perennes (perduran en el tiempo).

Los caracteres del ciberespacio son:

- Deslocalización: No está situado en un lugar específico.
- Transnacionalidad: Para la comunicación, no existen barreras.
- Universal: Se utiliza en cualquier parte del mundo.
- Popularizado: La mayoría de las personas en el mundo lo utilizan.
- Neutralidad: Libertad total al transitar por el ciberespacio.
- Descentralizado: No existe una autoridad o servidor central.
- Anonimato: Cada persona puede ser quien quiera ser en la red.
- Abierto: Los usos cambian constantemente, porque
- Permanente revolución: Las tecnologías avanzan constantemente

Estas últimas dos características son una problemática, ya que, si bien hay modalidades delictivas que no son nuevas, siempre aparecen nuevas modalidades.

No existe la figura de un guardián del ciberespacio, de una policía del ciberespacio o alguien que regule o evite lo que pasa en él. Por eso, nosotros, los usuarios, somos las únicas personas que podemos configurar la seguridad de nuestros dispositivos electrónicos y evitar ser víctimas de la ciberdelincuencia.

V.III) Cibercrimen

Primero, es conveniente hacer una diferencia entre delitos informáticos y cibercrimen. Obviamente, esta definición varía entre distintos autores y fue mutando a lo largo del tiempo. Desde Argentina, Gustavo Sain (2017), dice:

> El cibercrimen no representa un tipo de criminalidad específica, no es parte del crimen completo ni organizado (…) Cuando se habla de delitos informáticos nos referimos a aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo. En este sentido, los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo. Si una persona intimida o intenta chantajear a otra persona

> vía correo electrónico, el dispositivo informático actúa como medio para cometer el hecho ilícito, siendo el delito de amenaza el hecho ilícito en sí. En el segundo caso, el dispositivo informático es el objeto o blanco del crimen, donde una persona puede enviar un virus a la computadora de un tercero y así dañarla a los fines de inutilizarla o alterar su funcionamiento. En este último caso la figura delictiva podría encuadrarse dentro del daño en tanto delito contra la propiedad, considerando el dispositivo informático como un bien tangible, tanto así como la información que puede almacenar. (Azzolin, H. y Sain, G, 2017, p.8)

Si analizamos a otros autores, Jaishankar distingue entre "delitos informáticos" y "cibercrimen" al señalar que los primeros se refieren a actividades ilegales que utilizan la computadora como medio o fin, mientras que el segundo término abarca un rango más amplio de delitos en línea, incluyendo aquellos que no involucran directamente la computadora, como la difamación cibernética. Miró Llinares, por su parte, refiere a los delitos informáticos como aquellos delitos que ocurren a diario, tipificados penalmente, pero que ocurren de forma independiente, individual o aislada, sin una organización y regularidad (por ejemplo, una persona que accede a la red social de su expareja; un empleado que borra información de su empresa; o realizar amenazas por Whatsapp) y entiende al cibercrimen como una serie de delitos informáticos que ocurren de manera más profesional, organizada, sin motivaciones personales más que las económicas, políticas o religiosas.

Marcelo Temperini (2018) sostiene que las víctimas personas de los delitos no suelen tener interés para el ciberdelincuente, ya que éste busca optimizar sus logros a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología. Si bien es posible encontrar ciberdelincuentes especializados que trabajan de forma independiente, es más común encontrarlos organizados en bandas, con una clara distribución de tareas. También hay que tener en cuenta la diferencia entre delito y crimen, la cual un crimen es un delito grave, con altas penas de prisión y que atenta contra la moral de las personas. Un crimen es un delito, pero no todos los delitos son crímenes.

En mi opinión, teniendo en cuenta la frase anterior, no todo delito informático es cibercrimen. Se entiende que las unidades de investigación sean en “cibercrimen” para investigar todos los delitos informáticos, pero claro está que no podemos comprar un caso de extorsión y amenazas en grooming, con una operación de DDoS. Tampoco podemos comparar un caso de ingeniería social, donde el atacante se hace pasar por el Ministerio de Salud, con un descuido personal en las medidas de seguridad al descargar un programa

de un sitio no oficial o crackeado, que nos instala un malware internacional que nos roba algunos datos, donde los pesos argentinos no les sirven para nada. Por un lado, tenemos un delincuente que busca a su víctima. Por otro lado, la víctima fue hacia el delincuente. Dicho esto, definiría a los delitos informáticos como aquellos delitos tipificados en el Código Penal, mientras que el cibercrimen son todas las operaciones delictivas (individuales o grupales) con una clara organización y objetivo concreto, donde también pueden aparecer varias figuras penales.

Según el FBI, las organizaciones cibercriminales funcionan como empresas, y cuentan con expertos especializados para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana.

Cuando hablé de la criminogénesis de la delincuencia, vimos que Cohen y Felson señalaron que el origen de la conducta criminal se desencadena por la convergencia ocasional de tres elementos: un delincuente motivado, una víctima accesible y la ausencia de elementos de protección. Es decir que el crimen se provoca cuando se unen, en un espacio y tiempo determinado, un objetivo, un delincuente motivado y la ausencia de un guardián capaz de darle defensa al objetivo. El gráfico de la confluencia de estos tres elementos lo denominaron “triángulo del crimen”.

Si bien en el ciberespacio se ven modificados los parámetros espaciotemporales, no sólo éstos pueden incidir en una modificación de los condicionantes del delito, sino que el campo de la oportunidad criminal es aún mayor, gracias a la inexistencia de barreras. Se puede atacar a varias víctimas en un mismo instante, en distintas partes del mundo, con una sola acción (un clic). Existe una reducción del tiempo y espacio para la llegada y la huida, tal como el ejemplo que detallé en la introducción de este trabajo, donde ya no se tiene que pensar en cómo entrar a robar, cómo robar, que artilugios utilizar, qué personal reducir y cómo escapar de la policía. Tampoco se requieren de grandes insumos para cometer el delito, sino que con mínimos recursos (una computadora) se pueden generar grandes daños sin salir de casa y manteniendo un anonimato difícil de rastrear.

Los blancos u objetivos del cibercrimen también sufren una modificación. Primeramente, existe un gran contacto a víctimas y poca resistencia a los ciberataques. Los conceptos de ciberseguridad aún son muy lejanos para la mayoría de las personas y, por consecuencia, los dispositivos quedan desprotegidos. En el caso de una víctima persona, no entran todos sus bienes, es decir que no se ataca a la vida o a la salud, pero esto es

discutible, ya que hemos visto que existen delitos contra la integridad sexual que se cometen a través de internet. Además, hay algunas acciones maliciosas que generan un gran tormento para la vida de la víctima, como por ejemplo la ciberextorsión, la difusión no consentida de imágenes y videos íntimos, el ciberacoso y el ciberbullying. También hay que tener en cuenta que la víctima es quien decide incluir o no información personal y compartirla, como realizar actividades económicas, dónde navegar, qué descargar, qué exponer y a quién tener en las redes sociales.

Por otro lado, el valor de cosas cambia en el ciberespacio. Por ejemplo, una contraseña no tiene valor comercial. Uno no puede ir a comprar la contraseña del homebanking de una persona tan libremente, pero sí se puede comprar de forma ilegal y tiene gran valor en el ciberespacio. Mientras la persona sea más importante, tendrá más valor y habrá más probabilidades de que sea ciberatacada.

No existe la figura de un guardián y es por ello que el elemento para consumar el delito es justamente esa ausencia. La protección depende de la víctima y de las organizaciones. Nosotros somos nuestros propios autoguardianes, la "capa 8". El control suele ser familiar (aplicaciones de control parental) o institucional. La actuación policial es reducida y solamente está focalizada en la investigación de una causa puntual posterior a la consumación del delito. No existe una prevención policial y el control social es reducido.

También, hay que tener en cuenta que, mientras más cosas se pueden hacer en el ciberespacio a nivel trasnacional, menos será la capacidad de protección, debido a la amplitud de acciones que se pueden realizar. A esto se le suma la constante evolución tecnológica, que complica las protecciones, ya que siempre surgen usos nuevos.

Por último, en el año 2001, se firma en Budapest (Hungría) el Convenio sobre la ciberdelincuencia en el seno del Consejo de Europa ante la necesidad de "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos…". El Convenio establece diferentes tipos del delito en la esfera de la cibercriminalidad como modelo legislativo, tanto en el ámbito de derecho penal como procesal penal; principios generales de cooperación entre los diferentes países en materia judicial y procedimientos vinculados a la investigación criminal.

V.IV) Tipos de cibercrímenes

En este apartado, me resultó interesante analizar las posturas de 2 autores. Por un lado, Miró Llinares, que clasifica al cibercrimen según el ciberataque (puro, réplica y de

contenido) y según el motivo (económico, social y político). Por su parte, Aldo R. Valdez Alvarado habla de dos grandes grupos, los cibercrímenes violentos o potencialmente violentos y los no violentos.

En un sentido amplio, Valdez Alvarado (2012) dice que los cibercrímenes violentos o potencialmente violentos "pueden realizar daño físico a alguna persona o personas". Dentro de esta categoría, incluye al ciberterrorismo, amenazas de ataques, la pornografía infantil y el -muy debatible- ciberespionaje. Desde mi punto de vista, el ciberespionaje se encuentra en la mayoría de los ciberataques y, en muchas ocasiones, forma parte de una etapa previa y silenciosa (no violenta) de un ataque concreto posterior más dañino, como puede ser un ransomware, una denegación de servicios o el robo de información confidencial.

En cuanto a los cibercrímenes no violentos, sostiene que "La mayoría de los cibercrímenes son crímenes no violentos debido al hecho de que la principal característica de este mundo en línea es la capacidad de interactuar sin necesidad del contacto físico" (Valdez Alvarado, 2012) e incluye figuras como ciberviolaciones, ciberrobo, ciberfraude, cibercrímenes destructivos, publicitar o solicitar servicios de prostitución en Internet, apuestas, venta de drogas, lavado de dinero y cibercontrabando. Con esta definición, no sólo confirmo mi desacuerdo con la figura violenta del ciberespionaje, sino que percibo una acción violenta en las ciberviolaciones, entendiéndola como posibles casos de grooming.

Por otra parte, Miró Llinares (2012) clasifica a los distintos tipos de cibercrímenes desde una perspectiva criminológica más exhaustiva, que a continuación se enuncian:

<u>Según el ciberataque</u>

- Cibercrimen puro: Objetivo hacia sistemas informáticos de alterar, destruir, inutilizar archivos, dispositivos o sistemas. Uso de la informática como medio y como fin. Aquí encontramos al hacking, algunos malwares, ataques DoS, DDoS y exploits.
- Cibercrimen réplica o físico: El uso de la informática como medio para cometer el delito y la víctima puede tener un daño en el plano físico (offline). El ataque no se realiza hacia un dispositivo electrónico, ni tampoco es la información el objetivo de este, sino que la red de internet es el nuevo medio a través del cual se comete un delito que utilizaba anteriormente otros medios para consumarse. Son réplicas de crímenes que ya se realizaban en el espacio físico, pero adaptadas al ciberespacio. Aquí encontramos a

delitos como la estafa informática (phishing, vishing), ciberextorción, sextorción (ambas entendidas legalmente bajo el tipo penal de la extorsión) y grooming. También, algunas acciones que no existen como delito en nuestro país, como el spoofing ciberespionaje, cyberstalking, cyberbullying y ciberacoso.

- Cibercrimen de contenido: El objetivo es comunicar o poseer algo indebido. Uso de la informática para la difusión u obtención no consensuada de imágenes íntimas, conversaciones, material de abuso sexual contra las infancias (MASI, mal llamada "pornografía infantil"), ciberpiratería, difusión de contenido ilícito (online hate speech - odio racial).

La difusión no consentida de imágenes o videos íntimos (dependiendo del motivo, también llamado "pornovenganza") es la publicación o puesta a disposición, o la amenaza de hacerlo, al público en general o de terceros en particular, de forma deliberada, utilizando internet u otra tecnología de la comunicación, de imagen/es, o audio/s o contenido/s audiovisuales de naturaleza sexual explicita, sin el consentimiento de la víctima, por parte de un individuo con el que ésta mantuvo una relación íntima. Esta problemática la retomaré más adelante.

Con respecto al MASI, hay una problemática en cuanto a la facilidad de descarga, de entablar relaciones, de intercambios, sexting, posibilidad de anonimato y un mercado global de forma inmediata. Hay una deslocalización de las fases del proceso, que significa que no es igual el lugar donde se obtienen las imágenes, de subida o alojamiento y de consumo. Existen webs pagas con tarjeta de crédito, chats en tiempo real, intercambio por correo electrónico, compra directa, grupo de noticias o foros, asociaciones de consumidores e intercambio, p2p y mafias organizadas con división de competencias y creación de contenido.

La ciberpiratería son formas de explotación ilícita de obras protegidas. Industrias de música, películas, videojuegos y libros afectadas con pérdidas de dinero por el intercambio gratuito de archivos (P2P Ares o Emule, Torrent, streaming, Mega, Mediafire). Está penado en muchos países, pero no en Argentina. Además, siempre hay riesgo de descargar malware.

El online hate speech o discurso de odio en línea son mensajes que se llevan a cabo en ciberespacio, con el propósito de atacar a una persona o un grupo sobre su raza, religión, orientación sexual, discapacidad o género. Es la difusión del odio online con mensajes racistas y violentos. Gran presencia en redes sociales. Es global, de difícil

persecución y anónimo. Si bien podemos imaginarnos insultos por forma de pensar o política en un grupo de Facebook, tiene más relación con el ciberterrorismo, por ejemplo, cuando el ISIS sube videos decapitando gente.

Según el motivo

- Cibercrimen económico: El dinero es la principal causa de la mayoría de los ciberataques. Incluso si estamos ante un caso de grooming, puede pasar que el groomer esté recolectando imágenes para después venderlas. Los ataques a las grandes empresas u organismos estatales mayormente se realizan con ransomwares, donde se exige un pago para el rescate. No es sólo un tipo de ataque delictivo que afecta al patrimonio de las personas o a un sistema económico en Internet. También se asocian todos los ciberataques cuyo objetivo final es el logro de un beneficio económico, aunque afecten a otros bienes jurídicos como la intimidad, la seguridad de los sistemas y redes, etc. El cibercriminal económico utiliza la red, los sistemas conectados a ella, la información contenida, los servicios y cualquier otro elemento de los dispositivos electrónicos como medio u objeto para el beneficio económico, así sea crear una cadena de ataques con el mismo fin.
- Cibercrimen social: Vimos como el ciberespacio permitió que nos podamos comunicar con cualquier persona en cualquier parte del mundo. Las redes sociales en particular e Internet en general forman, hoy en día, un nuevo ámbito de desarrollo personal, un nuevo espacio vital en el que cada individuo pasa varias horas al día, se comunica con otros, crea relaciones, etc. Todas las esferas personales que, al relacionarse con los demás, pueden ser puestas en peligro, lo están también en el ciberespacio; y todas las conductas criminales de ataque a las personas que no requieran de una inmediatez física también se realizan por medio de Internet. Por ejemplo, la violación de la intimidad personal, y no sólo como parte del cibercrimen económico como medio para la consecución del futuro fraude, sino con el mero fin de desvelar secretos personales y dañar la intimidad de la víctima, se muestra como conducta delictiva en el ciberespacio debido a la enorme cantidad de información personal que la gente coloca y comparte en sus redes sociales. Todas las formas de acoso de una persona o grupo de personas a otra también mutaron al ciberespacio. Con el simple uso del correo electrónico o redes sociales para enviar mensajes ofensivos contra la víctima, o que permiten tanto la exclusión de un sujeto por parte de un grupo, como la creación de perfiles falsos y la difusión de imágenes, vídeos y textos respectivos a la víctima con el objetivo de ofenderla y dañar su imagen o su dignidad. En

esta categoría también entran las modalidades vistas como grooming, ciberacoso, ciberbullying, difusión no consentida de imágenes o videos íntimos o conversaciones, etc.

- Cibercrimen político: En esta categoría, el motivo no es conseguir un beneficio económico ni tiene que ver con el uso de internet en nuestra vida social, sino que es la aplicación de la informática para la aplicación de políticas por parte de estados u organizaciones. Internet se convirtió en un instrumento para la lucha política o ideológica de muchas formas distintas: como forma de captación ideológica, como medio para el ataque a servicios estatales o institucionales, y es un medio de comunicación entre individuos o grupos separados geográficamente, pero unidos por una misma propósito político o ideológico. Dentro de esta categoría, definimos al ciberterrorismo, al ciberhacktivisimo y a la ciberguerra. El terrorismo son actos de violencia ejecutados para infundir terror, inseguridad o intimidación con fines políticos o religiosos. El ciberterrorismo es el terrorismo que utiliza el ciberespacio. El uso de las tecnologías de la información (sistemas informáticos) con fines de intimidar, coaccionar o causar daños con fines políticos o religiosos. Algunos objetivos son: búsqueda de mayor daño y difusión posible, difundir mensajes de violencia e incitación al terrorismo, reclutamiento, adoctrinamiento, sensación de pertenencia, realización de ataques informáticos a objetivos sensibles del Estado para dañar o inutilizar dispositivos. Con fines de recaudar fondos, existen casos de phishing producidos por ciberterroristas. El ciberhackitivismo es el activismo político en Internet. Son ataques llevados a cabo por hackers para lanzar mensajes ideológicos, de lucha política o defensa de ideas relacionadas con la libertad en Internet. No tiene fines económicos o para causar daños. Se llevan a cabo por intrusiones en sistemas y redes de una actividad política dirigida contra empresas o estados. La ciberguerra es la agresión informática por parte de un Estado. Los objetivos pueden ser: dañar un sistema informático, interrumpir o romper el flujo de información, destruir físicamente la información, reducir la efectividad de los sistemas de comunicación, impedir acceder y utilizar los sistemas informáticos, engañar al adversario con falsa información, acceder al sistema del enemigo para robarle información, entre otros.

V.V) Ciberguerra

La incorporación de las computadoras (ordenadores) y la conformación de redes en la sociedad en general, y en las organizaciones militares en particular, han dado una nueva configuración a la forma de relacionarse desde lo interpersonal hasta lo global. Esta nueva

realidad conlleva el surgimiento de nuevas fortalezas y debilidades de los actores presentes en un escenario de conflicto armado. Si consideramos el sostenido crecimiento de usuarios de Internet, este incremento trae aparejado también como correlato una mayor vulnerabilidad de las redes de las Fuerzas Armadas a ataques, por lo cual es innegable que las guerras del siglo XXI serán diferentes de las que caracterizaron al siglo XX.

El ciberespacio presenta una posibilidad de combate ilimitado. Su incidencia en ámbitos propios de la Defensa provocó que el Departamento de Defensa de Estados Unidos emitiera el Documento "Estrategia para Operaciones en el Ciberespacio" (2011), donde señala que "El Departamento de Defensa está particularmente preocupado por tres áreas de la actividad de confrontación potencial: el robo o la explotación de los datos, la interrupción o denegación del acceso o servicio que afecta a la disponibilidad de redes, información o recursos de red con capacidad y acción destructiva como la corrupción, la manipulación o la actividad directa que amenaza con destruir o degradar las redes o dispositivos conectados".

La ciberguerra es el uso de ciberespacio por Fuerzas Armadas, como nuevo ámbito en las guerras del siglo XXI. Impondrá cambios para optimizar su empleo en forma disuasiva o efectiva para enfrentar agresiones que provengan de él, entre los cuales podemos señalar cambios culturales de los recursos humanos para gestionar y actuar en este ámbito; y cambios en las capacidades militares necesarias para identificar, ejecutar y sostener operaciones en este ámbito, de acuerdo con las misiones que se le asignen. A diferencia con la guerra física, la ciberguerra provoca menos daños físicos a soldados, tiene mayor espacio de combate, posee menor densidad de tropas, es una lucha intensa por la superioridad de la información y requiere mayor exigencia a las personas para detener los ataques informáticos.

Si nos basamos en las definiciones de la palabra "guerra" de la Real Academia Española y analizando los planteos de los autores, podemos afirmar que existen múltiples guerras (militares y no militares) en múltiples dominios. El desafío lo encontraremos a la hora de analizar los motivos de guerra y la integración de los dominios para alcanzar la victoria. Si tenemos un objetivo claro, con una estrategia sólida que abarque una combinación de operaciones en múltiples dominios, más fácil resultará llegar a la victoria. Por ejemplo: si un país le declara la guerra a otro, no será lo mismo limitarnos a un combate terrestre, que extender nuestra estrategia hacia el dominio marítimo, de aire, espacial, ciberespacial, económico, psicológico, de inteligencia y social. Una simple fakenew

(noticia falsa) puede resultar desorientadora para el oponente. El problema radica en que, si estamos hablando de conflictos bélicos, se requiere de personal militar altamente capacitado en múltiples dominios, no sólo limitarnos en los dominios terrestre, aire y mar. Lo seguro es que la guerra tiene un objetivo limitado con "campos de batalla" limitados. Nunca podría ser ilimitada, ya que los objetivos y los recursos siempre serán limitados.

Quiao Liang y Wang Xiansui en su libro "La guerra más allá de los límites" (1999) plantean la existencia de múltiples guerras, tanto militares, trans-militares y no militares. Estoy completamente de acuerdo con la idea de la existencia de múltiples guerras. Por ejemplo, si una persona se encarga de difamarme por redes sociales, no existirá una guerra militar, pero sí un conflicto entre dos personas y podrá generarse una lucha ya sea en tierra o en el ciberespacio.

Fernando Miró Llinares, en su libro "El cibercrimen", define al Ciberespacio como un espacio de relaciones virtualizado (mediante sistemas informáticos o dispositivos electrónicos con internet) con alcance global. Esto nos indica que el ciberespacio es un dominio de guerra, sea cual sea el motivo de la guerra y de implicancia militar o no militar.

Por mucho tiempo se consideraron tres "Dominios" del "Campo de Batalla": tierra, mar y aire. "Espacio Exterior" y "Ciberespacio" se agregaron a los otros 3 dominios ya existentes. Cuando se habla sobre la multiplicidad de dominios, lo que se plantea son los tipos de límites en los modelos de nuestra línea de pensamiento. Si nos alejamos un poco del pensamiento tradicional de los 5 dominios (tierra, mar, aire, espacial y ciberespacial) y nos paramos desde el punto de vista multidominio, podemos darnos cuenta de que muchos dominios pueden estar afectados por la guerra. Si tomamos en cuenta el conflicto actual entre Rusia y Ucrania, podemos ver claramente cómo la guerra afecta no sólo al ámbito militar entre los 2 países, sino también a la economía mundial. Si tomamos los múltiples dominios que están afectados por la guerra y los convertimos en cartas de juego, si se utilizan hábilmente, se pueden crear estrategias y tácticas para combinar todos los recursos de la guerra, y así lograr la victoria.

Las actividades de información afectan al carácter o al comportamiento de las personas, mediante el uso de la información, para influir en sus percepciones y su comprensión, y abarcan un amplio espectro de actividades diseñadas para afectar a una audiencia objetivo en tres aspectos: sus capacidades, su comprensión y su voluntad. Para ello, estas actividades intervienen en el plano psicológico.

Liang y Wang Xiansui también plantearon los dominios de la energía, de las finanzas internacionales, de la tecnología, de la psicología social y de la comunicación social. Teniendo en cuenta que este libro se escribió hace décadas atrás, está claro que los autores tenían una visión de los avances tecnológicos que se avecinaban y de cómo afecta la guerra en la sociedad, más allá del conflicto militar.

Si vemos a los distintos dominios como piezas de ajedrez, podemos utilizarlos inteligentemente para lograr vencer a nuestro oponente. Con objetivos claros, definidos y una estrategia sólida, podemos combinar los múltiples dominios, generando múltiples ataques desde distintos ámbitos, múltiples defensas, desorientaciones. Para lograr esto, se requiere de personal altamente capacitado. Es extender el pensamiento limitado de que los dominios son aire, tierra y mar; y preparar militares para una guerra "más allá de los límites", que pueda combatir en dominio ciber, en dominio financiero, en dominio de la comunicación social, en dominio de la psicología social, en dominio de la tecnología, etcétera. Esto implica un gran desafío para la Defensa Nacional Argentina y una gran exigencia de personas altamente formadas en múltiples disciplinas que se deberán integrar.

En la ciberguerra propiamente dicha, donde tenemos un conflicto entre Estados, los ciberataques no tienen el objetivo que comúnmente solemos estudiar. Tengamos en cuenta que, cotidianamente, los ciberataques tienen una motivación económica para los delincuentes. En la ciberguerra, no. El motivo es político. Aquí entran operaciones de ciberespionaje y de destrucción de sistemas informáticos.

El Manual de Tallin es un estudio académico sobre cómo debe destinarse el derecho internacional a los ciber-conflictos y la guerra cibernética. Fue escrito entre 2009 y 2012 en el Centro de Excelencia en Defensa de la Ciberdefensa Cooperativa de la OTAN con sede en Tallin por un grupo internacional de alrededor de veinte profesionales. El manual fue publicado por Cambridge University Press en abril del 2013 y está enfocado a la aplicación del derecho internacional humanitario de los conflictos armados a los ciberataques. Integra el concepto de la "responsabilidad penal internacional" (Kain Ambos, 2015) suponiendo la existencia y la participación de crímenes internacionales.

V.VI) Violencia digital

Resulta conveniente definir a las acciones atípicas, como aquellas acciones o conductas que no están tipificadas en el Código Penal. Es decir, que no son delito. Esto genera

un verdadero problema, ya que libra a las personas a que cometan acciones que generen un verdadero tormento en la vida de una persona. Estas acciones son: difusión no consentida de imágenes o videos íntimos, porno venganza, ciberstalking, ciberbullying y el ciberacoso.

El sexting, también llamado sexo virtual, es la práctica consensuada de enviar o recibir imágenes o videos sexuales. Conducta lícita, tratándose de una natural y legítima manifestación de la libertad sexual de las personas. La práctica abarca a personas adultas y menores, pero hay predominio entre menores. Consiste en la autoproducción de archivos de imágenes y videos, protagonizados por ellas mismas, en actividades sexuales explícitas o exhibiendo sus partes genitales con fines predominantemente sexuales, para su posterior difusión o facilitación a terceros.

Las problemáticas que trae el sexting son:

- Cuando es entre menores: Pornografía infantil. Grooming, cuando, por ley, se chatea con una persona menor de edad con fines sexuales. El art. 128 (C.P.) que pena al que tenga, produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere.
- Hacking: Acceso al dispositivo y robo de contenido
- Difusión no consentida de imágenes o videos íntimos o la Pornovenganza
- Sextorsión

La violencia es el uso de la fuerza o del poder en contra de una persona, grupo, o comunidad y que causa lesiones, muerte, provocaciones o abandono. No implica sólo maltrato físico como acción, sino que la violencia psicológica y la violencia por omisión también son parte de este concepto integral. La violencia de género digital es el tipo de violencia cometida contra cualquier persona o grupo de personas por su sexo, género, orientación o identidad sexual en entornos digitales. Dentro de este tipo de violencia, diferenciamos las acciones típicas que son delito (hacking, violación de secretos y de la privacidad, sextorsión, discurso de odio/discriminación), de las atípicas (difusión no consentida de imágenes y/o videos de índole sexual, pornovenganza, ciberstalking, ciberbullying y ciberacoso). A continuación, veremos algunas conductas no mencionadas anteriormente.

Difusión no consentida de imágenes o videos íntimos

Subir al ciberespacio imágenes y/o videos que atentan directamente contra la libertad, la privacidad y dignidad de una persona, sin su consentimiento o autorización. Motivaciones: represalia, resentimiento, extorsión, venganza o sentimientos de apatía respecto de sus exparejas o relaciones ocasionales de intimidad. Es la publicación o puesta a disposición al público en general o de terceros en particular, de forma deliberada, utilizando internet u otra tecnología de la comunicación, de imagen/es, o audio/s o contenido/s audiovisuales de naturaleza sexual explicita, sin el consentimiento de la víctima, por parte de un individuo con el que ésta mantuvo una relación íntima. Los motivos de quienes ejercen esta práctica espuria podrían resumirse en tres grandes grupos:

1) Humillar públicamente (que suele ser el motivo más común),

2) Lucrar con las imágenes de las afectadas y

3) Extorsionar a la víctima para sacar provecho de índole económico o sexual a cambio de no divulgar la información.

El Senado de la Nación dio media sanción al proyecto de ley en el que se penaliza la "publicación y/o difusión de imágenes no consentidas de desnudez total o parcial y/o videos de contenido sexual o erótico de personas", incorporando un nuevo artículo al Código penal (el 155 bis) cuyo texto es el siguiente: "Será reprimido con la pena de prisión de seis (6) meses a cuatro (4) años, el que hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, sin el expreso consentimiento de la o de las mismas para tal fin, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video (...)"

Ciberstalking

Uso de dispositivos electrónicos con internet para hostigar, perseguir o amenazar a alguien. Consiste en una mezcla de distintas formas de acecho a través de distintos medios, como el chat, foros, redes sociales, etc. Se sustituyen las llamadas de teléfono o las visitas al trabajo y a la casa o los seguimientos no deseados, por otras conductas como el envío de muchos correos o mensajes a través de redes sociales, la exposición público o difusión de fotos, mensajes o correos de la víctima en páginas webs o redes sociales. El cyberstalker elije a su víctima y realiza una o distintas formas de persecución, como

intentar contactar en repetidas ocasiones, amenazar, solicitar sexo de forma explícita, enviar imágenes sexuales, entre otras. Muy relacionado con el ciberacoso y tampoco es delito.

Ciberacoso y ciberbullying

El ciberacoso es el acoso a través de Internet y dispositivos electrónicos, que comprende amenazas, hostigamiento, humillación, molestias y atormento. El acoso sexual consiste en reiteradas solicitudes de actividad sexual con una persona que las está rechazando. Requerimientos verbales o escritos para tener relaciones sexuales con alguien que ya ha manifestado que no quiere. Insistir en realizar actos sexuales haciendo uso de conductas coercitivas, intimidantes o humillantes. Generalmente, es reiterativo y hacia mujeres. Un ejemplo claro de ciberacoso es recibir una foto íntima de alguien que no conocemos o no hemos solicitado.

Por tal motivo, el grooming es abuso y no ciberacoso, como comúnmente se lo llama, ya que el abuso comprende la incapacidad para consentir. Ya sea por manipulación, engaños, minoría de edad, inmadurez sexual, enfermedades mentales o estados de inconsciencia (sueño, borrachera), la víctima es incapaz de darse cuenta de que está siendo víctima de un delito y, por ende, de manifestar el consentimiento o no.

El ciberbullying es similar al ciberacoso, pero en entorno escolar. Hay grandes probabilidades de que continúe el bullying físico en el colegio. Genera un daño psicológico de forma voluntaria y repetitiva.

Ambas figuras no constituyen delito en nuestro país.

Ciberextorsión y sextorsión

Entendidas como una forma de extorsión “tradicional” pero con el uso de las TIC. La diferencia con la sextorsión es cuando se extorsiona particularmente con publicar fotos o videos íntimos de una persona, sin consentimiento, a cambio de más material pornográfico o, por ejemplo, que un exnovio amenace a su exnovia para volver a estar juntos o realice alguna determinada acción. La extorsión es la conducta por la que se obliga a una persona, mediante el uso de la violencia o intimidación, a realizar u omitir algún acto en perjuicio propio o ajeno. Por lo general, el motivo principal es económico. En internet, la ciberextorsión consiste en el mismo acto, de uso de violencia o

intimidación, aplicada a través de sistemas informáticos (hackers que piden dinero a cambio de publicar información o archivos, ransomware, grooming).

Otro caso de ciberextorsión tenemos en el grooming, cuando el groomer comienza a extorsionar a su víctima con publicar o difundir el contenido íntimo a sus amigos o a sus familiares, con el objetivo de exigirle aún más material íntimo.

Violación de secretos y privacidad

El delito dice "el que abriere o accediere indebidamente (...); o se apoderare indebidamente (...); o indebidamente suprimiere o desviare de su destino (...) una comunicación electrónica que no le esté dirigida." Esto implica que se puede ejercer violencia digital accediendo indebidamente a llamadas, correos electrónicos, mensajes de texto o por aplicaciones de mensajería instantánea (WhatsApp, Telegram, Facebook) sin la autorización de la víctima.

V.VI) Perfiles cibercriminales

Desde una perspectiva criminológica, el estudio del sujeto que comete el delito reviste de una especial importancia para una adecuada política preventiva. Pese a que todo estudio criminológico debe tener en cuenta las circunstancias concretas del fenómeno criminal y de la persona del criminal, la identificación de "perfiles" puede ser una técnica eficaz para introducir políticas de seguridad y posterior identificación de los delincuentes. Por otra parte, el estudio de determinados tipos de comportamiento, asociados a perfiles socioeconómicos concretos, ha arrojado algunas conclusiones importantes en el campo de la prevención delictiva. Así, por ejemplo, estudios como el realizado por SHAW (2006), arrojan sugerentes postulados sobre el papel general de los patrones de comportamiento, pues en muchos casos estos formaron la base de la investigación para determinar y evaluar las conductas de los delincuentes cibernéticos. Así, el estudio del cibercriminal puede ser relevante para comprender la naturaleza y el modus operandi que requieren los diferentes delitos informáticos, además de ayudar a la identificación de los autores cuando aún son desconocidos para los medios de control social formal; incluso, teniendo en cuenta las especificidades de esta clase de criminalidad, el estudio de perfiles puede coadyuvar a la detección de los riesgos dentro de una persona jurídica o para comprender el funcionamiento de las organizaciones delictivas que se dedican a este tipo de delitos.

Por otra parte, considero aún más importante poner el foco en las víctimas del cibercrimen, básicamente porque nosotros somos la "capa 8", la capa más vulnerable, donde los criminales van a querer atacar. Ningún ataque por malware se daría por descargar (involuntariamente) un software y ninguna estafa se consumaría si las personas no cayeran. Entonces, ¿Por qué las personas seguimos siendo víctimas? ¿Por qué es tan fácil para los ciberdelincuentes?

En cuanto a los rasgos psicológicos, hay muchos tipos diferentes de personalidades presentes entre los cibercriminales. Cámara Arroyo (2020) sostiene que, generalmente, aquellos más especializados en el dominio de la informática son extremadamente creativos, brillantes, agudos y audaces, rebeldes y soñadores. Les resulta más satisfactorio tratar de aprender experimentando que mediante el estudio tradicional. Algunos pueden mostrar rasgos que denotan timidez e, incluso, tendencias misantrópicas, pero estos desaparecen en sus intensas relaciones en el ciberespacio: les resulta más sencillo relacionarse con otros de manera electrónica (a través de chats, foros, redes sociales, etc.), mientras que no se sienten completamente cómodos en una sola persona. La protección y el anonimato del ciberespacio puede explicar esta clase de comportamiento social. La presencia de patologías o trastornos de la personalidad no es frecuente, como en la mayor parte de la delincuencia tradicional. De hecho, es habitual que sus habilidades de autogestión se encuentren más desarrolladas que la media. No obstante, es posible encontrar algunos supuestos en los que se han detectado rasgos psicopáticos o trastornos de la personalidad. Uno de los rasgos psicológicos que más se destaca es la tendencia a la paranoia de esta clase de criminales. Estos sentimientos son causados por el miedo constante a la detención y la incertidumbre causada por no saber con quién está tratando online. Es frecuente el insomnio, al alternar sus actividades nocturnas en el ciberespacio con sus ocupaciones diurnas.

Fanjul Fernández (2018) sostiene que no es excesivamente frecuente el uso de estupefacientes o el abuso del alcohol, aunque podría existir consumo de las denominadas drogas "blandas" (cannabis). Solamente los menos cualificados entre los hackers abusan de estas sustancias, dado que la falta de claridad mental les impide realizar un ataque sin cometer errores y evita que alcancen los niveles más altos de sus capacidades técnicas.

En lo atinente a las relaciones y antecedentes familiares, la existencia de un mayor desarraigo o debilitación de los vínculos es superior a la media: padres ausentes o excesivamente protectores, familias desestructuras o disfuncionales, falta de atención o

métodos de crianza pobres, etc. En algunos casos, esto puede explicar el refugio del sujeto en el ciberespacio y la dedicación a la adquisición de sus aptitudes y conocimientos en el campo de la informática. Uno de los métodos de crianza deficientes que se observan en la mayor parte de los supuestos es que a los padres no les importa lo que sus hijos hacen con sus ordenadores, no existiendo control al respecto.

Respecto a las relaciones con los pares, frecuentemente no se sienten aceptados por sus compañeros, experimentando cierto sentimiento de abandono. Prefieren lidiar con las computadoras, ya que las computadoras no son críticas y no discriminan. Sin embargo, esto se torna completamente distinto en el ciberespacio, donde pueden pertenecer a subculturas y comunidades clandestinas, con las que comparten valores e intereses comunes, desarrollando un sentimiento de pertenencia. En estos grupos contraculturales pueden desarrollar nuevas escalas de valores y obtener referencias morales que difieran con las habituales en el mundo físico.

Los ciberdelincuentes pueden provenir de cualquier estrato social y pertenecer a cualquier clase socioeconómica. Aunque algunas investigaciones indican que los delitos informáticos como la piratería informática son más frecuentes en las clases sociales altas, lo cierto es que el ciberespacio es un lugar, hasta cierto punto, libre de los condicionamientos de las clases sociales tradicionales o, al menos, ejerce un efecto nivelador. Ciertamente, como ya hemos tenido oportunidad de exponer, existen algunas diferencias en el acceso a los medios tecnológicos, pero actualmente incluso en los sustratos sociales más humildes es posible el acceso a aparatos informáticos o una conexión a Internet.

En cuanto a su nivel educativo, tampoco existe homogeneidad: si bien la mayor parte de los cibercriminales son curiosos y están dispuestos a aprender, esto no significa necesariamente que quieran hacerlo a través de los medios tradicionales. Muchos cibercriminales han tenido altas cotas de fracaso escolar o, directamente, han abandonado sus estudios formales para dedicarse a aprender sobre lo que realmente les interesa. En los estudios realizados hasta la fecha, los datos arrojan la evidencia de que, en la mayor parte de los casos, los hackers tienen un nivel de estudios algo superior a la media de la población.

Habitualmente se suele hablar de menores víctimas de los delitos cometidos a través de las nuevas tecnologías de la comunicación. Sin embargo, en los últimos años también se ha evidenciado la tendencia de algunos menores a ser también victimarios, es decir, autores de esta clase de delito (Vidal Herrero-Vior, 2016). La razón, por lo demás,

es bastante conocida: los jóvenes tienen un mayor acceso a esta clase de tecnologías y, además, muchos de los delitos que cometen los menores de edad tienen como víctimas a otros menores de edad, frecuentemente pertenecientes a su grupo social cercano. Los menores suelen aparecer como autores de los denominados delitos informáticos en general, es decir, de los ilícitos realizados con el ordenador y que tienen como principal objetivo otro terminal.

En cuanto a la necesidad de cualificación técnica en materia de programación o telecomunicaciones, el estudio arrojaba algunos datos interesantes: en la mayor parte de los casos, se trataba de personas que tienen un mediano o alto conocimiento de computadores y redes en general, así como de sujetos con conocimientos en cómputo por encima del promedio (cambio de IP, uso de programas Keyloggers, uso de navegadores inusuales, etc.). Como puede apreciarse, no se hace mención del conocimiento técnico de confección de herramientas informáticas para la comisión de hechos delictivos, sino que el estudio se centra en el conocimiento acerca del mero "uso" de las diferentes vías que permiten la comisión de cibercrímenes.

La comisión de una gran parte de estos delitos no requiere de un conocimiento técnico avanzado. Cualquier persona con una conexión a Internet puede desarrollar una actividad delictiva o criminal. Basta con tener el conocimiento necesario para utilizar tales herramientas. En ciberseguridad, existe el concepto SaaS, que significa "software as a service" o "software como servicio". Una empresa que no tiene desarrolladores de aplicaciones le paga a otra empresa para desarrollar un software específico. Lo mismo ocurre con los malwares. Por ejemplo, existe el RaaS, ransomware as a service, en el que los desarrolladores de este software malicioso lo alquilan a otros ciberdelincuentes para que ellos lo usen. Otro ejemplo ocurre con las páginas de phishing, en las que ya no se requiere de conocimientos en desarrollo web, sino que existen softwares que crean páginas webs idénticas a las de la entidad a simular, automáticamente en cuestión de segundos y con una dirección web habilitada. Basta con saber utilizar estas herramientas.

Antiguamente, siempre se creyó que los cibercriminales son personas con fuertes conocimientos en tecnología y, por ende, están escolarizados o tienen un nivel socioeconómico acorde a poder tener su propia computadora para cometer delitos. Hoy en día, si nos ponemos a analizar al delito de grooming, nos damos cuenta de que cualquier persona con un celular y con una aplicación de mensajería instantánea (por ejemplo, WhatsApp), ya son suficientes para cometer el delito. Podrá tener faltas de ortografía y tener

dificultades en el habla, pero no hace falta que sepa escribir y hablar correctamente, mientras se haga entender por chat. Asimismo, cuando hablamos de cualquier verbo típico de artículo 128 del Código Penal. No hace falta un conocimiento técnico para grabar un video y compartirlo en un grupo.

Clasificación cibercriminal

Existen dos grandes grupos de ciberdelincuentes, que posteriormente cada uno tendrá sus subcategorías o perfiles cibercriminales: los expertos en redes y computadoras; y los inexpertos. El primero es especializado y atiende principalmente a la fabricación de instrumentos informáticos y posterior comisión de ciberdelitos. Será un sujeto con aptitudes informáticas más técnicas, para quien el medio para cometer el delito puede ser el puro desafío de optimizar sus conocimientos. El objetivo de su delito es el desarrollo de herramientas y capacidades. El de la segunda categoría sólo utiliza la tecnología como un medio para ejecutar el delito. Es mucho más práctico y no teórico, siendo un simple usuario de las nuevas tecnologías para fines ilícitos y su motivación podrán ser muy diversas, comprendiendo desde la venganza, el dinero, la gratificación sexual, etcétera. El objetivo es cometer el delito a toda costa, sin suponer ningún reto a la hora de cometerlo. En otras pocas palabras, el primero crea herramientas maliciosas y el segundo las utiliza.

<u>Cibercriminales especializados</u>:

- Hacker: ya explicado en el capítulo *III.III,* se consideran delincuentes a los hackers de sombrero negro.
- Cracker: hacker que realiza actividades maliciosas, destructivas o criminales, modificando el comportamiento de sistemas y redes. Su motivación es económica o de reconocimiento.
- Viruckers: fabricantes de malwares. Podrían tener rasgos psicopáticos.
- Traficante de ciberarmas: venta de malwares. Facilita a terceros para posibilitar la comisión de hechos delictivos. Operan en mercados de la darkweb. La principal motivación es económica.
- Banquero: Ciberdelincuentes especializados en el robo de información. Posteriormente, podrán proveer a terceros esa información o venderla para obtener una recompensa económica.

- Contratista o hackers for hire: hackers por contrato. “Sicarios” del ciberespacio”. Prestan servicio por precio o recompensa, que pueden ser por el robo de información, denegación de servicio o cualquier ataque informático a un sistema de información, que pertenezca a una persona física o a una persona jurídica. El objetivo es económico y pueden actuar de manera individual o en grupo.

- Agente especial: operadores con un nivel de especialización y conocimientos informáticos muy alto. Pueden pertenecer a organizaciones criminales o a los servicios de inteligencia de los Estados.

- Ciber-soldados: se trata de hackers especializados en la guerra virtual, con el objetivo final de inutilizar la capacidad militar de un oponente. Su cometido es principalmente militar, siendo su tarea principal la de penetrar en los sistemas o redes de otro Estado con la intención de provocar daños, interrupciones o explotaciones de datos; o bien la ciberdefensa.

- Spammer: el spam puede definirse como la creación y difusión de mensajes no deseados, en su mayoría publicitarios. Una vez creado el contenido, se envía de manera automática y en masa.

- Domainer: sujeto que compra y registra dominios con el fin de explotarlos económicamente. La principal actividad delictiva en la que pueden incurrir esta clase de ciberdelincuentes es la estafa consistente en montar empresas que ofrecen un servicio de comprobación de disponibilidad de dominios que, tras la realización del chequeo de inexistencia, adquirirlo para una futura reventa a la misma empresa solicitante o a una tercera de la competencia.

- Espías Informáticos: expertos en la intromisión informática, el robo de información, el sabotaje y la coerción. Mayormente, dirigen sus ataques contra empresas del sector privado (espionaje industrial), pero pueden atentar contra los sistemas de información de los gobiernos y personales.

- Sniffer: hackers especializados en la confección y uso de programas capaces de controlar y analizar el tráfico red transmitido de una localización de red a otra, con el objetivo de robar información (por ejemplo, en una red de empresa).

- Ciberterrorista: se trata de un terrorista con conocimientos informáticos. La principal característica de este perfil es la motivación y justificación de los actos criminales por motivos como la religión, la economía o la política.

- Phisher: suplantadores de identidad. Su principal objetivo es la obtención de datos personales, financieros, credenciales, etc., de la víctima. Su principal objetivo es el beneficio económico y su modus operandi más habitual es el envío de correos electrónicos de phishing.
- Hoaxer: difunden bulos (hoax) o correos electrónicos en cadena con contenido falso o engañoso y atrayente. Relación con las fakes news.
- Ciberhacktivista: Su objetivo es ingresar a sistemas informáticos únicamente con fines de publicar propaganda.

Ciberdelincuentes no especializados:

- Emugger: delincuente que ha conseguido los conocimientos básicos necesarios para desarrollar programas maliciosos, con el fin de obtener ganancias económicas.
- Wannabe: aspirantes a hackers especializados, siendo ésta su principal motivación para llevar a cabo actividades ilegales. Tienen un conocimiento y unas aptitudes informáticas más elevadas que los emuggers, pero se encuentran completando su aprendizaje como expertos.
- Script kiddie: usuarios, habitualmente jóvenes, que carecen de conocimientos amplios de informática, pero que utilizan herramientas creadas por otros delincuentes especialistas.

En la mayoría de los tipos de ciberdelincuentes, los tipos penales más comunes son el art. 153 bis (hacking) y el art. 183 (daño o sabotaje informático), salvo por el phisher, que se encuadra en el art. 173. Recordemos que, lamentablemente, el robo de información, el spam, la compra de dominios y la suplantación de identidad, por sí solas, no son figuras penales, no son delitos.

V.VII) Cibervictimología

A diferencia de la victimología tradicional, la cibervictimología destaca la naturaleza global y sin fronteras de los delitos informáticos, así como la importancia de la seguridad digital y la protección de la información personal en la sociedad actual. Se enfoca en las víctimas, considerando los aspectos específicos y retos únicos que enfrentan las personas en el entorno digital.

Existe una escasa percepción sobre los riesgos existentes en el ciberespacio, lo cual se corresponde con el escaso miedo de las personas al ciberdelito frente al miedo a otros

crímenes cuya probabilidad de comisión sobre la víctima es claramente inferior. En una conversación con personas que no son del ambiente, no poseen conocimientos informáticos o sobre la problemática actual, es frecuente escuchar las frases "¿Quién va a querer hackearme a mí?", "No tengo nada que ocultar", "Si entran a mi homebanking, van a ver que no tengo plata". Esto denota la clara falta de concientización y de información, donde a las personas comunes (futuras víctimas) no les interesa ni preocupa la seguridad de sus dispositivos.

Existe una íntima relación entre la victimización y el estilo de vida en relación con Internet (número de horas en Internet, tipo de seguridad utilizada, la información personal publicada en redes sociales) de las víctimas de grooming o phishing. La falta de educación en materia de seguridad informática, la inexistencia de unos usos sociales por todos aceptados relativos a la utilización segura de los sistemas y las redes informáticas puede ser comprensible dada la novedad de las TIC y de los cambios sociales asociados a ellas, pero es factor determinante del incremento de la cibercriminalidad. Por otro lado, la falta de conocimiento desemboca en una falta de controles parentales. Los padres piensan que su hijo está jugando normalmente, sin representar ningún riesgo, e ignoran completamente que pueden estar siendo víctimas de grooming.

Las escuelas de criminología, como la clásica, la positivista y la criminología crítica, también pueden influir en la comprensión de la cibercriminalidad y la Cibervictimología. La criminología clásica podría abordar la cibercriminalidad desde la perspectiva de la elección racional y la disuasión, mientras que la criminología positivista podría examinar factores biológicos y sociales relacionados con la cibercriminalidad. La criminología crítica podría explorar las desigualdades y estructuras de poder en el ámbito digital, cuestionando la relación entre tecnología, corporaciones y cibercriminalidad. La Cibervictimología podría incorporar elementos de varias escuelas de victimología. Por ejemplo, la atención a la experiencia de la víctima (escuela contemporánea), el enfoque en la prevención (control social) y la consideración de la victimización múltiple (nueva victimología). Además, se podría explorar cómo las etiquetas y estigmatizaciones en línea afectan a las víctimas (etiquetamiento), y cómo las normas y subculturas digitales contribuyen a la victimización (cultural).

Miró Llinares (2012) plantea tres factores que hacen que la víctima adquiera una especial importancia para la explicación y prevención del delito en el ciberespacio. El primero, y como se ha visto, es que la víctima potencial del ciberdelito tiene, en primer

lugar, gran capacidad para dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado por el mismo: ella misma determina, desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida. Si no entra en el afectados, al igual que no lo podrá ser su patrimonio si no utiliza la banca electrónica y no comunica sus claves en Internet. Podría decirse que esto es idéntico a que si la víctima no sale a la calle no puede ser víctima de robos en ella. Pero seguirían pudiendo robarla (matarla o violarla) yendo a su domicilio, lo cual no es posible en Internet si la víctima no introduce en él los bienes de que se trate. Al fin y al cabo, en el ciberespacio no está la persona sino una expresión suya por ella misma elegida.

En segundo lugar, la víctima define con su interacción en el ciberespacio el grado de visualización de sus objetivos y, por tanto, las posibilidades de contacto con un agresor motivado en un mismo tiempo y espacio o en otro distinto. La víctima define el ámbito de riesgo al que puede acceder el agresor motivado. Podría argumentarse que esto no es más que lo que sucede en el espacio físico con el aumento de las posibilidades de sufrir delitos en el caso de visitar determinados lugares, hacerlo en determinados períodos del día, etc. Ciertamente es similar, pues se basa en que las actividades cotidianas de la víctima son parte de la explicación del evento criminal. La única diferencia es que en el ciberespacio no es necesario tiempo ni distancia física para la interacción, y que la misma en Internet depende por igual de todos los agentes, de modo que una vez hay una conducta criminal iniciada el que la misma afecte a uno, dos, cientos o miles de personas dependerá mucho de lo que hagan éstas. También cambia que mientras que ya hemos identificado en el espacio físico, y para determinado tipo de delitos, las conductas que pueden resultar peligrosas, aún no nos hemos preguntado todavía sobre cuáles son los comportamientos de riesgo en Internet, y es indudable que resultará esencial hacerlo de cara a la prevención de este tipo de criminalidad.

Por último, y, en tercer lugar, la víctima va a ser prácticamente la única que puede incorporar guardianes capaces para su autoprotección. Al no existir en este ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección serán determinantes a la hora de convertirse en víctima del cibercrimen. Si tenemos en cuenta, además, que en Internet, también al no existir distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta, no sólo sencillo, sino incluso en

muchos casos (virus y demás) instantáneo, y que la dirección del nuevo objeto del ataque la marcará la ausencia de sistemas de protección o las vulnerabilidades del objetivo (entonces adecuado), parece evidente concluir el protagonismo de la víctima en su proceso de autoprotección y, en caso de carecer de ésta, de victimización. Claro que la víctima también influye en la capacidad de sus guardianes en el espacio físico, pero si bien no se venden casas sin puertas o pisos en una urbanización sin vecinos, sí que se venden sistemas informáticos con acceso a redes sin antivirus o sin actualización de estos, así como redes sociales y demás lugares de comunicación social sin información sobre los riesgos de su uso.

CONCLUSIONES

Con todas estas explosiones tecnológicas, también explotaron (y cada vez más) las nuevas modalidades de conflictos entre seres humanos donde de por medio hay ordenadores o dispositivos que manejan información digital, nuevas modalidades de delinquir, nuevas constataciones a realizar por este medio, nuevos desafíos informáticos. Ante esto, la sociedad no está del todo preparada y estos conflictos se gestionan en muchos casos en el ambiente judicial. Si bien nuestro Código Penal tipifica las defraudaciones y la figura penal de las estafas son las mismas, constantemente están surgiendo modalidades nuevas de estafar a la gente. Un claro ejemplo actual son los llamados de ingeniería social (vishing) haciéndose pasar por el gobierno o por Mercado Libre, por ejemplo.

Por otro lado, hay que tener en cuenta que muchos autores han escrito sus obras hace 10 años atrás o más. Esto significa que la tecnología ha avanzado y, por consecuente, los usos que nosotros usuarios le damos, tanto para el bien, como para el mal. Además, el aislamiento por la pandemia generó un crecimiento exponencial de los delitos informáticos, que antes no existía y la figura de nuevas modalidades nunca antes vistas, como las estafas por cualquier vía de comunicación que no sea el email, como redes sociales (WhatsApp, Instagram, Facebook, Telegram).

Sabemos que la principal motivación de los ciberdelincuentes es económica y cada vez existen métodos nuevos y herramientas más sofisticadas, de fácil acceso y anonimato para lograr el cometido. Por otro lado, en las operaciones ilegales de ciberespionaje entre Estados o empresas, el objetivo no es económico, sino robar información. En casos de grooming, el objetivo es la adquisición de contenido pedofílico. Con esto, quiero decir

que, ya sea que estemos hablando de cibercrimen económico, social o político, en ningún caso la motivación sería destruir archivos. Es por ello por lo que, hoy en día, queda descartada la idea de ciberataques utilizando virus como tipo de malware, porque nadie lograría absolutamente nada con destruir archivos. Dicho esto, hago una salvedad y, a modo de reflexión personal, diré que el único caso de mayor trascendencia en la historia argentina donde se han borrado archivos fue en la notebook personal del fiscal fallecido, Alberto Nisman.

Para realizar ciberdelitos económicos, puedo afirmar que el ransomware es el malware más utilizado, pero necesariamente va acompañado junto con las técnicas de ingeniería social, ya que ningún malware se instala solo, sin hacer nada. Hoy en día, los grupos criminales se han ganado de cierto prestigio por el servicio que brindan. Esto logra que las víctimas paguen por el rescate de sus archivos, ya que la "empresa" criminal es "profesional" y conocida por devolver la clave que descifra los archivos cifrados. Recordemos que, para haber instalado un malware en nuestro dispositivo, se tuvo que haber ingresado a algún sitio, hacer clic o realizar alguna acción que no se debía. Los ataques de spear-phishing (phishing dirigido, personalizado) están en auge.

En los ataques de spear-phishing, se envía un enlace o archivo malicioso que descarga un malware. El malware va a ser siempre un troyano, ya que se debe enmascarar. Los troyanos permiten controlar el dispositivo infectado de forma remota y robar datos. Los spywares son un tipo de troyano. El motivo de la utilización de este método de ciberataque es el robo de información, ya sea que se utilice con fines políticos, económicos para extorsionar con publicarla o económicos para vender esa información en la dark web.

El uso de gusanos, hoy en día, es factible con la utilización de pendrives o unidades USB desconocidos y ejecutarlos en una computadora laboral. El objetivo será tomar el control de algún dispositivo infectado o un software específico, tal como fue el caso de Stuxnet. Una vez infectado el dispositivo con el gusano, se pueden instalar Rootkits que lo controlen.

En lo que respecta a los ataques de denegación de servicios (DoS y DDos), el motivo puede ser político (ciberguerra o ciberterrorismo) entre Estados o empresas, ya que el objetivo no es robar o destruir información, sino impedir que un servidor u entidad preste su servicio.

En ambientes empresariales u organismos estatales, la principal causa de incidentes es el uso inapropiado de recursos. La causa es el factor (error) humano por negligencia,

imprudencia o impericia. Básicamente, es utilizar los dispositivos laborales o personales conectados a la red laboral para cuestiones ajenas al trabajo y haber caído en una trampa. Por ejemplo, entrar a redes sociales desde el trabajo o abrir el correo electrónico y hacer click en un link malicioso. Es de vital importancia la capacitación en materia de ciberseguridad, en spear-phishing, ingeniería social y cibercrimen. La mejor forma de hacer prevención es capacitando a las personas, dando charlas y seminarios para concientizar. En este sentido, el rol de la Cibercriminología es clave, no sólo para identificar el origen del ciberataque y el modus operandi, sino para identificar qué error (acción u omisión) cometió la víctima, qué características tuvo el ataque y la víctima; y, a raíz de eso, crear planes de concientización y prevención, para que no vuelva a pasar y aprender de ello (ciberresiliencia). La realidad es que esta causa no es la principal sólo en ambientes laborales, sino también en los hogareños, donde el desconocimiento y la ignorancia provocan que las personas cometan errores (de acción u omisión) con sus dispositivos. En cualquier hogar se configura un ambiente hostil de sufrir cualquier ciberataque, donde los dispositivos cuenten con contraseñas fáciles, inexistencia de antivirus y configuraciones de seguridad, exposición de datos personales en redes sociales y la ignorancia sobre estafas, grooming y malwares, entre otros.

En cuanto a entender por qué nace la conducta cibercriminal, claro está que existen muchos factores que permiten esta criminogénesis. Por un lado, puedo determinar que la dificultad y falta de investigaciones, la falta de concientización y control parental; y el gran campo de oportunidad, permiten que chicos se encierren en sus habitaciones con una computadora o su celular y generen un interés técnico por querer ir más allá. Ese interés podría hacer que desarrollen capacidades técnicas más avanzadas a lo largo de los años. Por otro lado, también sabemos que la mayoría de los ciberdelitos no son técnicos y, en Argentina, pertenecen a ciberestafas. La situación económica genera un "terreno" más hostil para las víctimas y los delincuentes se aprovechan de las víctimas que no identifican una estafa o llamado de ingeniería social. Tengamos en cuenta que, si existe un ciberataque provocado por un cibercriminal, necesariamente existe una víctima que no posee elementos de protección de ciberseguridad. La falta de un guardián del ciberespacio obliga necesariamente a que los usuarios seamos nuestros propios autoguardianes, configurando nuestros dispositivos de la manera más segura posible y realizando las acciones u omisiones más seguras posibles en el ciberespacio.

Teniendo en cuenta la gran diversidad de delincuentes, modalidades delictivas que existen y que siempre van a surgir nuevas, este trabajo cuenta con una serie de recomendaciones para evitar que seamos víctimas de ciberataques:

• La desconfianza y sospecha de todo y todos, como premisa.

• Nunca, ninguna entidad bancaria u organismo del Estado le va a pedir ningún código ni contraseña.

• Configure la verificación en 2 pasos.

• Mantenga al día todas las actualizaciones de todas sus aplicaciones y antivirus, ya que las actualizaciones, por lo general, son parches contra fugas de seguridad y evita ataques exploits.

• Instale antivirus, ya que protege de los malwares y del Man in the Middle.

• Nunca brinde información personal a ningún desconocido en internet. No aceptar solicitudes de personas desconocidas. Tener perfil privado.

• Utilice contraseñas robustas.

• Evite conectarse a una red WiFi pública, salvo que tenga una VPN.

• Nunca debe insertar en su equipo una unidad USB desconocida.

• No brindar nunca datos personales, códigos de verificación o datos de usuario, contraseña y tarjetas de crédito o débito por teléfono ni por mensaje. Ante cualquier consulta, llamar directamente a la entidad (banco, empresa) o entrar en la página oficial, sin hacer clic en ningún link de ningún correo electrónico o red social.

• Tenga cuidado con los posibles correos electrónicos que le solicitan que actualice su contraseña, que su cuenta ha sido bloqueada o cualquier otra página web de inicio de sesión. En lugar de hacer clic en el vínculo proporcionado en el correo electrónico, escriba manualmente la dirección del sitio web en su navegador y verifique que el nombre de la página web esté bien escrito.

• No instale software a petición de ninguna persona que no sea idónea en la materia, a no ser que lo descargue de fuentes oficiales.

• No abra ningún .exe, .apk o cualquier otro archivo ejecutable. Podría ser malicioso. Si lo necesita, primero compruebe esos archivos con un antivirus.

• Revise siempre que el sitio que esté visitando sea seguro. La mayoría de los navegadores muestran un ícono de candado junto a la URL cuando el sitio web es seguro. Si no ve el símbolo, revise la dirección web y compruebe que comience con "https". Recuerde que esta información significa que los datos de tráfico entre usted y la página web

están cifrados y ningún intermediario puede leerlos, pero eso no asegura que la página no sea fraudulenta.

• No ingrese a ningún enlace sin verificar que no sea malicioso.

• Aprender sobre las nuevas tecnologías, para saber a qué riesgos nos enfrentamos nosotros y nuestros hijos.

• En caso de querer practicar sexting, saber los riesgos existentes frente a la difusión de fotos y videos íntimos, grooming y material de explotación infantil. Practicar sexting con los recaudos necesarios para que, en caso de caer en manos equivocadas, no se logre identificar al practicante (no mostrar cara ni rasgos particulares, como lunares, tatuajes, cicatrices).

Los aportes de la Cibercriminología resultan evidentes. En este trabajo, se estudiaron las causas, factores y escenarios que permiten el cibercrimen; y también se determinó qué herramientas necesitan los usuarios de internet para prevenir ser víctimas de ciberataques. Las recomendaciones del párrafo anterior son las herramientas fundamentales, básicas y completas para proteger cualquier dispositivo, cualquier información personal y la integridad tanto de los datos, como la integridad de las personas. La Cibercriminología, también nos hizo comprender y determinar que la causa madre de todo incidente en materia de ciberseguridad, desde grandes empresas hasta dispositivos hogareños, se debe a la falta de educación en materia de seguridad digital a temprana edad. En Argentina, existe una falta de educación temprana en la educación primaria y secundaria en materia de Ciberseguridad, que desemboca en un incidente causado por la ignorancia del tema, la falta de concientización y, por ende, la ausencia de elementos de protección. Con educación temprana, herramientas y conceptos de seguridad, se puede reducir considerablemente el número de víctimas por ciberataques, tanto usuarios comunes como empleados de la industria IT. Además, la reducción del número de víctimas implica, consecuentemente, la reducción de los gastos en investigaciones forenses posteriores. La implementación de programas de educación temprana en ciberseguridad en el sistema educativo argentino, desde la educación primaria hasta la secundaria, tendría un impacto significativo en la reducción de cibercrímenes y delitos informáticos al proporcionar a niños y adolescentes las habilidades y la conciencia necesarias para protegerse en línea. Hay que tener en cuenta que, hoy en día, los chicos menores de edad nacen en un mundo digitalizado. Contrariamente a nosotros, los adultos, que no tuvimos. Nosotros tuvimos que adaptarnos y aprender de este nuevo mundo y nosotros somos los responsables de enseñarles

a los chicos. Si se enseñaran estos riesgos y estas herramientas desde temprana edad, el número de víctimas futuras se reduciría considerablemente. El niño crecería sabiendo sobre estos riesgos y estas herramientas. Así como en cualquier aspecto de la vida, la famosa frase “la educación empieza desde casa”.

BIBLIOGRAFÍA

Aguiar, E. (2016). *Seguridad Informática: Para No Informáticos*. Estados Unidos: Palibrio.

Agustina, José R.; Montiel Juan, Irene, y Gámez-Guadix, Manuel (2020). *Cibercriminología y victimización online*. Madrid: Síntesis.

Alcalde, Eduardo (1994). *Informática Básica.* Madrid: McGraw-Hill.

Alvarado, R., & Morales, R. (2012). *Cibercrimen*. Guatemala: IUS Ediciones.

Anónimo (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet.* Compilado por Ricardo Antonio Parada y José Daniel Errecaborde: Erreius: Ciudad Autónoma de Buenos Aires.

Ambos, K. (2015). *Responsabilidad penal internacional en el ciberespacio*. Colombia: Universidad Externado de Colombia.

Anitua, Gabriel Ignacio (2005). *Historias de los pensamientos criminológicos.* Buenos Aires: Del Puerto

Arroyo, Sergio Cámara (2020). *La Cibercriminología y el perfil del ciberdelincuente*. Derecho y cambio social, 60.

Azzolin, H. y Sain, G. (2017). *Delitos informáticos: investigación criminal, marco legal y peritaje*. Buenos Aires: BdeF.

Baratta, Alessandro (2004). *Criminología crítica y crítica del derecho penal: Introducción a la sociología jurídico penal.* Buenos Aires: Siglo XXI.

Cámara Barroso, M.C. (2020). *Plataformas digitales: problemas jurídicos derivados de su actuación.* Madrid: Centro de Estudios Financieros.

Código Penal de la Nación Argentina.

Cohen, Lawrence E. y Felson, Marcus (1979). *Social change and crime rate trends: A rutine activity approach*. American Sociological Review, 44.

Convenio sobre la ciberdelincuencia. Budapest.

Cuarezma Terán, S.J. (1996). *La Victimología*. En: Estudios básicos de derechos humanos (p.295-318). Instituto Interamericano de Derechos Humanos. Recuperado el 9 de septiembre de 2024 de http://biblioteca.corteidh.or.cr/tablas/a12064.pdf

Darahuge - Arellano Gonzalez (2011). *Manual de Informática Forense*. Buenos Aires: Errepar.

Di Iorio y otros (2017). *El Rastro Digital del Delito*. Mar del Plata: Universidad FASTA.

Douglas Je., Burgess Ag. y Ressler R. (1992). *Crime Classification Manual.* Lexington: Lexington Books.

Fanjul Fernández (2018). *Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas.* Madrid: AMEC Ediciones.

Farrington, David (2005). *Childhood origins of antisocial behavior*. Clinical Psychology & Psychotherapy.

Gottfredson, M. y Hirschi, T. (1990*). A general theory of crime*, California: Stanford University Press.

INCIBE (s/f). *Protección de la información*. España: Instituto Nacional de Ciberseguridad

Hawking, Stephen (2018). *Breves respuestas a las grandes preguntas.* Título original Brief Answers to the Big Questions. Traducción de David Jou Mirabent, Buenos Aires: Ed. Paidós.

Ingenieros, José (1913). *Criminología*. Madrid: Daniel Jorro.

Instituto Europeo de Ciencias Forenses y Seguridad (2018). *Perfilación Criminal.* España.

Jahankhani, H. (2018). *Cyber Criminoloy*. Londres: Springer.

Jaishankar, K. (2011). *Cyber Criminology: Exploring internet crimes and criminal behavior*. Florida: CRC Press, Taylor and Francis.

Kyung-Shick, C. (2015). *Cybercriminology and digital investigation*. LFB Scholarly Publishing.

Kyung-Shick, Choi, Toro Álvarez, Mike y Marlon, Mike (2018). *Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital*, Bogotá: Universidad Antonio Nariño.

Liang, Quiao y Xiangsui, Wang (1999). *La guerra más allá de los límites*. China: Echo Point Books & Media.

Lipsey, Mark W. y James H. Derzon (1998). *Predictors of violent or serious delinquency in adolescence and early adulthood*. Serious and Violent Juvenile Offenders: Risk Factors and Successful Interventions. California: Sage Publications.

Miranda, J. J. C. (2020). *Factor Humano: La Teoría de las Actividades Cotidianas en la Ciberseguridad.* Recuperado el 2 de septiembre de 2024 *de* https://www.academia.edu/download/65051818/Factor_Humano_TAC_en_Cibe rseguridad.pdf

Miró Llinares, Fernando (2012). *El cibercrimen*. Madrid: Marcial Pons.

Molina (2003). *Tratado de Criminología*. Valencia: Tirant lo Blanch.

Palazzi, Pablo A. (2016). *Los Delitos Informáticos en el Código Penal*. Buenos Aires: Abeledo Perrot

Palazzi, Pablo A. (2020). El Consejo de Europa y el Convenio sobre la Ciberdelincuencia. *Revista Derecho y Nuevas Tecnologías* (2). Recuperado en marzo de 2023 de https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16879/1/RDYNT%20n%C2%B02.pdf

Riquert, Marcelo. (2011). *Delincuencia informática en Argentina y Mercosur.* Buenos Aires: Ediar. Recuperado el 2 de septiembre de 2024 de https://riquertdelincuenciainformatica.blogspot.com/2011/

Saín, Gustavo (2012). *Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet*. Buenos Aires: Editores del Puerto.

Saín, Gustavo (2015). *¿Qué son los Delitos Informáticos?* Buenos Aires: Rubinzal Culzoni.

Schmitt, Michael (2002). *La guerra de la información: los ataques por vía informática y el jus in bello*. Comité Internacional de la Cruz Roja. Recuperado el 2 de septiembre de 2024 de https://www.icrc.org/sites/default/files/document/file_list/ricr_2002_0.pdf

Stallings, William (2004). *Comunicaciones y redes de computadores*. Madrid: Pearson Educación.

Sueiro, Carlos (2020). *Inteligencia artificial y vigilancia electrónica*. Buenos Aires: DPyC.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Tolosa, G. (2014). *Protocolos y modelo OSI*. Recuperado el 18 de agosto de 2024 de http://www.tyr.unlu.edu.ar/pub/02-ProtocolosOSI.pdf.

Trigo, Ruíz De Ángeli y Cirimelo (2022). *Seguridad en el ecosistema digital: ciberseguridad, ciberespacio y las personas*. Universidad FASTA, Facultad de Ingeniería.

Van Creveld, Martin (2007). *La transformación de la guerra*. Ed: José Luis Uceda Editor.

Zaffaroni, E. R., Alagia, A. y Slokar, A. (2006). *Manual De Derecho Penal: Parte General*, Buenos Aires: Ediar.