Inseguridad en el Ciberespacio: respondiendo más allá de los Servicios de Seguridad

Cyberspace Insecurity: Responding beyond Security Services

Miguel Torrealba[1]
Departamento de Computación y Tecnología de la Información, Universidad Simón Bolívar, Miranda, Venezuela[1]
mtorrealba@usb.ve[1]

Fecha de recepción: 17/03/2021
Fecha de aceptación: 21/04/2021
Pág: 200 – 232

Resumen

Mientras las computadores se han diseminado más en los ambientes cotidianos, la inseguridad que los rodea también se ha hecho notar. Los incidentes han aumentado y han mostrado un crecimiento en su sofisticación. Aún así, para el común de la ciudadanía la conceptualización de esa realidad sigue estacionada en una realidad de cómo fue la misma durante sus inicios, cuando el tema se consideraba como un problema de asegurar lo confidencial con algunos datos digitales. Algo que inicialmente se resolvió con criptografía y que luego se extendió con ciertas protecciones específicas a las redes de computadoras. Pero un análisis más amplio y moderno de los incidentes de inseguridad, revela que el problema se ha hecho más complejo y que ahora existen actores de importancia, llegando a situaciones donde algunos han invertido sus roles y en vez de disminuir la inseguridad tratan de sacar provecho de esta. En consecuencia, las soluciones a instrumentar se hacen más complicadas de desarrollar y aplicar. Este trabajo es un ensayo que recoge significativos sucesos en esta área, que han marcado cambios y delineado potenciales líneas de acción. Para ello se revisa documentación sobre la evolución cronológica de los incidentes y se enumeran aquellos más recientes, que lucen como significativos para reconocer racionalmente las áreas y tendencias que ameritan mayor atención o de nuevas aproximaciones, recomendando así un tratamiento más amplio que provea mejores resultados en las sociedades modernas.

Palabras clave: seguridad de datos, ciberespacio, ciberarmas, amenazas digitales, tendencias de inseguridad tecnológica.

Abstract

While computers have spread more in everyday and every environments, the insecurity that surrounds them, has also become noticeable. The incidents have increased and have shown a growth in their sophistication. Even so, often the conceptualization of that reality is still parked in how it was, in the past that was in its beginnings, a problem focus of only securing the digital data. Something that was initially solved with cryptography and then extended, with certain specific protections in computer networks. But today, an analysis of the incidents reveals that the problem has become more complex and that there are now important participants, who have reversed their roles and instead of reducing insecurity, try to take advantage of it. In consequence, the solutions to be implemented are more complicated to develop and apply. This work is a position paper that recovers significant successes in this area, which has marked changes and outlined potential lines of action. It reviews documentation on the chronological evolution of the incidents and lists those most recent, which are significant to rationally reconcile the areas and trends that give the greatest attention to new approaches, recommending further treatment that provides better results in the modern societies.

Key words: data security, cyberspace, cyberweapons, digital threats, technological insecurity trends.

"Tecnologías y procedimientos fuertes en seguridad ya han sido desarrolladas, pero la evidencia sobre su eficacia y la efectividad de su costo, es algo de lo que aún hoy carecemos."
Dilemas de la Ciberseguridad: Tecnología, políticas e incentivos
Sumario de discusiones del foro científico estadounidense y británico del 2014
Academia Nacional de Ciencias de los EEUU y Real Sociedad Científica del Reino Unido

Introducción

En su libro "La quinta disciplina", Peter Senge describe una parábola que denomina como la rana hervida para señalar que algunas organizaciones son incapaces de responder a las amenazas crecientes, especialmente cuando estos suceden gradualmente y envuelven a esas empresas [Senge, 1998]. A esas organizaciones les resulta cuesta arriba identificar a tiempo los cambios ligeramente crecientes, que se van sucediendo y que conducen a riesgos potenciales. Pero debe comprenderse que frecuentemente las organizaciones son manejadas por equipos directivos y que la percepción predominante de los individuos que conforman tales equipos, inclinará sus decisiones. Por su parte, la Agencia Central de Inteligencia (CIA) estadounidense desde hace años ha investigado sobre la percepción humana, con la intención de sacarle provecho para facilitar engaños de sus oponentes. En el reporte de investigación de Abril de 1981, denominado

"Máximas del Engaño: hecho y folclore"[1], dentro de la argumentación el tema refiere a la "Máxima Nro. 2: Limitaciones Humanas en el Procesamiento de Información". Y en referencia a ese tema, allí se expresa la siguiente sentencia:

> Otra limitación humana en el procesamiento de la información que es relevante para la planificación del engaño, es la frecuente inhabilidad de actores para detectar pequeños cambios en observaciones, incluso cuando el cambio acumulado durante el tiempo resulta grande. Esto es una contraparte de la hipótesis de Jervish #3 (26) "actores pueden más fácilmente asimilar en sus imágenes establecidas la información de otro actor que contradiga sus imágenes, si esta información es transmitida y considerada pedazo a pedazo, que en el caso de que esta se reciba entera de una sola vez." Esta es la base para el uso del condicionamiento como una técnica del engaño. [CIA, 1981]

El presente artículo recoge cambios en la seguridad de computadores, redes y sistemas, que han sucedido en las últimas seis décadas y que algunas veces, por ser graduales, pasan desapercibidos, incluso para profesionales y practicantes. En otras ocasiones actores contrarios aprenden a engañar deliberadamente y explotan esa ventaja para instrumentar ataques cibernéticos; a esto se le conoce como técnicas de *Ingeniería Social*. Esta realidad incide en la protección real de los activos informáticos corporativos e institucionales. Este artículo aspira a contribuir con la exposición de una interpretación lógica de la evolución y cambios de los peligros en el ciberespacio, un juicio personal con sustento en el recorrido de la línea de tiempo, que discurre sobre sucesos trascendentales, pero a veces juzgados como no significativos o no encadenados, más que si han marcado y alineado el desarrollo de la aún cambiante área de seguridad. Una comprensión más amplia de estos eventos puede contribuir a que las aproximaciones de protección y resiliencia sean manejadas, por gobiernos, empresas, comunidades y la ciudadanía, en modo distinto a lo que con frecuencia se aplica y en consecuencia, se puedan obtener mejores resultados.

Buscando alternativas ante las recetas defensivas a ciegas:

En materia de seguridad tecnológica digital en numerosos cursos y adiestramientos se ha extendido la idea de aplicar respuestas preconcebidas y que han sido consideradas como contramedidas clásicas. Así por ejemplo, ante un problema de resguardar un secreto se acude de inmediato a la criptografía, descuidando a veces otras soluciones alternas más adecuadas o desestimando la dificultad de aspectos complementarios, como es por ejemplo la complejidad de distribuir las claves que soportan tal aproximación defensiva. Esto sucede entre otras razones, por presiones de tiempo limitado para los diagnósticos y etapas de análisis, así como privilegiar la eficiencia de costos de las soluciones. De modo que con frecuencia la atención se

[1]Ese material fue liberado al público en Diciembre de 2015 por una solicitud FOIA y pudo ser obtenido a partir del portal `governmentattic.org`

dirige a los instrumentos comerciales y a las técnicas que el mercado laboral ya ha aplicado, mientras se descuida la mirada al desarrollo, evolución y contexto que el flujo cronológico de las amenazas ha acontecido sobre los sistemas.

Dado que las soluciones preconcebidas son genéricas y en materia de seguridad cada detalle cuenta; un único elemento fuera de control, puede derrumbar una arquitectura entera. Además, muchas de esas soluciones también incluyen debilidades intrínsecas y si en el momento en que se les pone a prueba, contienen vulnerabilidades de software -algo muy frecuente- y carecen de los parches correctivos que sus fabricantes, progresivamente suministran, según van advirtiendo los problemas, estos sistemas de protección en vez de asegurar los bienes a resguardar pueden terminar sirviendo a la causa contraria. Es así como se hace necesario aplicar una visión más amplia y ello ya ha sido expresado por conocedores del tema. Así por ejemplo, Peter "*Mudge*" Zatko, el líder del grupo "*hacker*" llamado "*L0pht*" y que testificó ante el senado de los EE.UU. en calidad de experto, ha escrito sobre las fallas de seguridad esto:

> La meta aquí no es iluminar tecnologías particulares, sino hablar acerca de algunos ambientes y situaciones psicológicas que causan que la seguridad llegue a ser débil. En orden para lógicamente llegar a comprender mejor donde esas debilidades se presentarán, es importante considerar las influencias externas y restricciones que han sido colocadas sobre los que instrumentan una tecnología. Mientras es un divertido juego mental representar el lado ofensivo de la moneda, cuando los defensores también juegan eso, se les conduce además a nuevas dimensiones y a) previenen errores que de otra forma llevarían a ataques o b) usan y operan a su favor las mismas técnicas con las que juegan los atacantes. En este punto, el juego de la seguridad se convierte en lo que considero, algo bello. [Mudge et al., 2009]

Esta visión incorpora la consideración psicológica de cómo percibimos la inseguridad en computadoras y las acciones que realizamos para controlarla, un asunto que ha cambiado con el tiempo y que exige mirar más allá de los tecnicismos electrónicos. También es necesario señalar que estas perspectivas no están circunscritas únicamente al área técnica, ya que existen trabajos de análisis conceptuales académicos, donde se señala que la propia definición de lo que es seguridad ha recibido poca atención y que el problema que ello genera, sobrepasa el fracaso de un ejercicio intelectual para ubicarse en la real incapacidad para determinar si esta se ha alcanzado o no [Baldwin, 1997]. En 2010, en una charla que dictó para la Universidad Estatal de Penn, el matemático y criptógrafo Bruce Schneier expresó claramente la práctica común de la industria:

> Les daré la respuesta corta. La respuesta es que respondemos a la sensación de seguridad y no a la realidad. Ahora, la mayoría de las veces, eso funciona. La mayor parte del tiempo la sensación y la realidad son iguales. [TEDtalk, 2010]

En consecuencia, sobre un fenómeno de tanta importancia aún existe espacio para debatir sobre estas complejas definiciones, sus teorías, la inclusión de nuevas perspectivas psicológicas

y las extensas alternativas lógicas a emplear. Así pues, entre los numerosos enfoques, uno de los existentes para comprender mejor los peligros, se fundamenta en conocer la historia de estos y las respuestas existentes, al igual que las respuestas que se les han dado y enmarcar estas dentro de un enfoque que emplee la ingeniería de la seguridad como la disciplina a usar durante la formulación de respuestas.

Esta revisión de pasos dados y de donde estamos no es irrelevante, ya que es común que en tecnología de la seguridad de computadoras, las respuestas se han dado sobre visiones parceladas, más como requerimientos de servicios de seguridad [2] de los sistemas y no sobre la propia seguridad de esos sistemas. Así se puede entender la rápida inclinación a emplear criptografía para atender necesidades de confidencialidad y la propensión a usarla para muchos casos que podrían tener otras respuestas. Algo tan notable, que incluso hoy muchos cursos y textos académicos de ciberseguridad en todo el mundo tienen como eje central el estudio detallado de los algoritmos de cifrado, descifrado, firmado y certificación, por encima del análisis, diseño y la evaluación de la seguridad de los sistemas. Y sin restarle importancia a la matemática de soporte criptográfico, los avances tecnológicos de la seguridad de hoy, llenarían fácilmente una programa de formación profesional de cuatro años universitarios, pero con frecuencia en los cursos aislados de carreras de tecnología e ingeniería, en computación, electrónica y ciencias afines, se repiten los esquemas de temarios válidos hace cinco décadas atrás.

Para otros casos la inseguridad de muchos sistemas modernos ha variado y se impacta más con la falta de privacidad que con problemas de secrecía, pero como esto aún no predomina en las recetas defensivas de cada desarrollo de nuestro tiempo, hay que esperar a que los productos y sus tecnologías salgan al mercado y sufran perjuicios, para que el fabricante admita que existen tales dificultades que pudieron haberse supuesto, con bases razonables, desde su concepción inicial. Los populares sistemas electrónicos del tipo asistentes virtuales en el hogar, como Amazon Alexa® y Google Asistant® son ejemplo de esto.

La primera aproximación sólida en el área se concentró en la criptografía:

En comparación con otras ciencias o disciplinas profesionales, la computación es relativamente nueva. Si se descarta sus fundamentos matemáticos y las aproximaciones mecánicas de la misma, sus inicios pueden ser asociados al final de la década de los años cuarenta del siglo XX [Ceruzzi, 2003, Esmenger, 2010]. Por otra parte, las aproximaciones para proveer de seguridad a tales sistemas, fueron surgiendo después de haber desarrollados los primeros computadores. Esto significa que el progreso en esa línea no siguió el esquema,

[2] Definidos en la Recomendación X.800 del Sector de Estándarización de las Telecomunicaciones de la Unión de Telegrafía Internacional (ITU-T)

ISSN: 2244-7423

actualmente recomendado, de atender la *seguridad desde la etapa de diseño* [3].

Por los años 60 los primeros requerimientos no resultaron muy exigentes, ya que la tecnología que predominaba era la de Computadores Centrales comerciales con *multiprocesamiento y tiempo compartido* ("*Main Frame*"), que se usaban con terminales de acceso a estos [Ralston, 1976]. De manera que las necesidades de seguridad se centraron principalmente en el control del acceso al sistema y sus recursos, al igual que proteger la confidencialidad de los contenidos que almacenaban. Esa situación, unida con el hecho de que desde el inicio de las guerras, para proveer confidencialidad en las comunicaciones se colocó a la criptografía como el elemento técnico más usado, condujo a que las primeras aproximaciones de seguridad en el mundo de la computación y redes de datos, se orientara hacia el empleo de técnicas e instrumentos matemáticos como eje central de las protecciones.

Este patrón se percibe cuando se revisa los materiales bibliográficos de esos tiempos; así por ejemplo, en el prefacio de su libro, Criptografía y Seguridad de Datos, que fue publicado en 1982, la doctora en matemáticas, Dorothy Denning escribió:

> Seguridad de datos ha evolucionado rápidamente desde 1975. Hemos visto excitantes desarrollos en criptografía: cifrado de clave pública, firmas digitales, el estándar de cifrado de datos (DES), esquemas de salvaguardas de llaves criptográficas y protocolos de distribución de esas llaves. Hemos desarrollado técnicas para verificar que los programas no filtren datos confidenciales, o que transmitan datos clasificados a usuarios con bajas autorizaciones de seguridad. En bases de datos estadísticas hemos encontrado nuevos controles para proteger datos y nuevos métodos para atacar esas bases de datos. Hemos llegado a un mejor entendimiento de las limitaciones teóricas y prácticas de la seguridad. [Denning, 1982]

Por otro lado, para ese entonces, la contraparte divulgaba con mayor organización sus logros; así por ejemplo, en Enero de 1984 salió a la luz la polémica publicación periódica 2600, que alcanzó notoriedad por discutir claramente modos técnicos en que se explotaba las vulnerabilidades de algunos sistemas. En el editorial de su primer número, que ahora se le atribuye a Eric Gordon Corley, alias "Emmanuel Goldstein" [4], se expresó:

> La idea de 2600 nació a principios de 1983. Nosotros vimos una enorme necesidad de disponer de alguna forma de comunicación entre aquellos que realmente aprecian el concepto de la comunicación: entusiastas tecnológicos. Por supuesto, otros tienen diferente forma de describir a tales personas -ese rango de palabras va desde *hacker* o *prheaker* a términos más fuertes como son criminales o anarquistas-.

[3] "*Security by design* (SBD)" es la denominación en inglés que el área de la ingeniería del software acuñó a esa aproximación

[4] El nombre proviene de la figura del líder de la hermandad, que se opone al totalitarismo del "Gran Hermano", en la conocida novela del escritor británico George Orwell y que lleva por nombre 1984.

> Nuestro propósito es no entrar en juicios. 2600 existe para proveer información e ideas a individuos que viven para esas cosas. Todos los items que contienen estas páginas son provistos para propósitos de información únicamente. 2600 no asume responsabilidad por cualquier uso que se le pueda dar a esta información. [Goldstein, 2004].

El hecho es que desde esos tiempos, erróneamente se popularizó el término de "*hacker*" como el antagonista con el que deben tratar los protectores y aún hoy persiste la idea de que son únicamente quienes atentan contra la seguridad tecnológica. Muchos cursos y publicaciones de nuestros tiempos, ignoran la presencia de otros actores, que en nuestros tiempos ganan más relevancia con sus acciones, pero que se cuidan de aparecer en los modernos medios de comunicación. Así pues, retomando a finales de la década de los ochenta, los gusanos "*Christmas Tree EXEC*" y el de "Morris Jr." conocido como el *gusano de la Internet* [Spafford, 1988], mostraron su real eficacia como elementos de *ataques*, al interrumpir el funcionamiento normal de grandes redes de computadoras.

Se debe agregar que posteriormente el ámbito académico reconoció que nunca se alcanzaría el objetivo ideal de hacer completamente invulnerable al sistema [Spafford, 1989] y es necesario señalar que, como resultado de estudiar serios perjuicios, la visión del problema que alcanzaron los expertos se amplió aún más. En 1992 un programador búlgaro, bajo el seudónimo "*Dark Avenger*" creó el primer virus polimórfico que mostró que los controles del tipo antivirus podían ser engañados. Dos (2) años más tarde, diez (10) millones de dólares fueron robados del Citibank® en un aún confuso incidente, que los medios actualmente siguen atribuyendo al bioquímico y matemático ruso Vladimir Levin [El País, 1995]. Eventos desastrosos como estos fueron conduciendo a los guardianes de la información e infraestructura técnica a reconocer la compleja realidad computacional[5] y también, a comprender que la tarea de asegurar un *sistema sociotécnico* demanda más que añadir instrumentos de protección al mismo. Es por ello que en el año 2000, el reconocido matemático Bruce Schneier, escribió en el prefacio de su libro Secretos y Mentiras una llamativa y pública corrección a su previo pensamiento que provenía del mundo criptográfico: "Si usted piensa que la tecnología puede resolver sus problemas de seguridad, entonces usted no comprende los problemas y no entiende la tecnología." [Schneier, 2000]

Del lado de algunos poderes, ciertas propuestas para proteger los sistemas resultaron polémicas; tal fue el caso de los procesadores conocidos como "*Clipper*", con esquemas de cifrado que el gobierno estadounidense intentó se aplicara en la industria y que usaba una *clave bajo custodia* para recuperar la información en texto plano. Iniciativa que la comunidad académica rechazó y además demostró, con elementos científicos, que podían ser un peligro mayor que los que pretendía erradicar [Blaze, 1994]. De forma que observando el incremento

[5]Para ese momento, las redes de computadoras, la telefonía móvil y el acceso a la Internet se había convertido en elementos de uso común entre los usuarios.

ISSN: 2244-7423

de ataques, los grados de sofisticación que alcanzaban y sus variaciones, así como las fallas en las herramientas de protección, se fue extendiendo una creencia de que lo que se necesitaba aplicar era métodos, procedimientos y técnicas más orientadas a lo que es la ingeniería. Ross Anderson del Laboratorio de Computación de Cambridge, en 2001, expresó que la materia demandaba experticia de diferentes áreas y se refirió específicamente al término de Ingeniería de la Seguridad de este modo:

> Ingeniería de la seguridad trata acerca de construir sistemas que se mantengan confiables al enfrentar la malicia, el error y el infortunio. Como disciplina, se enfoca en las herramientas, procesos y métodos necesarios para diseñar, implementar y comprobar sistemas completos, y para adaptar los sistemas existentes de acuerdo a la evolución de sus ambientes. [Anderson, 2001]

En 2003 aparece en escena el peculiar grupo "Anónimos" (*Anonymous*) y en 2004 la agencia rusa Pravda informa que Corea del Norte declaró haber entrenado quinientos (500) hackers para acciones políticas contra Corea del Sur. Una unidad que se presume se formó a finales de los años noventa. Esta información, difícil de verificar, públicamente inició la participación de las naciones estado como actores que podían atacar y subvertir sistemas en el ciberespacio [6], pero en realidad es difícil precisar quienes están en esa línea y desde cuando lo hacen, por lo que mucha información proviene de fuentes de "expertos" y con aproximaciones del tipo Delphi [Wook Boo, 2016] Esto es consecuencia de que estas labores se mezclan con la del espionaje o con los ámbitos que las naciones realizan en secreto y a menudo niegan; pero en Julio de 2010 Ronald Deibert, profesor de Ciencias Políticas de la Escuela de Estudios de Extranjeros de Munk, en Toronto, escribió en un número de "*MIT Technological Review*", que la militarización del ciberespacio es real.

Retomando la cronología de cómo ha cambiado la seguridad digital, en 2005 se extendió el uso del término *Amenaza Avanzada Persistente* (APT) para indicar peligros sofisticados tecnológicamente -software del tipo explosivos de día cero, "*malware*" que se adapta a las necesidades, instrumentos avanzados de intrusión- que estaban dirigidos a comprometer sistemas vinculados con funciones gubernamentales, militares y económicas. Un notable ejemplo son las primeras versiones de "*Duqu*", las cuales se hicieron públicas en 2011. Este tipo de evolución en el "*malware*" preocupó además, por que las medidas de protección tradicionales, tales como sistemas antivirus, cortafuegos ("firewalls") y detectores de intrusos fallaban notablemente para contener estas nuevas amenazas. La Figura: 1 resumen algunos de esos peculiares eventos e incidentes, en las últimas décadas del siglo anterior y la primera del vigente.

[6] El término Ciberespacio que originalmente refería a una representación de la realidad con soporte de computadoras, proviene de un autor de ciencia ficción, estadounidense y canadiense William Gibson, quién en 1984 lo popularizó a través de su novela Neuromante. Actualmente, su concepción se ha extendido y hasta diversificado, llegando a un punto que algunos colocan a la Internet como parte del mismo y otros hacen una asociación directa del concepto con ese desarrollo técnico.

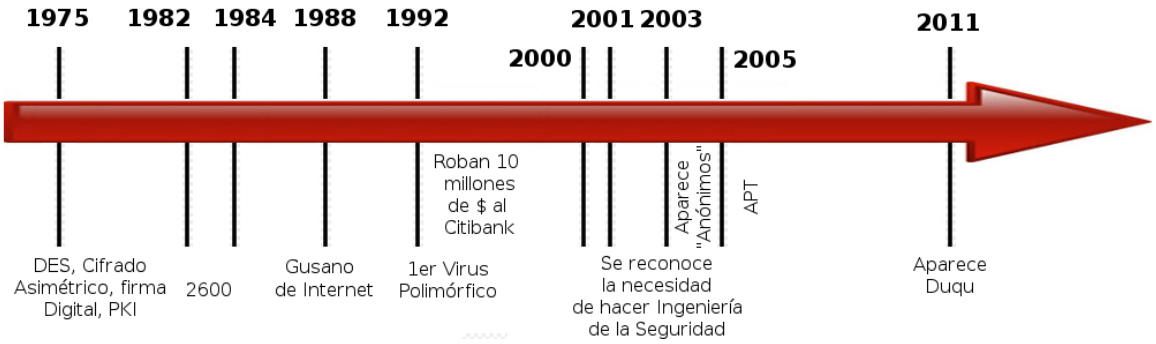

Figura 1: Notables eventos de seguridad/inseguridad a finales del siglo XX e inicios del XXI. Fuente: Torrealba (2021)

De la seguridad digital al ciberespacio como campo de batalla:

Así como en una primera etapa de la perspectiva de seguridad de datos, se extendió la mirada para reconocer a la seguridad de la información y la seguridad de redes de computadoras, al inicio del segundo milenio, se pasó de seguridad de las *tecnologías de la información y comunicaciones* (ICT) a la seguridad del ciberespacio. Y es que de una visión convencional del ámbito corporativo se evolucionó a considerar otra más, plena de elementos críticos y posteriormente uno consideración sobre las infraestructuras a nivel de naciones, a las de dominio industrial y la de servicios básicos que pudieran soportar la actividad funcional de un país.

Esto fue sucediendo por incidentes y a veces por *pruebas de conceptos*. Por ejemplo, en 2007 el Laboratorio Nacional de Idaho realizó una comprobación de nombre "Prueba de Vulnerabilidad del Generador Aurora", controlado a través de un sistema de control industrial y al cual se accedió a través de una conexión remota. El generador eléctrico fue físicamente dañado a través de un conjunto de operaciones anormales y exageradas, ya que se pretendía examinar el grado de utilización de un SCADA[7], como un medio para el ataque [Meserve, 2007]. La prueba reveló a los expertos que atentar contra un sistema crítico industrial era prácticamente posible, ya que en teoría ello se daba por válido. Y es que muchos de los sistemas de control industriales que los fabricantes desarrollaban en ese entonces, pasaron a usar la Internet y a compartir redes de datos corporativas a final del siglo veinte; lo delicado de esa exposición fue que ese cambio no estuvo acompañado de mejoras sustanciales en las protecciones y muchos protocolos de comunicación, como en el caso de Mobdus, seguían operando como cuando lo hacían sobre redes aisladas y dedicadas, ya que lo que con frecuencia se hacía era transportar sus paquetes encapsulados en Datagramas IP. Automáticamente

[7]SCADA es el acrónimo de la tecnología de sistemas del tipo Control Supervisado y Adquisición de Datos, que a través de sensores y controladores lógicos programables, permiten recoger información en tiempo real sobre plantas industriales y maniobrar adecuadas respuestas desde una localización remota.

heredaron las debilidades del *Protocolo de Internet (IP)* , pensado originalmente en los 70's y sin tomar la seguridad como un elemento central de su diseño, más bajo un enfoque de únicamente hacer el "mejor esfuerzo" en sus entregas.

Estos acontecimientos pueden ser difícil de entender ahora, por lo que resulta necesario explicarlos señalando que al final del siglo XX e inicio del XXI, el mundo estaba en medio de cambios y hasta de crisis políticas. El incidente sobre las torres gemelas del Centro de Comercio en Nueva York incidió en nuevas legislaciones y doctrinas de los sistemas y proveedores de servicios en Internet. Un ejemplo de ello fue que a la Agencia de Seguridad Nacional de EE.UU. (NSA) se le autorizó a espiar comunicaciones de ciudadanos de ese país sin órdenes judiciales. La tecnología para interceptar y escuchar secretamente millones de llamadas y mensajes, ya hacía años estaba disponible y esto cambió paradigmas de ejecución de muchas agencias de inteligencia. El espionaje se hizo masivo y se desviaron sistemas con propósitos específicos para interceptar y escuchar furtivamente comunicaciones.

Adicionalmente, la evolución tecnológica digital incidía notablemente en las sociedades, al igual que las aspiraciones de esta, servían para darle forma a esa misma tecnología. Otro aspecto resaltante es el relativo a la responsabilidad por el desarrollo del software, que para ese momento e incluso hoy, no ha sido regulada legalmente y en computación, ha resultado común que los criterios comerciales supediten los de seguridad. El reconocido investigador Manuel Castells explica algo de eso en el prefacio de la edición 2010, del primer volumen "El surgimiento de la sociedad en red" de su obra "La Era de la Información". Un extracto del mismo, ilustra el punto:

> (...) la creciente incapacidad de las instituciones políticas basadas en la noción nación – estado, para tratar problemas globales y demandas locales: todas estas son diversas expresiones de un proceso multidimensional y cambios estructurales que toman lugar en la mitad de la agonía e incertidumbre. Estos son pues tiempos problemáticos. El sentido de la desorientación está compuesto por cambios radicales en la realidad de la comunicación, derivadas de la revolución con las tecnologías de la comunicación. El desplazamiento de los tradicionales medios en masa en un sistema de redes de comunicación horizontal, organizado alrededor de la Internet y de las comunicaciones inalámbricas, ha introducido una multiplicidad de patrones en las comunicaciones como la fuente de una transformación cultural fundamental, así como que la virtualidad se convierte en una dimensión esencial de nuestra realidad. [Castells, 2010].

Un ejemplo de lo convulsionado de los desarrollos tecnológicos de esa época se refleja con los enfrentamientos entre Phillip Zimmermann y el gobierno estadounidense. En 1991, como consecuencia de una propuesta ante el senado de EE.UU para luchar con el crimen, se establecía la necesidad de proveer al gobierno con mecanismos del tipo puerta trasera sobre los sistemas de cifrado, para así poder controlar a los delincuentes que encriptaban sus comunicaciones. Pero

algunos ciudadanos de ese país interpretaron que ante la capacidad tecnológica que adquiría su gobierno, requerían protegerse de potenciales intromisiones en sus vidas; eso incidió en la distribución del PGP[8]®, que Zimmermann había escrito [Lucas, 2006]. El dilema puede ser percibido al leer este extracto del documento de Zimmermann titulado "Por qué escribí PGP":

> El derecho a la privacidad está implícitamente extendido en los derechos humanos. Pero cuando se forjó la Constitución de los EE.UU., los padres fundadores no vieron la necesidad de deletrear explícitamente la necesidad de tener derecho a una conversación privada. Eso habría sido tonto. Hace doscientos años, todas las conversaciones podían ser privadas. Si alguien más podía escucharle, bastaba con que usted se fuera detrás, al establo y tener su conversación allí. Nadie podría escucharle sin su conocimiento. El derecho a tener una conversación privada era un derecho natural, no en un sentido filosófico sino que dada la tecnología de esa época, se trataba del sentido que provee una ley de la física.
>
> Pero con el advenimiento de la era de la información, comenzando con la invención del teléfono, todo esto ha cambiado. Ahora la mayoría de nuestras conversaciones son conducidas por medios electrónicos. Esto permite que nuestras más íntimas conversaciones estén expuestas sin nuestro consentimiento. [Zimmermann, 1999].

Y a pesar de que la propuesta no alcanzó a ser aceptada y Zimmerman ganó en los tribunales, el interés gubernamental por controlar las comunicaciones y proteger sus intereses no ha cesado. Así por ejemplo en el año 2009, el Secretario de Defensa de los Estados Unidos de América (EUA) dirigió el establecimiento de una unidad Cibercomando de ese país y en el 2011, el Secretario de Estado de esa misma nación proclamó al Ciberespacio como un nuevo dominio de operaciones militar [Lennon, 2011]. Ese mismo año, un Tanque de Pensamiento independiente en La Haya publicó un reporte describiendo lo que veían como el futuro del área. Allí se expresaba que:

> Hoy el ciberespacio se está expandiendo más rápido que nuestra habilidad para defenderlo. El ciberespacio se define como sistemas TIC, redes y la información contenida dentro de esos sistemas y redes, estén en línea o fuera de esta. La ciberseguridad se define como el funcionamiento ininterrumpido de esos sistemas. Las capacidades de ciberatacar se están extendiendo rápidamente entre actores estados y no estados, tales como "hacktivistas", grupos terroristas y el crimen organizado. Al mismo tiempo, más funciones basadas en las TIC están creciendo

[8]Pretty Good Privacy, fue el nombre que recibió el software que para la ciudadanía común desarrolló Zimmermann y que se popularizó por sus iniciales PGP. Años más tarde, cuando fue adquirida por una empresa privada y se restringió su distribución, surgieron iniciativas abiertas o bajo licencia GNU -con las cuatro (4) libertades del Software Libre- que se denominaron OpenPGP® y GPG®. Esa fue la respuesta tecnológica de la comunidad internacional, para no perder la protección que había ganado gracias a la lucha de Zimmermann.

> con mayor interdependencia, incrementando el riesgo de fallas tipos 'cascada' o 'dominó'. [Tessier, 2011]

El 28 de Noviembre de 2010 bajo la iniciativa del portal "*Wikileaks*", dio inicio un escándalo de filtración masiva de documentos secretos de EEUU que se conoció como el "*Cablegate*". Más de 250 mil cables diplomáticos de embajadas y consulados, que fueron expuestos por diarios como "*The New York Times*", "*The Guardian*", "*Der Spiegel*" y "El País". Otro incidente que tuvo repercusiones en las relaciones internacionales se derivó de comienzos de Diciembre de 2012, cuando el ex-empleado de una contratista de inteligencia estadounidense, Edward Snowden, contactó por correo electrónico al periodista Glenn Greenwald del diario británico "*The Guardian*", para denunciar el espionaje masivo ilegal de la NSA. Esta filtración reveló además el cómo y los instrumentos técnicos que facultaban lo que por indicios ya se conocía, tales como el peculiar programa PRISM [Greenwald, 2014]. Entre las consecuencias, aconteció un desencuentro internacional entre EUA y las naciones que ofrecieron asilo diplomático a Snowden, siendo Rusia el país donde actualmente reside el informante.

Para cierta gente la creencia de que operar un sistema parte de la *Infraestructura de Claves Públicas* (PKI) no tiene dificultades más allá de seguir las directrices ya establecidas, quedó en entredicho en Marzo de 2011, cuando se falsificaron certificados de conocidas organizaciones suplantando el respaldo de una *Autoridad de Certificación* (CA) reconocida, como era en ese tiempo la empresa Comodo®. Parte de la investigación posterior involucró a una empresa italiana que era socia de Comodo y además resultaba un elemento importante en las relaciones de confianzas corporativas; también se señalaron problemas relativamente simples como el de que ciertos servicios informáticos empleaban el *Sistema de Nombre de Dominios (DNS)* para la resolución de nombres y no la variante *DNSSec* ue opera cifrada; un error poco aceptable en novatos. Un "hacker iraní" se atribuyó el ataque y esto generó mayor ruido en el problema; aún así, el suceso no reflejó fallas en el diseño de la arquitectura PKI, de hecho ésta de por si, provee esquemas formales para revocar certificados que fueron activados de inmediato, pero si reveló lo delicado y complejo de cuidar la aplicación de los procedimientos técnicos, al igual que la gran debilidad que produce el hecho de que los usuarios finales no comprenden verdaderamente el valor de un *certificado digital* cuando usan el *Protocolo de Capa de Enchufes*[9] *Seguros (SSL)* . También sembró dudas acerca de la exposición con la cual un programa navegador puede funcionar y su modo de interacción con el usuario que es quien aprueba o rechaza certificados. De cualquier forma, este no es el único caso de un CA comprometido, como una vez más se evidenció seis meses después, con la empresa alemana Diginotar® [10] , pero el modo como la empresa Comodo manejó el caso, la secuencia de fallas de seguridad y el crucial hecho de que

[9]En inglés la designación es "*Secure Socket Layer*" donde un socket es un enchufe lógico para que las aplicaciones se conecten a los sistemas en búsqueda de atención de servicios.

[10]Esta empresa se declaró más tarde en bancarrota y dos años después, en una programa de TV sobre el espionaje electrónico de la NSA a ejecutivos de la empresa brasileña PetroBras®, se indicó que fue la agencia estadounidense quien usó un ataque del tipo MITM para hacer fraude con los certificados de Diginotar, que fueron procesados en mensajes de correo electrónicos soportados por Google®. La evidencia de los señalamientos

la inseguridad alteró elementos de plena confianza en la estructura de seguridad Web, pusieron en tela de juicio la robustez práctica del esquema instrumental PKI. Tal vez la debilidad de todo el sistema interconectado, se mostró a través de una declaración del fundador y jefe ejecutivo de Comodo, cuando públicamente señaló "No hay seguridad 100 por ciento" para enseguida añadir: "Cualquier gran emisor de certificados digitales es susceptible a ataques concertados. Verisign y Comodo, ambas han tenido ese tipo de problemas." [McCullagh, 2011]

En 2013 otro suceso tuvo impacto sobre los especialistas del tema y se trata del ataque del gusano "Stuxnet" a equipos centrífugos, en plantas de desarrollo de tecnología nuclear de Irán, lo cual abrió la carrera de las *ciberarmas*. Es decir, se convirtió en un punto de quiebre en el área, dado que fue un gusano dirigido a un objetivo específico, que logró su objetivo y demoró considerablemente, el programa de desarrollo de la nación persa. [BBC News, 2010]

Esto fue una ruptura con el esquema tradicional de las infecciones digitales, que acostumbraban a contaminar y dañar la mayor cantidad posible de sistemas víctimas para pasar a ser un arma dirigida a un objetivo previamente designado. Para algunos especialistas, los ataques dirigidos a Estonia en el 2007 y a Georgia en 2008, representan el inicio de la *ciberguerra*, ya que se afectó a objetivos específicos y las razones que justificaron la agresión fue de índole político y militar. [Andress y Winterfeld, 2014]

Por su parte, Ross Anderson en el 2009 divulgó un Reporte Técnico del laboratorio de computación de la Universidad de Cambridge, en el que señaló el ataque de un *"malware social"*, inoculado por el correo electrónico, sobre personal de la oficina del Dalai Lama en el Tibet. Evento que supuso complicidad, permisividad o laxitud de controles de parte del gobierno chino para efectos de sacar ventaja con espionaje. De cualquier modo, lo crucial aquí es que expertos en el tema, sostienen que la complejidad y magnitud de esos instrumentos de ataques, demandan recursos que solamente una nación-estado puede proveer. La motivación y el uso posterior, generalmente con propósitos políticos, parecen reforzar esa idea. Adicionalmente, algunos técnicos en occidente han señalado varias veces, sin pruebas irrefutables, que China ha construido varias herramientas sofisticadas para instalar control, censura y restricciones a la navegación en Internet de su ciberespacio; el *"Gran Cortafuego de China*[11][Bu, 2013]-a veces visto como una gran muralla digital- y el *"Gran Cañón"* [Marczak et al, 2015] son vistos como medios sofisticados para corromper las consultas DNS, lanzar ataques de *"hombre en el medio"*,crear ataques de negación de servicios, bloquear direcciones IP y puertos lógicos, sabotear protocolos de transporte como TCP, restringir accesos a sitios webs específicos, impedir el tráfico de ciertas cuentas de correo electrónico, desviar tráfico a portales y buscadores locales, contaminar y comprometer navegadores de usuarios que accedan a sitios webs chinos. La Figura:

fueron documentos de manera que se le atribuyeron a la NSA estadounidense, relatando detalles técnicos de cómo sucedió la intrusión, aunque no estuvo claro si la NSA fue quien se aprovechó de la brecha abierta o también la detectó para posteriormente explotar su utilidad.

[11]Los términos "*Great Firewall of China*" o "Firewall (GFW)" fueron acuñados en 2002 por Charles Smith."

2 ilustra algunos sucesos que vinculan la tecnología de protección o la que perjudica, con estados naciones. Un giro que expandió las fuentes de los peligros en el ciberespacio de hoy.

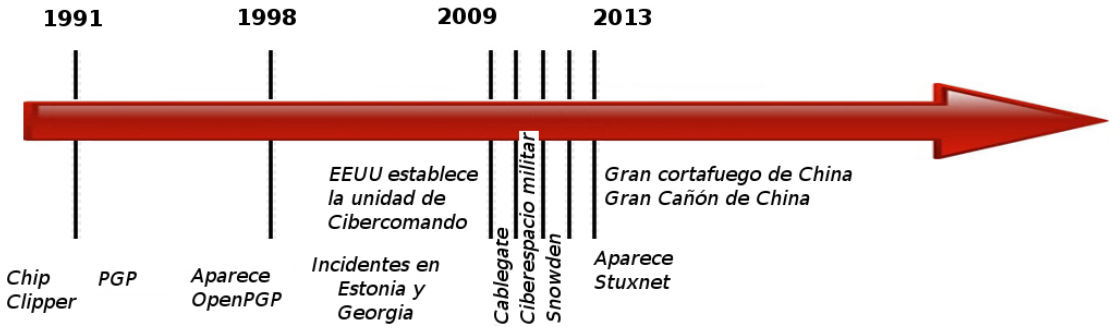

Figura 2: Intervenciones de las Naciones Estados en el mundo de la Seguridad del Ciberespacio. Fuente: Torrealba (2021)

No es de extrañar entonces que ya existan estudiosos del tema, que sostienen que se deben colocar reglas a este nuevo ámbito de acciones de confrontación. Tal es el caso de investigadores y académicos del Instituto de Internet en Oxford, que han emitido una advertencia pública, solicitando una doctrina que regule el empleo de la *Inteligencia Artificial (IA) en ciberarmas*. Un extracto de su artículo en la prestigiosa revista Nature, contiene la siguiente sentencia que resulta específica sobre las consecuencias del peligro que ellos perciben:

> El riesgo es una carrera de armas cibernéticas. A medida que los estados utilizan estrategias impulsadas por la Inteligencia Artificial que son cada vez más agresivas, sus oponentes, cada vez, responderán con más ferocidad. Tal círculo vicioso podría conducir a un ataque físico. [Taddeo y Floridi, 2018]

La Industria del delito cibernético y los sistemas críticos:

A la par de todo esto, el ciberespacio se ha vuelto un terreno virtual donde en las últimas décadas el crimen ha industrializado algunos modos de acción. El problema del "SPAM" es muestra de ello, ya que durante un tiempo fue poca la regulación legal y los controles técnicos, favoreciendo de ese modo la posibilidad de que individuos sin mucha reflexión ética sobre sus acciones, hicieran enormes fortunas monetarias a un bajo costo. En el libro del 2004, que escribió un sujeto que se presenta por el alias de "Spammer-X", se describen algunos modos y herramientas para operar en el cartel del envío masivo de mensajes de correo electrónico no solicitado. Un extracto de lo que sostiene ese autor, muestra el tipo de pensamientos que rodea a algunos sujetos de ese mundo:

> (...) Era la oportunidad de vender un producto u ofrecer un servicio a todo el mundo con muy poco o ningún gasto en publicidad. Por supuesto, esta idea estaba

> directamente unida a la idea de obtener enormes cifras de ventas y ganar millones para todos. Aunque, a efectos prácticos, no ocurrió de esa manera. Pero surgieron algunas cosas interesantes de las burbujas .com ,una de ellas es el correo no deseado. [Spammer-X, 2005]

Las consecuencias de ese tipo de problemas tecnológicos han llegado a ser tan agudas, que en el 2014 fue reportada una nevera que enviaba "*SPAM*". Y es que para ese instante ya se conocía lo que se denomina "*Botnet*", una palabra en inglés que se conforma a partir de la conjunción de la sílaba final del término "*Robot*" con la primera de "*Network*"; este término refiere a una red que puede usarse para enviar "*Spam*" u otras actividades que demanden alto volumen de tráfico en la red, por ejemplo, lanzar ataques de *Negación de Servicios Distribuidos (DDos)*. El asunto más importante es que actualmente este artilugio técnico puede conformarse por dispositivos del tipo *Internet de las Cosas (IoT)*, ya que muchas cámaras de vigilancia, consolas de vídeo juegos, sensores electrónicos en comercios[12], construcciones y edificios, dispositivos digitales de salud y sensores industriales modernos, tienen precarias protecciones para controlar su uso, a la vez que los protocolos que emplean son débiles en materia de seguridad. En consecuencia, apropiarse de estos dispositivos y estructurar una "Botnet" resulta atractivo, por que en modo semejante a lo que ocurre con grandes Bases de Datos de direcciones vigentes de correo electrónico, que son además verificadas, estos pueden comercializarse y resultan lucrativas en el bajo mundo de la Internet.

En 2010 el Laboratorio de Computación de Cambridge publicó un trabajo de investigación en un congreso de seguridad, donde se expuso una debilidad técnica en el *Protocolo de Pago Europay MasterCard VISA (EMV)*, que permitía hacer una operación en un sistema de tarjeta electrónica sin conocer el PIN de seguridad [Drimer, 2008] [Murdoch et al, 2010]. Esta grave vulnerabilidad afecta a gran cantidad de sistemas en el mundo que usan la tecnología Chip y PIN, la cual comúnmente se emplea en tarjetas de compras por débito. La respuesta del mundo comercial fue restarle importancia y sostener que eso no podía suceder en la realidad bancaria y las operaciones venta-compra diarias. Un problema que un año más tarde fue nuevamente comprobado por otros especialistas, quienes expresaron con énfasis que el protocolo "definitivamente estaba roto". También en el 2010 fueron noticias algunos proveedores de *"servicios en la nube"* como Google® que resultaron víctimas de ataques a sus plataformas, bajo operaciones que según se informó, pretendía espiar desarrollos tecnológicos. Sin embargo, para mucha gente los sucesos acaecidos pusieron al descubierto lo vulnerable de la nube. En 2013, 2014 y 2015 surgieron notables trabajos y noticias sobre implantes y sistemas médicos subvertidos, algunos usando la tecnología de *Redes Inalámbricas de Sensores (WSN)*, otros a través de vulnerabilidades en sus diseños, implementaciones y hasta sus configuraciones. A mediados de la segunda década de este milenio, también hubo noticias de repetidas debilidades en redes de sistemas complejos y críticos, como son los aeropuertos [Paganini, 2015]. Un año después, se reportaron formalmente incidentes en

[12]Tecnologías como RFID y WSN es común que se entremezclen con IoT.

varios aeropuertos. Otro caso emblemático de inseguridad que se relaciona con otra industria ya establecida, salió a flote públicamente en 2015 y fue la de los automóviles. Se divulgó a través de una conferencia "*BlackHat*", donde se expuso lo vulnerable de los autos "*Jeep Cherokee*" modelo 2014 [Drozhzhin, 2015]. Esta no fue la primera vez que se indicó de debilidades en sistemas de modernos autos comerciales, ya que en otra conferencia del 2010 -"*Defcon 18*"- se había expuesto como manipular un sistema de aire en los cauchos de vehículos.

Desde 2015 algunos fabricantes vienen expresando el deseo de que se regule el uso de robots y sistemas de Inteligencia Artificial como instrumentos mortales, siendo la "*Joint Conference on Artificial Intelligence* (IJCAI) 2017" en Australia, posiblemente la más reciente y noticiosa. Tal vez ello se deba a que 116 fabricantes especializados a través de una carta abierta, señalaron que usar robots de ese modo es "moralmente erróneo". Otro suceso de interés entre conocedores, fue que en Julio de 2016, después de 45 minutos de fallida confrontación armada con un francotirador, el jefe de policía de Dallas acordó emplear un robot *"Remotec Androx Mark V A-1"*, para vencer a su adversario que le estaba causando significativas bajas y no lograba neutralizar. En esa maniobra se dispuso que el robot portara una carga de explosivo C-4, de una libra aproximada y su accionar fue remotamente controlado para aplicar una acción ofensiva y mortal. La publicación "*The Register*" discutió sobre la importancia del suceso y a través de una nota, expresó una afirmación de una académica de leyes de ese país que abajo reproducimos:

> Otros estuvieron de acuerdo. "Hasta donde yo se, esto parece ser el primer uso intencional de un robot letal armado por la policía en los Estados Unidos" dijo Elizabeth Joh, profesora de leyes en la Universidad de California en Davis. [Thielman, 2016]

Existen también ámbitos más escandalosos y es la continuidad de los ataques en masa de ayer, pero en forma más sofisticada tecnológicamente[13] Así por ejemplo, en el primer trimestre de 2017, el *"ransomware"* denominado *"Wannacry"* causó estragos en más de 300 mil sistemas de todo el mundo, teniendo como llamativa víctima al sector de salud en la Gran Bretaña. Utilizando variadas técnicas que fueron desde el "*phishing*" a explotar vulnerabilidades del tipo *Servidor de Bloques de Mensajes (SMB)* en sistemas de *Microsoft*, este *malware* afectó numerosos equipos comerciales e industriales de casi una centena de naciones. Comúnmente procedía a cifrar el contenido de la información de los sistemas con el algoritmo de encriptado *AES-128 bits* y exigía el pago de un rescate en criptomonedas. Adicionalmente, se ha reportado que adicionalmente se aprovechó de programas de explotación computarizados que se basaron en vulnerabilidades que fueron robadas a la NSA, como por ejemplo *"Eternal Blue"* Y es que resulta necesario señalar que existe información que señala que desde el 2015, un arsenal de ciberarmas de una unidad élite de inteligencia estadounidense, perteneciente a la NSA, fue filtrado a la Internet por un grupo de Hackers denominado *"ShadowBrokers"*

[13]Desde el 2013, con *Stuxnet*, se puso en evidencia como los programas antivirus resultan inútiles para proteger de novedosas amenazas informáticas del software. Esto se ha repetido con otros ataques a gran escala.

Esta seria exposición potencialmente dejó en manos de cualquiera, programas que explotaban vulnerabilidades de sistemas comerciales e industriales que los fabricantes desconocían y en consecuencia, para los cuales aún no existían correctivos. Se les conoce como *Programas de Explotación del día cero* "Exploit 0 Day" y con frecuencia, hasta que los fabricantes se enteran, lo estudian y producen una respuesta, no se pueden contrarrestar.

En Abril de 2018 la empresa de seguridad informática "*F-secure*" reveló que había descubierto un modo de vulnerar viejos sistemas *Identificación de Radio Frecuencia (RFID)* que se empleaban en cerraduras electrónicas de hoteles, permitiendo de ese modo tomar el control de habitaciones, ascensores y garaje. Grave también resulta el hecho de que ese mismo año 2018, el US-CERT emitiera la alerta (TA18-074A) en la que se indica que desde el 2016, el gobierno ruso ha ejecutado repetidas actividades en el ciberespacio, intentando comprometer infraestructuras críticas de EE.UU. como son: electricidad, plantas nucleares, plantas de agua, sistemas de aviación y manufacturas vitales. Esta acusación, al igual que la realizada contra Corea del Norte por el caso de la empresa Sony®, plantean la hipótesis de que los estados naciones ejecutan actividades que traspasan el espionaje industrial para ubicarse en el control de los sistemas o la agresión que perjudica servicios de alto impacto. El apagón de seis (6) horas efectuado el miércoles 23 de Diciembre de 2015 sobre Ucrania, donde se aplicó el "*malware*" denominado *"BlackEnergy 3"* [E-ISAC y SANS-ICS, 2016] y que afectó a más de la mitad de la nación, parece integrar actores no necesariamente gubernamentales, pero con motivaciones políticas; sofisticados grupos que toman partido ideológico se hacen responsables cuando ocurren o se acentúan disputas entre naciones. Pero el panorama no está claro y aún prevalece mucho debate sobre la capacidad y forma de atribuir un cibertataque. Hay investigadores del Departamento de Guerra de la Universidad King, del Reino Unido, que han sostenido específicamente que: "(...) En un nivel técnico, la atribución es un arte así como una ciencia." [Rid y Buchanan, 2015] Luego han añadido que existe un ámbito no necesariamente binario: "(...) En un nivel operacional, la atribución es un proceso matizado, no un simple problema." [Rid y Buchanan, 2015] Para seguidamente ampliar la concepción del fenómeno de este modo: "(...) En un nivel estratégico, la atribución es una función de lo que es políticamente riesgoso." [Rid y Buchanan, 2015].

Todo esto ilustra como ahora, sucesos significativos y de alto impacto, inicialmente propios del área técnica, sirven de divergencia entre explicaciones científicas ortodoxas y positivistas, propias de la ingeniería y ciencias naturales, con otras que son interpretativas, cualitativas y significativas, siendo estas últimas más usadas en las humanidades. De manera que la frontera entre lo técnico y lo político se está acortando y además resulta difusa, por lo que las declaraciones que recogemos de los medios de comunicación son delicadas de considerar. En otras ocasiones las esferas políticas asumen posiciones radicales donde la anulación o el minimizar las tecnologías digitales modernas son la norma; ejemplo de ello son la reducción o ajustes de dispositivos con procesadores, cámaras, micrófonos y redes que el servicio secreto del presidente de los EE.UU. impone a cada mandatario que asume ese

rol. La disputa por el uso de la bicicleta "Peloton", de Joe Biden, muestra que esto sigue vigente.

Y es que hay ámbitos donde se sostiene que cadenas de desastres de seguridad ha conducido a pensar que actualmente el problema de inseguridad desborda las aproximaciones e instrumentos de protección modernas. Que la participación de diferentes actores, con distintos intereses y motivaciones, hace que los controles y protecciones modernos no sean prácticos y verdaderamente viables; que se demanda una revisión y un nuevo y profundo enfoque sobre las protecciones. Así por ejemplo en Abril de 2017, la publicación "*The Economist*" le otorgó su portada y centro de atención al problema y señaló que – los computadores nunca serán seguros-. Un extracto de su contenido expresó lo complejo de la realidad:

> Lejos del asunto de gran escala y gran estrategia, la mayor parte del hacking es vista como vandalismo o simplemente acciones criminales. Además, eso se está incrementando con facilidad. En foros oscuros se discuten detalles y se agiliza el comercio para robar tarjetas de crédito, vendiendo así lotes de información por miles de dólares a través de una única acción. Halcones negocian datos que se llaman "*exploits*" (explosivos), que vulneran programas y permiten a atacantes malignos subvertir sistemas. Usted también puede comprar "*ransomware*[14]", con el cual cifrar fotos y documentos en los computadores de sus víctimas, antes de exigirles que le paguen para entregarles la clave que descifrará los datos encriptados y de ese modo recuperarlos. Así de sofisticados son esos mercados de facilidades, que empaquetan las destrezas de programación y existen enteramente para proveer alternativas. *Botnets* que congregan manadas de computadores que han sido comprometidos con software como Mirai[15], y que pueden ser alquiladas por horas, para inundar sitios webs con tráfico, sacándolos fuera de línea hasta que se pague el rescate exigido. Así, tal como si fuera un negocio legítimo, por unos dólares extras, los guardianes de las *botnets* también proveen de soporte técnico si este se requiere o si algo no va como se desea. [The Economist, 2017].

La Figura 3, presenta notables eventos peligrosos relacionados con la tecnología moderna y las industrias. Se observa allí como los incidentes en esa área han crecido significativamente en este tercer milenio y se puede intuir, potenciales y crecientes consecuencias de esas amenazas en las futuras sociedades.

[14]Software para secuestrar información.

[15]Un código que permitió, ilegalmente, conformar una famosa red mundial de dispositivos del tipo Internet de las Cosas y ejecutar otros crímenes electrónicos.

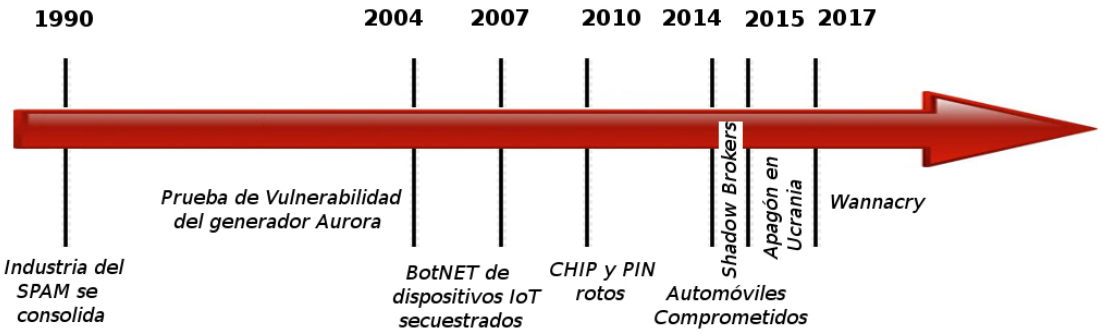

Figura 3: Principales acontecimientos vinculados con la Seguridad Cibernética Industrial.
Fuente: Torrealba (2021)

Áreas de inseguridad en el ciberespacio que hay que vigilar de cerca:

Ya hemos afirmado que a medida que la computación se expande y entrelaza en nuestras vidas, sus riesgos también se nos acercan y algunos tienen implicaciones que afectan a multitudes, a países o al mundo entero. Algunos de estos peligros modernos, con importantes consecuencias son:

- Automatización vulnerable de *Sistemas Electorales de Votación:*

  Existe una tendencia a automatizar las elecciones y en principio ello es comprensible, sin embargo, si eso no se realiza adecuadamente puede terminar generando un problema de alto impacto socio-político. Basta con observar lo ocurrido en las últimas elecciones presidenciales de EE.UU. en 2020 para comprender lo delicado y grave del tema. En noviembre del 2017 el reconocido profesor Matt Blaze, de la Universidad de Pensilvania, rindió testimonio en una audiencia ante la Casa de Representantes de EE.UU. para discutir la ciberseguridad de las máquinas de votación computarizadas en esa nación. Para esa ocasión el profesor que ha trabajado el tema por años expresó:

  > Hoy la integridad del voto depende enormemente de la integridad del software de los sistemas con los cuales las elecciones son conducidas -el software que corre en las máquinas de votación y en las redes de las oficinas de elección de los condados-. Cualquier debilidad de seguridad en algún componente de cualquiera de esos sistemas, puede servir como "enlace débil" y podría permitir que un actor maligno rompa las operaciones de la elección, alterando con precisión interesada los resultados o el derecho a votar de los electores. [Blaze, 2017]

- Incremento de la *Inteligencia Artificial (AI)* en sistemas críticos que incluyen toma de decisiones automatizadas:

  En general, el avance de la tecnología conlleva notables ventajas, pero también acarrea efectos adversos, que a veces se descuidan o se desconocen. Sin embargo, desde hace años algunas voces reconocidas, como la del científico Stephen Hawking, han alertado sobre algunas potenciales consecuencias de la AI. Incluso en prestigiosas revistas, como "Comunicaciones de la ACM" se ha presentado la controversia. Un ejemplo es un extracto de uno de sus números:

  > Alcanzar los beneficios del tremendo potencial de la AI para la gente y la sociedad requerirá estar vigilante y atento a los próximos y lejanos retos para establecer sistemas de computación robustos y confiables. Cada uno de los cuatro primeros retos presentados en este punto de vista (calidad de software, ciberataques, "aprendiz de brujo" y autonomía compartida) está siendo tratados por investigaciones vigentes, pero aún se requieren grandes esfuerzos. Urgimos a nuestros colegas, a la industria y a las agencias con fondos gubernamentales, para que dediquen más atención a la calidad del software, a la ciberseguridad y a la colaboración humano – computador de tareas, mientras incrementamos el soporte de la AI en funciones críticas para la seguridad. [Dietterich y Horvitz, 2015]

- Inseguridad de las Criptomonedas y sus repercusiones en los sistemas económicos:

  Algunos autores sostienen que las criptodivisas y criptoactivos son el quinto hito[16] del mundo de la computación, así como que por apoyarse en "funciones hash" y usar bloques de información cifrados, muchos piensan que esos sistemas son invulnerables. Eso no es cierto y con frecuencia hay brechas y mejoras en la seguridad de las criptodivisas [Weaver, 2018]. El año pasado el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó un trabajo que recoge los principales problemas de seguridad para Bitcoin, del cual vamos a extraer esta frase para respaldar la afirmación previa:

  > Bitcoin es la criptomoneda más popular y la primera que se ha sostenido desde el primer día en el mercado de la inversión de capital. Dado que tiene un modelo descentralizado con un ambiente no controlado, los *hackers* y ladrones han encontrado en el sistema de criptomoneda, un modo fácil para cometer fraude en las transacciones. [Conti et al., 2017]

[16] Para varios autores la aparición del "*Main Frame*", el surgimiento del "PC", el matiz de la Web para hacer de la Internet una red accesible a cualquiera y la plataforma de dispositivos móviles con redes sociales, serían las cuatro previas.

- Criptografía Post-cuántica:

  Se especula que las computadoras cuánticas acabarán con algunos de los algoritmos de cifrado más usados en nuestros días. Eso no es del todo exacto, pero toda mejora en prestaciones de sistemas, obliga a ajustar el tamaño de las claves secretas de muchos algoritmos para que estas pueda resistir *ataques del tipo fuerza bruta*. Con las computadoras cuánticas algo de eso será más agudo y por ello se está trabajando en el día después de que esas computadoras sean una realidad al alcance de cualquiera. En 2009 se publicó un texto dedicado al tema, en el cual el principal autor señalaba un plazo de tiempo, del cual ya han transcurrido casi una década. En el texto, para ese entonces, se expresó esto:

  > Entonces, ¿por qué tenemos que preocuparnos ahora por la amenaza de las computadoras cuánticas? ¿Por qué no continuar enfocándonos en RSA[17] y ECDSA?[18] ¿Y si alguien dentro de quince años anuncia la construcción exitosa de una gran computadora cuántica, por qué no simplemente cambiar a McEliece, etc. en ese momento?
  >
  > Esta sección ofrece tres respuestas, tres razones importantes por las que partes de la comunidad criptográfica ya empezó a enfocar su atención en la criptografía *postquantum*:
  >
  > - Necesitamos tiempo para mejorar la eficiencia de la criptografía post-cuántica.
  > - Necesitamos tiempo para generar confianza en la criptografía post-cuántica.
  > - Necesitamos tiempo para mejorar la facilidad de uso (usabilidad) de la criptografía post-cuántica.
  >
  > En resumen, todavía no estamos preparados para que el mundo cambie a criptografía post-quantum. Quizás esta preparación sea innecesaria. Tal vez en realidad ahora no necesitemos de la criptografía post-cuántica. Tal vez nadie nunca anunciará éxito en la construcción de una gran computadora cuántica. Sin embargo, si no hacemos nada y de repente al pasar los años los usuarios necesitan criptografía post-quantum, años de investigación crítica se habrán perdido. [Bernstein, 2009]

[17] RSA refiera al algoritmo de cifrado criptográfico de tecnología de clave pública con las iniciales de sus autores Rivest, Shamir y Adleman.

[18] ECDSA son las iniciales de algoritmo de firma digital de curvas elípticas.

- Explotación indebida de herramientas *bioinformáticas*:

  La interrelación entre la biología y la informática está presentando interesantes desarrollos, que tampoco están exentos de problemas de seguridad. Nuevos escenarios pueden surgir de esta interacción. Un notable ejemplo es el uso de secuencia de ADN como un tipo de "malware" que se inyecta en un sistema informático. Una porción del artículo que se presentó en un congreso científico señala que:

  > Nuestra investigación sugiere que hasta la fecha, el secuenciamiento y el análisis del ADN no han recibido -si las hubiera- significativa presión de adversarios. La pregunta clave que motiva nuestra investigación, es la siguiente: ¿Cuán robusta resultará la secuencia y el procesamiento entubado del ADN si se manifiestan presiones adversas? Esta línea de investigación plantea preguntas relacionadas con eso, tales como: ¿Son posibles los ataques basados en ADN? ¿Qué posibles consecuencias podrían ocurrir si un adversario compromete un componente del proceso de conducción del ADN? ¿Qué tan graves podrían ser esas consecuencias? Dado que el secuenciamiento del ADN progresa rápidamente hacia nuevos dominios, como son la medicina forense y el almacenamiento de datos de ADN [2, 9, 10, 15, 17], creemos que antes de proceder con la adopción masiva es prudente comprender los actuales desafíos de seguridad en la progresión del secuenciamiento del ADN. [Ney et al, 2017]

- Software con potencialidad para falsificar vídeos y declaraciones:

  Desde hace varias décadas existen técnicas para alterar vídeos y grabaciones cinematográficas que presentan imágenes que a los ojos de muchos parecen reales, pero no lo son. Se trata de alteraciones con programas de computadoras que permiten rejuvenecer a alguien, suplantar a otra persona y hasta crear participaciones en un filme, que nunca sucedieron. Sin embargo, eso es hecho en tiempo no real y demanda muchos recursos. A pesar de eso, los avances en materia de manipulación de vídeos están haciéndose más comunes, económicos y en tiempo real. Y aunque eso no es en sí un desarrollo en el área de la seguridad digital, sus efectos si se vinculan con esta área. Seguidamente transcribimos una porción de un trabajo que ha llamado la atención por la calidad del producto resultante:

  > (...) En contraste con los previos enfoques de recreación que se ejecutan fuera de línea [5, 11, 13], nuestra intención es la transferencia en línea de expresiones faciales capturadas por un sensor RGB, provenientes de una fuente con un actor hacia otro actor, como su objetivo final. La secuencia en el objetivo destino puede ser cualquier vídeo monocular; por ejemplo, metraje legalmente

> descargado de vídeos de Youtube con un buen rendimiento facial. Nuestro propósito es modificar el vídeo objetivo de una forma tan foto-realista, que sea virtualmente imposible notar la manipulación. La fiel recreación facial foto-realista es la base para una variedad de potenciales aplicaciones; por ejemplo, en las videoconferencias, la alimentación de vídeo se puede adaptar para que coincida con el movimiento de la cara de un traductor, o los vídeos de la cara se pueden doblar de manera convincente a un idioma extranjero. [Thies et al, 2016]

- Violación repetida a la Privacidad de los Datos de los usuarios de servicios.

Una angustia creciente entre los Internautas es poder usar la red, sus aplicaciones y servicios sin ver comprometida su privacidad de datos. Y es que en ese ámbito existen fuertes intereses para explotar esa información, a veces comercial y otras políticamente, de una forma tan peculiar que incluso se dan dicotomías extrañas cuando algunos estados, promulgan leyes para resguardar y proteger la privacidad mientras que con sus entidades de inteligencia, actúan deliberadamente para violarla. El experto alemán Holvast ha sido claro en señalar el problema de trasfondo, cuando expresó:

> Se puede jugar un papel más activo cuando el consumidor o ciudadano puede usar medios técnicos, pero también para este caso es la política y el gobierno quien determina cuándo y cómo se pueden usar esas técnicas. El gobierno es quien quiere controlar el uso de la información y se niega a fortalecer la posición del individuo. Por esa razón, casi todo el énfasis está en el control reactivo de las problemas de privacidad. Si se les da alguna forma de control participativo, siempre se provee bajo la restricción de que, al final, será el gobierno quien tendrá el control final. Solamente en relación con la industria, el rol del consumidor se legaliza con respecto al uso de las galletas de software (cookies) y al correo electrónico no solicitado (spam). [Holvast, 2009]

Por su parte, muchas empresas han asumido el papel de ofrecer servicios y a la vez, incorporar los mecanismos para que los usuarios decidan cómo y cuando comparten su información. Ese modelo parece válido, pero de nuevo sus conflictos internos parecen resultar obstáculos de peso para lograr la meta. El reciente escándalo de Facebook® y Analytica® sirve para ejemplificar lo engorroso de la realidad. Un problema que llevó al fundador y más alto directivo de Facebook a testificar ante una comisión del Congreso de EE.UU. y expresar:

> Pero ahora está claro que no hicimos lo suficiente para evitar que estas herramientas se usen también para hacer daño. Eso se aplica a las noticias

> falsas, a la interferencia extranjera en elecciones y al discurso de odio, al igual que con los desarrolladores y con la privacidad de los datos. No tuvimos una visión suficientemente amplia de nuestra responsabilidad y eso fue un enorme error. Fue mi error y lo siento. Inicié Facebook, soy quien lo conduce y soy el responsable de lo que allí sucede. [Zuckerberg, 2018]

- Actos de Ciberguerra sin un marco común de legislación mundial.

La guerra es una desavenencia significativa entre partes en conflicto, que comúnmente altera un estado de paz o normalidad social. Recientemente se asocian las acciones hostiles en Internet, o sobre sistemas pero que acontecen a través de esta, con la esfera cibernética de la guerra. Estas operaciones pueden extenderse sobre otros sistemas tecnológico como son los drones y los robots, para entrelazar las peligrosas consecuencias físicas de la guerra tradicional con las de los ciberconflictos. De forma que cuando las acciones de ataques y defensas deliberadas, se vinculan con intereses políticos de las partes, resulta posible referirse a los mismos, como actos de ciberguerra. Ya algunas naciones han declarado que se reservan el derecho de responder a agresiones de ciberguerra, con medidas propias de sus jurisdicción. Así por ejemplo el secretario general de la Organización del Tratado del Atlántico Norte (OTAN), hace poco escribió:

> Para la OTAN un serio ciberataque podría activar el artículo 5 de nuestro tratado fundacional. Esto es, nuestro compromiso de defensa colectiva, donde un ataque contra un aliado es tratado como un ataque contra todos. Nosotros hemos designado al ciberespacio como un dominio en el cual la OTAN operaría y se defendería a sí misma, tan efectivamente como lo hace en el aire, en la tierra y en el mar. Esto significa que nosotros detendríamos y nos defenderíamos contra cualquier agresión hacia los aliados, tanto que esta ocurra en el mundo físico como que suceda en el virtual. [Stoltenberg, 2019]

Por otro lado, en Octubre de 2012 el presidente estadounidense Barack Obama promulgó la Directiva Presidencial de Política número 20 (PPD-20) para definir la política de ciberoperaciones de esa nación, que no fue expuesta al público en modo directo pero que un año más tarde, como parte del material filtrado por Edward Snowden, el periódico británico "*The Guardian*" divulgó. A partir de entonces, un documento expuesto en la red, que pretende ser esa directiva, contiene lo siguiente:

> El gobierno de los Estados Unidos deberá reservarse el uso de tales respuestas a circunstancias cuando la defensa de la red y las medidas de las agencias de seguridad estatal, sean insuficientes o no puedan ser puestas a tiempo para mitigar la actividad ciber maliciosa (...) [US PPD-20, S/F]

Esto es parte de los elementos que muestran como en nuestro días, algunas naciones del mundo tratan un tema tan delicado y ayuda a comprender que la carencia de una normativa específica internacional, en el ámbito jurídico, que no facilita los juicios legales de los actos que puedan suceder. Semejante debilidad deja espacio abierto para que ocurran delicados conflictos y diatribas, con cercanía a actos clásicos de guerra y sus trágicas consecuencias. Y es que la entrada de naciones-estados como potenciales actores ofensivos sobre el ciberespacio, es algo que impactaría sensiblemente las aproximaciones defensivas tradicionales, haciendo que muchas de las premisas establecidas en los esquemas y mecanismos de protección, resulten inútiles o al menos más fácilmente vulnerables. Al momento de escribir este trabajo ya algunas naciones han acusado a otras de efectuar actos incorrectos para dañarles, son algunos ejemplos de eso el caso del año 2016, cuando funcionarios gubernamentales de EE.UU. acusaron a Rusia de interferir durante sus elecciones presidenciales, o el de Venezuela, que en 2019 tras sufrir una grave caída del servicio eléctrico de impacto nacional, señaló a EE.UU. como el promotor de un ataque hostil con base a la tecnología de *Pulso Electro Magnético (PEM)*.

Retomando una vieja apreciación para mejorar la defensa:

Proveer protección a los servicios de seguridad del ciberespacio, una plataforma socio-técnica dinámica y compleja, donde surgen novedosas amenazas resulta algo retador y difícil. Las respuestas que se deban proveer deberán ir más allá de colocar uno u otro artefacto de protección, ya que está visto que las soluciones que se requieren trascienden del ámbito técnico para conformar sistemas con participación humana, dentro de marcos jurídicos previamente establecidos, algo que hace mayor la dificultad para predecir ese complicado todo. Una alternativa es trabajar partiendo de que siempre habrá áreas desconocidas y que la esencia de los problemas de inseguridad es donde hay que poner la atención de primero. Esto es retomar un principio científico universal, que el matemático Bronowski describió el pasado siglo en una serie de TV británica de nombre El Ascenso del Hombre:

> Heisenberg llamó a esto el Principio de Incertidumbre. En un sentido, este es un principio robusto de todos los días. Sabemos que no podemos pedir al mundo que sea exacto. Si un objeto (una cara familiar, por ejemplo) tiene que ser exactamente la misma antes de que la reconozcamos, nunca la reconoceríamos de un día al otro siguiente. Nosotros reconocemos al objeto para que sea el mismo dado que este es mucho más que el mismo; nunca es exactamente igual a como fue, es tolerablemente igual. En el acto de reconocimiento, un juicio es construido -un área de tolerancia ante la incertidumbre. Así que el principio de Heinsenberg dice que no hay eventos, ni siquiera los eventos atómicos, pueden ser descritos con certidumbre, esto es, con tolerancia cero. [Bronowski, 1973]

De forma que las aproximaciones puntuales y segmentadas a requerimientos específicos, las recetas predefinidas de los libros clásicos, deben ser subordinadas ante el análisis completo, que inicie explorando las raíces de confianza del sistema, descubra los principios de seguridad

intrínsecos en cada mecanismo y termine en procedimientos y protocolos funcionales, que puedan ser examinados y hasta auditados en su eficacia y eficiencia. En otras palabras, la simple atención de los requerimientos de inseguridad, sin examinar en paralelo el progreso de la industria del cibercrimen, al igual que considerar la dinámica de los roles de actores como son los estados-naciones, la de los intereses de proveedores de tecnología de protección y de los prestadores de servicios de resguardo, sería algo incompleto. De actuar así, se corre el riesgo de ignorar los recursos y motivaciones del atacante, algo que en la práctica puede modificar las posibilidades reales de subversión y compromiso de un sistema. Y es que no son iguales las probabilidades de triunfo y dedicación que puede tener un grupo de jóvenes ciberdelincuentes, que las que posee una fuerza organizada y disciplinada como son aquellas de tipo cibercomando o inteligencia de un estado-nación. Una aproximación limitada facilita una percepción engañosa y la respuesta posiblemente sea inapropiada. Adicionalmente, el abuso de posiciones de poder así como el sabotaje deliberado, ya son figuras conocidas con incidentes reales, cosa que demanda al menos una deliberación antes de proponer una solución centrada en lo técnico. Y es que todas esas consideraciones, plenas de incertidumbre, pueden alterar por completo la formulación de un plan defensivo, así como la de los mecanismos de salvaguarda a aplicar.

La ciudadanía debe entender además que la mayoría de los fabricantes y desarrolladores de soluciones de protección, dan preferencia a infraestructuras corporativas o que funcionen con apoyo de organizaciones, dejando relegados los enfoques de control comunitarios así como no indicando, claramente, la frágil exposición de muchos dispositivos tecnológicos de uso particular. Por su parte, el ente que tradicionalmente los representa, para obligar a que quienes comercian con tecnología lo hagan de modo seguro, los gobiernos, parecen tener un conflicto de interés en esto al asumir sus otras atribuciones de seguridad y control social. Así fue posible que hubiese receptividad en el gobierno alemán ante la sospecha de que un teléfono móvil de tecnología celular, como era el de la canciller Ángela Merkel, pudiera haber sido interceptado y espiado por la inteligencia estadounidense.[MacAskill, 2015]

Otro punto a considerar es que la experiencia vivida en otras áreas de la seguridad, como es la seguridad física, hace tiempo que ha mostrado como los problemas pueden llegar a aumentar y sobrepasar las respuestas aisladas. Hay reportes de casos donde grupos de guardianes ceden ante la corrupción y cruzan la línea para actuar como delincuentes, al igual que es reconocido que ciertos fabricantes dan prioridad a sus intereses comerciales, antes que la seguridad de sus clientes. En el ámbito de la ciberguerra, aún no regulado, también se han hecho declaraciones donde se deja entrever que las respuestas ofensivas forman parte del repertorio de posibilidades por parte de entes oficiales [Corfield, 2019]. Por todo lo anterior resulta cada vez más difícil instrumentar soluciones genéricas, mientras los árboles de amenazas sobre cada objeto siguen creciendo.

De manera que la conformación de grupos de trabajo multidisciplinarios y con una *visión*

holística, serán indispensables para proveer aportes para el tratamiento de la incertidumbre con verdaderas protecciones técnicas digitales, apegadas a los marcos legales -que deberán también actualizarse- que accionen más sobre áreas de inseguridad que sobre necesidades puntuales y que puedan interpretarse o evaluar, como servicios bajo estricta vigilancia, sean estos últimos que operen en modo aislado o en conjunto. Un ejemplo específico de todo esto, es estudiar sobre un sistema cualquiera su funcionamiento, lógico y el real, luego se debe determinar si durante la operación de su esquema de seguridad/inseguridad el mismo se apega al principio del *menor privilegio*,o si se adapta a una estrategia de *protección a través de la oscuridad*. Esas respuestas permiten entender la operación macro más allá de si le urge un esquema de control del acceso o de filtrado de operaciones. A eso se puede llegar más tarde, pero teniendo en cuenta el comportamiento global del sistema, sus elementos confiables, críticos, las ventanas de exposición o debilidades y otros aspectos que proveen una imagen más amplia. En seguida se puede dibujar el árbol de amenazas y establecer cualquier esquema que exprese la *gestión del riesgo* que estará presente y guiará las defensas a fijar o mejorar. Es en ese instante cuando se puede pensar en la guía de los servicios de seguridad y especificar las respuestas con el nivel de detalle que se desee. Si se aplica ese tipo de aproximación, se debe poder establecer los esquemas de evaluación y control de lo que se instrumente.

Cuando se construya las amenazas, es deseable que se examine la evolución histórica y el estado de la industria, así como lo que ocurre comúnmente y la dinámicas de los roles de los participantes. Así por ejemplo, al momento de escribir este artículo, se ha publicado noticias en foros de seguridad de sistemas informáticos, acerca de un ataque a los sistemas basados en la falsificación de las bibliotecas abiertas de funciones y métodos que soportan su programación [Schneier, 2021]. De manera que se tiene evidencia de que atacantes han colocado bibliotecas de software trampeadas, con programas dañinos, que presentan las mismas interfaces de programación y que si no son cuidadosamente revisadas antes de emplearlas, pueden engañar a desarrolladores que desconozcan esos peligros. Esta es una moderna aplicación del viejo truco del *Caballo de Troya*, que desde hace décadas ocurre, pero que requiere nuevas formas de engaño para poder funcionar. Esta amenaza vá más allá de instalar una contramedida técnica común, ya que lo que verdaderamente exige para un fabricante, es comprobar que los procedimientos que usa para la verificación de software de terceros sea examinado y se pueda constatar que no será burlado. En el caso de un cliente, la contramedida pudiera ser, para aquellos casos donde únicamente el fabricante conoce la estructura del software del sistema, el de comprobar la *integridad del software* que se le provee. Ello aplicaría si el fabricante ha diseñado un sistema donde únicamente él tiene el conocimiento y control de lo interno del sistema, algo parecido a la pauta de seguridad a través de la oscuridad. Para los ingenieros de software que programan el sistema la seguridad a través de la oscuridad pudiera darse con el software de terceros, este pudiera estar oculto a sus ojos y allí radicaría la vulnerabilidad del artefacto de software que ellos construyen. Se puede apreciar entonces, que este modo de obrar para responder es más amplio que el de la simple consideración de un problema con un servicio de seguridad -*integridad del código*- y emitir una respuesta clásica. El trasfondo real es la dinámica común

de los desarrollos de software y sus modificaciones, algo delicado sobre el cual los especialistas en el tema tienen tiempo advirtiendo:

> Si los sistemas que usted escribe no manejan apropiadamente los cambios, tarde o temprano usted tendrá problemas de seguridad, ya sean estos leves o graves. [Johnsson et al, 2019].

Corolario:

En materia de ciberseguridad los tiempos actuales demandan aplicar políticas, paradigmas, estrategias y respuestas coordinadas en forma de ingeniería de la seguridad, que tomen en consideración una visión histórica, panorámica, multifactorial e integral de los problemas. La mera respuesta técnica, característica de procesos entrelazados con la ingeniería industrial y de producción del siglo XX, viene siendo sobrepasada desde las últimas décadas, por lo que se puede esperar que los próximos retos críticos en el área afectarán notablemente el funcionamiento tradicional de las sociedades. Nuevas perspectivas deben ser formuladas, más resistentes a la confusión y visión restringida, para posteriormente ser aplicadas con miras a sostener eficazmente la gobernabilidad y economías electrónicas, que por las interconexiones de sistemas tecnológicos, funcionan en modo o con dependencia global. Por su parte, las comunidades y ciudadanos deben entender que urgentemente requieren generar soluciones a sus medidas y necesidades, ya que comúnmente los desarrollos de protección comerciales van dirigidos hacia infraestructuras tecnológicas de organizaciones, al igual que a menudo, demandan o se expresan para conocedores o entendidos en el tema. Un buen punto de partida para defender sus derechos en el ciberespacio es concentrarse en los aspectos que enunciamos como notables de atención.

Bibliografía

[Anderson, 2001] Anderson, R. (2001). *Security Engineering: A guide to building dependable distributed systems.* (Second Edition,). United Kingdom: Wiley.

[Andress y Winterfeld, 2014] Andress, J. y Winterfeld, S. (2014). *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners.* (Second edition). Amsterdam: Elsevier, Inc.

[Baldwin, 1997] Baldwin, D. (1997). The concept of security. *Review of International Studies.*Vol. 7, No. 1 - Vol. 41, No. 5. Recuperado de https://www.jstor.org/journal/revinterstud?refreqid=excelsior%3A1ff7d0d55bb9e49034af2451d949ca82.

[BBC News, 2010] BBC News. (26 de Septiembre de 2010). *Stuxnet worms hits Iran nuclear plant staff computer.* [Página Web]. Disponible: https://www.cnet.com/news/comodo-hack-may-reshape-browser-security/

[Bernstein, 2009] Bernstein, D. (2009). *Introduction to post-quantum cryptography.* (First Edition). Berlin: Springer.

[Blaze, 1994] Blaze, M. (1994). Protocol Failure in the Escrowed Encryption Standard. *AT&T Bell Laboratories*. Recuperado de https://www.mattblaze.org/papers/eesproto.pdf.

[Blaze, 2017] Blaze, M. (Noviembre de 2017). US House of Representatives. Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee Intergovernmental Affairs. Hearing on Cybersecurity of Voting Machines. University of Pensylvania. Recuperado de https://www.govinfo.gov/content/pkg/CHRG-115hhrg30295/pdf/CHRG-115hhrg30295.pdf.

[Boo, 2016] Boo, H-W. (2016). *An Assessment of North Korean Cyber Threats*. NIDS International Symposium of Security Affairs. Capítulo 2. http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf

[Bronowski, 1973] Bronowski, J. (1973). *The Ascent of Man.* (Primera edición). British Broadcasting Corporation. Macdonald Futura Publishers.

[Bu, 2013] Bu, R. (2013). *The Great Firewall of China.*. [Página Web]. Recuperado de: http://campus.murraystate.edu/academic/faculty/wlyle/540/2013/Bu.pdf

[Castells, 2010] Castells, M. (2010) *The Age of Information. Economy, Society and Culture.* (Second Edition,Vol I). USA: Wiley – Blackwell.

[Ceruzzi, 2003] Ceruzzi P. (1998). *A History of Modern Computing* (Second Edition). Londres: The MIT Press.

[CIA, 1981] Central Intelligence Agency, CIA (1981). Deception Maxims: Fact and Folklore. Deception Research Program. C00036554. XD-OSD/NA. *Office of Research and Developmen*. Recuperado de https://www.governmentattic.org/18docs/CIAdeceptionMaximsFactFolklore_1980.pdf.

[Conti et al., 2017] Conti, M., Kumar E., Sandeep, L., Chhagan, L. y Sushmita, R. (2017). A Survey on Security and Privacy Issues of Bitcoin. *ArVix 2017.* Recuperado de https://arxiv.org/pdf/1706.00916.pdf.

[Corfield, 2019] Corfield, G. (27 de agosto de 2019). *We will hack back if you tamper with our shiz, NATO declares to world's black hats.* [Página Web]. Disponible: https://www.theregister.com/2019/08/27/nato_repeats_article_5_cyber_attack_bombast_again/

[Denning, 1982] Denning, D. (1982). *Cryptography and Data Security.* (First Edition). Estados Unidos: Addison-Wesley Publishing Company, Inc.

[Dietterich y Horvitz, 2015] Dietterich, T. y Horvitz, E. (2015). Rise of Concerns About AI: Reflections and Directions. *Communications of the ACM,*. 58 (10). 38-40.

[Drimer, 2008] Drimer, S. (2008). *Security Vulnerabilities of Chip and PIN.* [Internet]. Recuperado de: https://murdoch.is/talks/ccc10chipbroken.pdf

[Drozhzhin, 2015] Drozhzhin, A. (6 de Agosto de 2015). *Black Hat USA 2015: the full history of how that Jeep was hacked..* [Página Web]. Disponible: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

[E-ISAC y SANS-ICS, 2016] E-ISAC y SANS-ICS. (2016). *TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case..* [Página Web]. Disponible: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[El País, 1995] El País (1995). *Un 'pirata' informático entra en el sistema del Citibank y provoca alarma en la banca.* [Internet]. Madrid: El País. Recuperado de: https://elpais.com/diario/1995/08/19/economia/808783221_850215.html

[Esmenger, 2010] Esmenger N. (2010). *The Computer Boys Take Over* (First Edition). Londres: The MIT Press.

[Goldstein, 2004] Goldstein, E. (2004). The Army needs more Blueboxes. *2600, The Hacker Quarterly* . 21(1).

[Greenwald, 2014] Greenwald, G. (2014). *Snowden sin un lugar donde esconderse* (Primera edición). Estados Unidos: B de Books.

[Holvast, 2009] Holvast, J. (2009). History of Privacy. *IFIP AICT*. 298, pp. 13-42. Recuperado de https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf.

[Johnsson et al, 2019] Johnsson, D., Deogun, D. y Sawano, D. (2019). *Secure by Design.* (First Edition). London: Manning publications co.

[Lennon, 2011] Lennon, M. (2011). *Department of Defense: Cyberspace is a New Warfare Domain. Wired Bussiness Media.* [Página Web]. Disponible: https://www.securityweek.com/department-defense-cyberspace-new-warfare-domain

[Lucas, 2006] Lucas, M. (2006). *PGP y GPG. Email for the Practical Paranoid.* (1st ed). United States of America: PGP and GPG.

[MacAskill, 2015] MacAskill, E. (12 de Junio de 2015). *Germany drops inquiry into claims NSA tapped Angela Merkel's phone.* [Página Web]. Disponible: https://www.theguardian.com/world/2015/jun/12/germany-drops-inquiry-into-claims-nsa-tapped-angela-merkels-phone

[Marczak et al, 2015] Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R. y Vern P. (2015). An Analysis of China's "Great Cannon". *6Th USENIX Workshop on Free and Open Communication*

on the Internet, FOCI'15. Recuperado de https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf.

[McCullagh, 2011] McCullagh, D. (Abril de 2011). *Comodo hack may reshape browser security.* [Página Web]. Disponible: https://www.cnet.com/news/comodo-hack-may-reshape-browser-security/

[Meserve, 2007] Meserve, J. (26 de Septiembre de 2007). *Sources: Staged cyber attack reveals vulnerability in power grid.* [Página Web]. Disponible: http://edition.cnn.com/2007/US/09/26/power.at.risk/

[Mudge et al., 2009] Zatko, P., Stickley, J., Nichols, E., Wang, C., Bellis, E., Edelman, B.,Zimmermann, P., Callas, J., Wang, K., Curphey, M., McManus, J., Routh, J., Sabett, R., Chuvakin, A., Geyer, G., Dunphy, B., Wayner, P., Wood, M., Francisco, F. (2009). *Beautiful Security.Leading Security Experts Explain How They Think.* [O'Reilly Media, Inc.]. Estados Unidos. Disponible: https://b-ok.lat/book/701981/3e24da?id=701981&secret=3e24da

[Murdoch et al, 2010] Murdoch, S., Drimer, S., Anderson, R. y Mike, B. (2010). Chip and PIN is Broken. *2010 IEEE Symposium on Security and Privacy.* Recuperado de https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf.

[Ney et al, 2017] Ney, P., Koscher, K., Organick, L., Ceze, L. y Tadayoshi, Kohno. (2017). Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More. USENIX Security Symposium. Vancouver, BC, Canada. Recuperado de https://atc.usenix.org/system/files/conference/usenixsecurity17/sec17-ney.pdf.

[Paganini, 2015] Paganini. P. (2015). *Hacking airport security systems with a common laptop. Security Affairs.* [Página Web]. Disponible: https://securityaffairs.co/wordpress/39239/cyber-crime/hacking-airport-with-laptop.html

[Ralston, 1976] Ralston, A. (1976). *Encyclopedia of Computer Sience.* (First edition). Estados Unidos: Mason Charter Publishers Inc.

[Rid y Buchanan, 2015] Rid, T. y Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies.*38 (1-2), 4-37. Recuperado de http://dx.doi.org/10.1080/01402390.2014.977382.

[Schneier, 2000] Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World.* (15th Anniversary Edition). United Kingdom: Wiley.

[Schneier, 2010] Schneier, B. (Octubre de 2010). Reconceptualizando la seguridad. *Technology Entertainment Design Conferences LLC.* University Park, Pensilvania, Estados Unidos.

[Schneier, 2021] Schneier, B. (2021). *Dependency Confusion: Another Supply-Chain Vulnerability. Schneier on Security.* [Página Web]. Disponible: https://www.schneier.com/blog/archives/2021/02/dependency-confusion-another-supply-chain-vulnerability.html

[Senge, 1998] Senge, P. (1998). *La Quinta Disciplina.* (Primera edición). Estados Unidos: Ediciones Juan Granica, S.A.

[Spafford, 1988] Spafford, E. (2008). The Internet Worm Program: An Analysis. *Purdue e-Pubs. Department of Computer Science Technical Reports.* Paper 702. 88-823. Recuperado de http://bit.ly/4vb34F.

[Spafford, 1989] Spafford, E. (1989). Computer Recreations: Of Worms, Viruses and Core War. *Scientific American.* pp 110.

[Spammer-X, 2005] Spammer-X. (2005). *SPAM* (Primera edición). E Anaya Multimedia , SA.

[Stoltenberg, 2019] Stoltenberg, J. (2019). NATO Will Defend Itself. Cyber Resilience. *Prospect Magazine.* Recuperado de https://www.prospectmagazine.co.uk/content/uploads/2019/09/Cyber_Resilience_October2019-2.pdf.

[Taddeo y Floridi, 2018] Taddeo, M. y Floridi, L. (16 de Abril de 2018). *Regulate artificial intelligence to avert cyber arms race.* [Página Web]. Disponible: https://www.nature.com/articles/d41586-018-04602-6

[TEDtalk, 2010] TEDTalk. (2010). *Reconceptualizing Security.* Technology Entertainment Design Conferences LLC. PennState University. October 10, 2010. Video en formato MP4 que fue descargado de: https://www.youtube.com/watch?v=CGd_M_CpeDI

[Tessier, 2011] Tessier, S. (2011). *The Future of Cybersecurity.* [Página Web]. Recuperado de: http://hcss.nl/sites/default/files/files/reports/CybersecurityStrategy_Change_Paper_04_webversie_(2).pdf

[The Economist, 2017] The Economist. (2017). Computer Security. Everything is hackable. *Science & technology.* 66-68.

[Thielman, 2016] Thielman, S. (8 de Julio de 2016). *Use of police robot to kill Dallas shooting suspect believed to be first in US history.* [Página Web]. Disponible: https://www.theguardian.com/technology/2016/jul/08/police-bomb-robot-explosive-killed-suspect-dallas

[Thies et al, 2016] Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C. y Nießner, M. (2008). "Face2Face: Real-Time Face Capture and Reenactment of RGB Videos,"2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2387-2395, Recuperado de https://arxiv.org/abs/2007.14808.

[US PPD-20, S/F] US PPD-20. (S/F). *Presidential Policy Directive/PPD-20. Memoradum.* [Internet]. Recuperado de: https://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf

[Weaver, 2018] Weaver, N. (2018). Inside risks: Risks of cryptocurrencies. *Communications of the ACM*. 61(6), 20-24.

[Wook Boo, 2016] Wook Boo, H. (Julio de 2016). An Assessment of North Korean Cyber Threats. International Symposium on Security Affairs 2016 Tokyo, Japan. Chapter 2. http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf

[Zimmermann, 1999] Zimmermann, P. (1999). *Why I wrote PGP. PGP's user guide.* (1st ed.,Vol I). United States of America: Pretty Good.

[Zuckerberg, 2018] Zuckerberg, M. (2018). *Testimony to Congress on Cambridge Analytica.* [Página Web]. Disponible: https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978