TRABAJO FINAL DE INVESTIGACIÓN

TEMA:

Operaciones Particulares - Ciberdefensa: Comando y Control

TÍTULO:

Redes integradas de información ante la amenaza cuántica

AUTOR: Capitán Leonardo Emmanuel Szczupak

TUTOR: Coronel Ernesto Claudio Ballofet

Año 2022

Resumen

El usufructo, dominio o monopolio de la información cobra especial y proporcional relevancia conforme el devenir de los tiempos. Esta perogrullada entraña cuantiosos elementos a considerar, desde la posesión de datos fehacientes al momento de la toma de decisiones, la producción de inteligencia, el comando y control de las operaciones hasta la acción psicológica sobre el adversario. Por esta razón, sendos esfuerzos son direccionados en la agrupación, almacenamiento, oportuna distribución y protección de la misma. Así se estructuran complejas redes constituidas por bases de datos, servidores y vías de comunicación para obtener el máximo provecho en virtud de las necesidades particulares, explotando la conectividad permanente y la integración de distintos elementos, sistemas y subsistemas.

Por otro lado, los computadores cuánticos suponen una revolución sin precedentes, que no limita su repercusión al campo de la informática, sino también, a la humanidad en sí. Esta valía se fundamenta en la capacidad de procesamiento, siendo exponencialmente superior a los procesadores electrónicos convencionales. Conforme se avizoran tales horizontes, también inician las contemplaciones respecto a las posibles aplicaciones que de estos pudieran hacerse, una de ellas es la penetración y afectación de redes de información sensibles. Por esta causa, el presente trabajo de investigación versa respecto a la vulnerabilidad de las redes de información integradas frente a la eventual incursión por parte de computadores cuánticos, y las perspectivas y balances que de esta combinación se extraigan. A tal fin, se consideran y describen las estructuras actuales de redes informáticas en la nube e internet de las cosas; como también, los avances y potenciales virtudes de las nuevas tecnologías, el panorama actual y próximo en relación a la temática.

Palabras clave

Ciberseguridad – Amenazas – Comando – Cuántica – Internet

Índice

Introducción

"Vivimos en una sociedad profundamente dependiente de la ciencia y la tecnología y en la que nadie sabe nada de estos temas. Ello constituye una fórmula segura para el desastre"

Carl Sagan.

El proceso de toma de decisiones se fundamenta en la información disponible, ya sea del ambiente, del enemigo y/o propia. No en vano Sun Tzu (Cap. 4 pág. 10) alecciona:

> "Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca saldrás derrotado. Si eres ignorante de tu enemigo, pero te conoces a ti mismo, tus oportunidades de ganar o perder son las mismas. Si eres ignorante de tu enemigo y de ti mismo, puedes estar seguro de ser derrotado en cada batalla."

Así, el contar con datos precisos y oportunos significa una ventaja crucial para hacer frente a cualquier problema o plan a futuro. Además, un sistema versátil permite recoger información en tiempo real que, a su vez, posibilita contener o direccionar los esfuerzos en desarrollo, de manera tal de obtener los mejores resultados o limitar los efectos adversos que pudieran producirse.

Una de las tantas herramientas que se vale cualquier organización para manipular toda esa información y que la misma esté a disposición en manera oportuna, es a través de servidores físicos, virtuales, bases de datos, protocolos, enlaces de comunicación, por mencionar algunos. En adición, y cada vez cobrando mayor relevancia, es la computación en la nube (Cloud Computing), la cual, a su vez, permite establecer las bases para la explotación de IOT (Internet of Things – Internet de las cosas).

Es particularmente hacia estos dos últimos elementos donde se dirigen las miradas y voluntades tecnológicas para la explotación de la información. Aunque ya presentes, la proliferación y aplicación plena de tales innovaciones suponen un cambio radical en la forma de vida tal cual es conocida.

Estas nuevas propensiones no parece irrumpir en forma violenta en la cotidianidad para imponer un producto como, por ejemplo, cierto sistema operativo comercial. Sino que, considerando los tiempos que corren, ya a ningún individuo le son extraños los conceptos de reuniones virtuales, trabajo a distancia, análisis de datos masivos, etcétera; el arribo e instauración de estas nuevas herramientas son recibidas gratamente y con mesurada felicidad.

Las Fuerzas Armadas no son ajenas a estas tendencias, ya presentes con las impresoras o fotocopiadoras conectadas a una red local (LAN), hasta en las reuniones virtuales para el planeamiento o ejecución de alguna operación o adiestramiento. Debido a

que, dadas las dimensiones y alcance de sus estructuras y organizaciones, encuentran un bálsamo en estas ayudas informáticas por facilitar su administración y gerencia.

Es ineludible así, desviar la atención de la seguridad de aquellas herramientas que posibilitan, facilitan y se posicionan como referentes al momento del manejo de información y automatización de procesos y operaciones ante tal magnitud de vulnerabilidad. Por esto, es menester atender con celeridad los aspectos que apuntalan la protección de los mismos. Acaso se omita, los efectos pueden ser nefastos, quizás catastróficos, profundizando la gravedad de sus consecuencias si se aplican directamente sobre los esfuerzos operacionales militares.

En forma paralela a las cuantiosas amenazas actuales, se encuentran en desarrollo los procesadores cuánticos, que implican una capacidad exponencialmente superior a los tradicionales. Estos, según el observatorio tecnológico de Hidalgo, México, pueden lograr en una fracción de segundo lo que normalmente insumiría miles de años. Así, se crea una brecha tecnológica verdaderamente abismal entre las posibilidades cuánticas y las defensas informáticas tradicionales.

Desde otro orden de ideas, desde tiempos inmemoriales, la seguridad de la información es una temática sensible. Desde la detección de espías, la caza de palomas mensajeras, pasando por la tan afamada máquina enigma hasta las penetraciones o secuestros informáticos en servidores cruciales, los esfuerzos que se orientan hacia la protección de información son significativos y de vital importancia dadas las consecuencias que implicaría el no poder acceder a tan valiosos datos, o tal vez más grave, que algún adversario o tercero pueda hacerse de ellos y tomar ventaja.

Más aun, como es consabido, la Seguridad de la Información desde la antigüedad ha desempeñado un papel preponderante que surge de la necesidad de transmitir y almacenar la información en forma confidencial para disponer de ella a voluntad y criterio. Los primeros registros que se tienen al respecto datan del año 1500 antes de Cristo, particularmente de una tabla Mesopotámica que contiene una fórmula cifrada para producir vidriado para cerámica. Luego, puede hacerse referencia de cierto escribano hebreo que trabajó en el libro de Jeremías, quien usó un cifrado sencillo invirtiendo el alfabeto conocido como cifrado de sustitución entre los años 500 y 600 antes de Cristo. Pero recién en los albores de la edad media -año 855- en Arabia, surgen los primeros escritos de estudio en la materia. Y no es hasta el 1518, casi setecientos años después, que se publica el primer libro de criptografía “Polygraphia libri sex”, escrito por Trithemius en idioma alemán.

Pero más allá de estas crónicas, el ejemplo más popular de seguridad y vulnerabilidad en la información se halla durante el desarrollo de la segunda guerra mundial, más precisamente con el empleo y decodificación de la mencionada máquina Enigma, mediante la concepción y empleo del computador Bomba (Proyecto Ultra). La primera, fue diseñada por el alemán Arthur Scherbius en 1923 y operaba con una serie de rotores configurables. Mientras que el segundo, fue ideado y fabricado por Alan Touring -gracias a lo aportado por el polaco Biuro Szyfrow- para las FFAA británicas. Es destacable de este ejemplo, la capacidad de codificación de Enigma, pero sobre todo, el esfuerzo y la relevancia de su decodificación, ya que se trata ni más ni menos que de hasta 1.556.215.256.125.916.549.119.449.341 posibilidades según el Museo Histórico Militar de Burgos, España.

A partir de este hito, la lista de aportes al campo de estudio fue creciendo proporcional y progresivamente hasta la actualidad. Pueden mencionarse fórmulas, algoritmos, protocolos, estándares y personalidades de renombre como David Bell, LaPadula, Ellis, Cocks, Williamson, Diffie y Hellman por mencionar algunos. Pero hasta 1982 la computación cuántica no aparece en escena. Y no fue otro más que el reconocido Richard Feynman junto a Yuri Manin, quienes se basan en la mecánica cuántica -desarrollada entre 1900 y 1925- y diseñan el modelo teórico de una "computadora cuántica", dando inicio a un magnánimo esfuerzo por hacerse de tal tecnología a nivel mundial y por una multiplicidad significativa de actores.

A modo de marco conceptual, la mecánica cuántica es la rama de la física que estudia la naturaleza a escalas espaciales pequeñas, los sistemas atómicos, subatómicos, sus interacciones con la radiación electromagnética y otras fuerzas, en términos de cantidades observables. Se basa en la observación de que todas las formas de energía se liberan en unidades discretas o paquetes llamados quantums. Estos, tienen la característica de pertenecer a un grupo específico de bosones, estando cada uno ligado a una interacción fundamental. Sorprendentemente, la teoría cuántica solo permite normalmente cálculos probabilísticos o estadísticos de las características observadas de las partículas elementales, entendidos en términos de funciones de onda.

Las investigaciones antes mencionadas siguen su curso, pero con grandes y esperanzadores resultados, estimándose la finalización y consecuente operatividad de tales procesadores dentro de la siguiente década. Cabe destacar y aclarar que los avances percibidos en esta innovación fueron intempestivos y asunto de los últimos cinco a diez años, impidiendo a los teóricos de la seguridad de la información mantenerse al ritmo de las exigencias. Por tal motivo, las grandes instituciones dedicadas al tema en cuestión se encuentran realizando grandes erogaciones para hallar, primeramente, alguna manera de proteger sus activos, y consecuente-

mente, desarrollar la misma tecnología para emplearla tanto para la disuasión como para su usufructo. En este orden, se encuentran estudios tales como Cyber Security in the Quantum Era de Petros Wallden y Elham Kashefi o Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms por Targhi y Unruh.

Pero más allá de estos ejemplos -entre muchos-, no es posible encontrar en Argentina estudios avanzados respecto a la seguridad frente a la amenaza cuántica. Aunque, irónicamente, se haya llevado a cabo la XVII cumbre de criptografía en la ciudad de Buenos Aires en marzo de 2014, siendo tratada específicamente durante una de sus tantas instancias: la importancia de los procesadores cuánticos (respecto a la seguridad criptográfica). Pueden mencionarse sin embargo, numerosos artículos e investigaciones relacionadas con la mencionada tecnología, como por ejemplo, Computación Cuántica: Un Nuevo Paradigma, de Enrique Cingolani o a Felipe Rojo Amadeo con su trabajo Computación cuántica: análisis y ejecución de algoritmos cuánticos. Pero ahondando en la especificidad, no se encuentran estudios disponibles en relación a la temática propuesta. Sin mencionar o considerar siquiera su eventual influencia en las instituciones gubernamentales, las fuerzas armadas o su impacto en los niveles estratégicos, operacionales o tácticos.

Por lo expuesto, la inminencia de la amenaza cuántica es real y trascendental. Máxime, si no se repara en precauciones y medidas preventivas. Así, el alcance e impacto que significa relegarse ante tal poder es verdaderamente ominoso. De esta manera, se plantea o propone el siguiente cuestionamiento para el abordaje del tema: ¿Que consideraciones básicas pueden aparejarse del advenimiento de los ataques por computadores cuánticos a las herramientas de comando y control, particularmente en la internet de las cosas y la computación en la nube?

A simple vista, la amplitud del campo en el que se pretende indagar impone una estricta circunscripción a los temas específicos propuestos. Por el alcance y restricciones del presente escrito se dejan de lado cuantiosos aspectos intrínseca y sumamente relacionados, como el daño a la seguridad física o de lanza (Spear Phishing), siendo estos quizás los más probables en ocurrencia. En igual forma, por la vastedad que implica, se trata en forma tangente un aspecto fundamental y central, la criptografía. Se obvia este tema porque su solo desarrollo impone un estudio de dimensiones sustanciales y no aportaría mayores luces al presente.

Para iniciar el desarrollo de la temática, en primera medida, se trata el concepto de Cloud Computing (computación en la nube), sus orígenes, presente y futuro. En esta descrip-

ción se menciona su morfología, la forma en que trabaja, y los aportes que la misma hace u ofrece al comando y control.

Seguido, como producto o derivación del anterior, se razona respecto a Internet of Things (internet de las cosas), la que hace posible el comando y control en simultáneo de parámetros, información y cuestiones operativas, valiéndose de la interconexión e integración a la red global. Y en similar forma que el anterior, los aportes que realiza o propone al comando y control.

Finalmente, se explaya específicamente sobre los procesadores cuánticos, se ofrece una reducida explicación respecto a su funcionamiento, su presente, futuro, y las capacidades y previsiones que esta revolución supone. Para tal fin, necesariamente se contrasta con los computadores electrónicos tradicionales para mesurar y referenciar las diferencias entre ambos.

Es necesario destacar que se omite desarrollar el empleo ofensivo que pudiera hacerse con esta tecnología, por más que sea lo primero que llame la atención o a la curiosidad. No por la eventual extensión que implicaría -que en realidad es bastante simple y solo basta con enumerar la totalidad de las posibilidades de ataques o incursiones conocidas-, sino por no estar considerada como opción por la ciberseguridad en la República Argentina en base a la actitud estratégica seleccionada.

En relación con lo mencionado, son gratamente observados los esfuerzos que realiza el Estado Nacional respecto a la ciberseguridad y protección de objetos de valor, y más aún, de las fuerzas armadas. En la actualidad, se desarrollan planes de carreras específicos para todos los cuadros militares, incorporando también el aporte de especialistas altamente calificados del ámbito civil, convirtiéndose en un recurso de investigación y desarrollo de conocimientos más que destacable. Además, se conoce las inversiones financieras -en relación al campo en cuestión- que se han observado en cada una de las fuerzas en los últimos tiempos.

En sumatoria, con los temas expuestos, desarrollados y sopesados, este trabajo de investigación permite incorporar al ámbito castrense un incentivo para elaborar o continuar estudios, proyectos y programas que posibiliten la incorporación, desarrollo y fomento de esfuerzos y medios para estar, siempre y en todo lugar, a la altura de las circunstancias y exigencias.

Aunque el alcance de este escrito esté limitado en su extensión y profundidad, da el puntapié inicial necesario para la concienciación de la imperatividad y trascendencia de la implementación de la tecnología en cuestión, tanto para prevenir sus asedios como para su

explotación. Y en una visión ya a mediano y largo plazo, el cambio de paradigmas bélicos en los niveles estratégico, operacionales y tácticos que supone. Sobre todo, si se considera una integración acabada con demás elementos de la defensa y con la disciplina o ciencia de la inteligencia artificial.

Dada la relevancia del tema, y la mencionada restricción en la amplitud de la investigación para desarrollar los conocimientos que permitan un acercamiento a los conceptos perseguidos, se detalla el objetivo general: Reconocer balances y perspectivas del impacto de ataques perpetrados por computadores cuánticos sobre elementos sensibles del comando y control tales como la computación en la nube e internet de las cosas.

Para tal fin, los objetivos específicos que se disponen para su concreción son, a saber, primero, describir y fundamentar el concepto de Cloud Computing e Internet of Things, sus orígenes, actualidad, empleos, futuro, y la manera en que el comando y control de las FFAA hace uso de los mismos. Y segundo, el reunir y procesar información que permita una iniciación a la tecnología de procesadores cuánticos, nociones básicas de su funcionamiento, actualidad, desafíos y capacidades presentes y futuras.

Habiéndose tratados ambos elementos por separados, resta a las conclusiones el interpolar los factores que del análisis se destaquen y merezcan solicitud. Que, más allá de proponer un cierre a la temática, abre las posibilidades para nuevos desafíos relativos al campo de estudio.

Para el desarrollo de la propuesta, el presente trabajo cumple con las características de correlacional, según lo definido por Roberto Hernández Sampieri en su libro *Metodología de la Investigación;* ya que incluye la relación o grado de asociación que existe entre dos o más conceptos*,* categorías o variables en una muestra o contexto en particular, y las respectivas posibles incidencias y consecuencias de estos.

Focalizando aún más, el estudio pretende determinar la influencia de un concepto o variable, como lo es el desarrollo y empleo de los ordenadores cuánticos, mientras se conoce o domina el funcionamiento de otra u otras variables, en este caso, internet de las cosas y computación en la nube.

Esta metodología arroja un resultado explicativo y parcial, ya que trata y estudia escasos elementos; en contrario, si se contemplaran mayor cantidad de variables, produce un estudio más acabado y completo. De cualquier manera, es lícito destacar que el abarcar todas las variables posibles para su análisis sucede únicamente en casos excepcionales y raramente se alcanzan corolarios plenos. Y, explícitamente con el tema en cuestión, estas variables -más

allá de ser numerosas- son cambiantes en morfología, modus operandi y en magnitud, impidiendo acabados, aplicables y trascendentes deducciones.

CAPÍTULO I

"Herramientas del Comando y Control"

"Caballeros, el oficial que no conoce sus comunicaciones y sus suministros tan bien como su táctica es totalmente inútil"

Gral. George Smith Patton

El presente capítulo describe algunas de las ayudas en las que los decisores y quienes comandan se apoyan para efectuar sus misiones y tareas de la manera más eficiente y segura posible valiéndose de los elementos que proporcionan las tecnologías en la actualidad. Estas ofrecen una amplia gama de aplicaciones que van desde una simple video llamada hasta el control operacional efectivo de procesos y sistemas a distancia.

Para esto, una gran cantidad de opciones se presentan en socorro a las demandas de los niveles superiores de conducción. Algunas de ellas casi en desuso, otras en pleno apogeo y otras por arraigarse. Dentro de las primeras pueden mencionarse los deslucidos faxes (abreviación de facsímil), popularmente conocidos y oportunamente explotados, ya dentro de las segundas, la computación en la nube es un claro ejemplo; y por último, la internet de las cosas, una innovación que parece despegar hacia un futuro promisorio.

De esta manera, el presente apartado reseña estas dos últimas herramientas, en las que se apoyan abundantes aplicaciones, procesos y elementos para ofrecer al usuario la solución esperada. Es menester aclarar que estas son la base y concepto sobre la cual actúan otros sistemas y subsistemas, y no la interfaz al usuario en sí. Como por ejemplo, cualquier plataforma de correo electrónico en línea, donde el usuario accede a documentos ajenos a su ordenador y lo puede hacer desde distintas terminales.

Computación en la nube

Cloud Computing se presenta como una nueva revolución informática. Seguramente sea un tanto subrepticia como la Web o internet misma, pero avizora cambios sustanciales a nivel social, tecnológico y económico.

Una de las producciones personales que resalta del resto por su claridad y relativa especificidad es la de "Computación en la Nube e innovaciones tecnológicas - El nuevo

paradigma de la Sociedad del Conocimiento" por Luis Joyanes Aguilar. En este se detalla simple y entendible las nociones básicas para comprender este fenómeno.

Este documento describe a la Informática en la Nube (Cloud Computing) como el procesamiento de datos realizados por una serie infinita -no por su cantidad actual, sino por su potencial de integración- de servidores desplegados en centros de información en todo el mundo; en los que se administran aplicaciones, programas, procesos, protocolos, algoritmos e información de tan diversa índole para estar a disposición de cuantiosas organizaciones y empresas para su explotación. Esta red masiva integra servidores, procesadores, conexiones de distintos tipos y niveles, almacenamiento de datos, interfaces y más. Quizás llame a la memoria los nombres de Gmail, Facebook, Google Classroom, entre tantos para su ejemplificación.

Por su morfología y ventajas, la mayoría de las instituciones, organizaciones y empresas encuentran en tal tecnología la solución a la mayoría de sus problemas, principalmente de carácter económico, y luego por las infraestructuras o arquitectura informática, incluyendo la necesaria seguridad de las mismas. Así, las empresas más importantes a nivel global ya están volcadas a tal ingenio, hasta algunas de ellas ofrecen este tipo de servicio, como Amazon, Google, Yahoo, IBM, Microsoft, etcétera. Y aún más, sendas aplicaciones y programas basan su misma operación en ella, como las aplicaciones de mapas (Google, Bing, Garmin, Herewego), redes sociales (Facebook, LinkedIn, Twitch), las reuniones en línea (Zoom, Meet, Skype), los servidores de datos (Mediafire, Megaupload, Rapidshare); y aun más evidente para el usuario general, las aplicaciones de procesamiento de textos, cálculos y presentaciones en línea (Documentos de Google, Microsoft, Prezi) donde claramente se percibe que lo único que procesa el individuo -y su computador- es la interfaz, mientras que el proceso general de la operación y el cálculo masivo de datos, se hace en línea por una red de computadores situado, quizás, en Arizona, EEUU, o en Rosario, Provincia de Santa Fe.

Aunque no hay armonía o consenso global respecto a su definición, sí existen organismos que regulan las Tecnologías de la Información y, en particular, de Cloud Computing. El más conocido y de renombre es el National Institute of Standards and Technology (NIST) y su Information Technology Laboratory, y entiende a la computación en la nube como:

> Un conjunto de hardware y software, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. Los servicios de la nube incluyen el software, infraestructura y almacenamiento en Internet, bien

> como componentes independientes o como una plataforma completa basada en la demanda del usuario. El mundo de la nube tiene un gran número de actores o participantes. Los grupos de intereses del mundo de la computación en nube son: los vendedores o proveedores: que proporcionan las aplicaciones y facilitan las tecnologías, infraestructura, plataformas y la información correspondiente; los socios de los proveedores: que crean servicios para la nube ofreciendo y soportando servicios a los clientes; los líderes de negocios: que evalúan los servicios de la nube con el objetivo de contratarlos e implantarlos en sus organizaciones y empresas; los usuarios finales que utilizan los servicios de la nube bien de modo gratuito o con una tarifa de pago. El modelo de la nube, según NIST, se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. (Uso Seguro y Efectivo de la Computación en la Nube, Mell, P. y Grance, T.)

Los servicios ofrecidos por las grandes empresas proveedoras son compartidos entre los distintos entes y empresas contratistas, es decir, que la arquitectura, software, hardware, base de datos, etcétera, son utilizadas por todas ellas; sólo que en base al género y tipo de servicio sus credenciales y privilegios son acotados y direccionados para acceder únicamente a lo competente. De esta manera la administración de redes en todo su concepto (instalación, seguridad, mantenimiento, actualización y protección) pasa a quedar en manos de un tercero encargado de asegurar el servicio solicitado, simplificando enormemente la gestión de la información incluyendo, espacio, tiempo, energía y costos.

Además, la versatilidad que este sistema ofrece respecto a las terminales de conexión de los usuarios, permite la disponibilidad de los servicios desde casi cualquier interfaz en la mayor parte del planeta. Esto quiere decir que el CEO de Ford Argentina puede acceder al balance financiero o el estado de producción de cualquiera de sus modelos manufacturados desde su móvil, mientras toma un café en la sala de esperas del centro de conferencias de Ford en EEUU, o hasta en plena disertación, enlazando y proyectando tales datos. O quizás, a nivel castrense, llevar a cabo una videoconferencia para la coordinación de esfuerzos, propios a un ejercicio conjunto.

Los servicios mas comunes ofrecidos por las mencionadas empresas proveedoras son: PaaS (Platform as a Service), plataforma como servicio, IaaS (Infraestructure as a Service), infraestructura como servicio, y SaaS (Software as a Service), software como servicio. Y estos se estructuran a través de nubes privadas, públicas e híbridas.

Cuando se refiere a SaaS se hace mención al software instalado en la nube -en su gran mayoría-. Es la continuación de lo que otrora se conocía como Software on Demand (software a demanda). Estos programas o aplicaciones son accedidas a través de distintos dispositivos mediante una interfaz de usuario liviana, como una aplicación de smartphone o un navegador web. Permite que el cliente no recaiga en la preocupación de la seguridad, el lenguaje, administración de redes, ni siquiera del sistema operativo. Como ejemplo de esto puede mencionarse a las plataformas de correos electrónicos, de streaming y documentos en línea.

En lo que respecta a la plataforma como servicio (Paas), las empresas proveedoras ofrecen un marco o entorno a aquellos interesados en el desarrollo de software y aplicaciones. Estos últimos se valen de las herramientas puestas a disposición, para realizar el ingenio solicitado por parte de terceros en base a sus requerimientos particulares. Estos Toolkits (figurativo de caja de herramientas) suelen estar conformadas por lenguajes de programación e interfaces, estándares y protocolos, canales y conectividades. Este modelo permite a empresas intermediarias cumplir con la especificidad de las necesidades de sus clientes sin incurrir en gastos exorbitantes para el emplazado de redes, servidores y desarrollo de software. Cualquier entidad bancaria con servicios en linea seguramente haga uso de esta tipología.

IaaS (Infraestructura como servicio) es básicamente la puesta a disposición de los elementos físicos de la arquitectura informática. Generalmente está asociado al uso de almacenamiento de datos, procesamientos, servidores y conexiones. Este modelo es observado con el almacenamiento de información en línea (Google Fotos, Icloud, Onedrive, etcétera).

Son evidentes las prestaciones y ventajas que esta tecnología ofrece. Específicamente en el ámbito militar, pueden y son empleados en la representación de la situación táctica en distintos dispositivos en terminales distantes, y así, seguir el desarrollo de una operación en simultáneo por los niveles tácticos, operacionales, militar y nacional. Como también, la gestión de un sistema logístico integrado a nivel conjunto, que permite centralizar toda los requerimientos, situación actual y previsiones futuras en relación a los elementos ya provistos. Por mencionar algunas.

Pero, por otro lado, al centralizarse todos estos procesos e información en canales acotados y de acceso público, la seguridad de todos estos elementos es clave. El simple hecho de un corte de energía en la terminal de servidores en la India, puede limitar el acceso a información crítica o demorar en gran medida el arribo de la misma. Máxime si se considera

el manejo de información sensible o secreta, y que la misma no esté disponible al momento de algún proceso de toma de decisiones de relevancia.

Por esto, se dispone de un sistema de seguridad multicapa, que se basa en garantizar la protección en todas las capas en las que opera todo el proceso informático, desde la interfaz del usuario hasta los firewalls en los servidores y almacenamiento de datos. Para esto se utilizan distintos protocolos que van desde la autenticación hasta el control de flujo de información mediante cifrados, túneles, redes virtuales privadas, etcétera. Aún así, las vulnerabilidades en la información existen y son palpables en la actualidad y con procesadores convencionales.

Internet de las cosas

Internet de las Cosas fue nombrado en primera instancia por Kevin Ashton en 1999 cuando se encontraba trabajando en redes de identificación por radiofrecuencia (RFID) y en tecnologías de detección emergentes. Y aunque el término fuera propuesto en los fines del milenio pasado, la IOT recién parece realizarse entre 2008 y 2009.

Jordi Salazar y Santiago Silvestre explican que la IOT se refiere a la interconexión en red de todos los objetos cotidianos que están equipados con algún tipo de inteligencia o dispuestos para tal fin. En este contexto, Internet puede ser también una plataforma para dispositivos que se comunican electrónicamente y comparten información y datos específicos con el mundo que les rodea.

Evidencia así, la transformación a la que los tiempos, las sociedades y las tecnologías empujan a la internet, forzando interconexiones más numerosas, de mayor volumen y caudal respecto a la administración de información y operacionalización de terminales. Este avance permite contar con información más fidedigna y una mejor integración de servicios autónomos e inteligentes, facilita el intercambio de bienes y servicios entre redes de las cadenas de suministro por parte de los proveedores.

La IOT es otra de las ventajas que es facultada o que deriva de la computación en la nube, ya que se vale de la integración de terminales, redes, conexiones, y centrales de procesamiento para alcanzar su máximo potencial. Y al igual que esta, se basa en los protocolos de transferencia de hipertexto (HTTP) y los protocolos para transferencia simple de correo (SMTP) tradicionales, pero su fuerte radica en la comunicación máquina a máquina (M2M). Como dato, en 2010, el número de objetos físicos cotidianos y dispositivos conectados a Internet fue de alrededor de 12,5 mil millones. En la actualidad hay cerca de 50

mil millones de dispositivos conectados a la IOT. Más de cinco dispositivos inteligentes por persona.

La IOT está generalmente conformada por cuatro capas:

- Detección.
- Intercambio de datos.
- Integración de la información.
- Servicios de las aplicaciones.

Es evidente la imperativa integración al sistema que nuclea y relaciona estas capas, otorgándole el fundamento operacional y lógico, mucho más allá de la simple conexión a la red. De esta manera, estas cuatro capas en plena interacción y fundamentadas en un procesamiento inteligente, conforman el concepto de internet de las cosas.

El valor agregado que esta innovación pretende, es la eficiencia en los procesos de toma de decisiones y operacionales, debido a que mejora la reunión de información, su procesamiento y el direccionamiento de los esfuerzos. Permitiendo la orientación de los recursos ahorrados hacia otros requerimientos o nuevos emprendimientos o desafíos.

Los servicios que ofrece a través de aplicaciones o programas está limitado a la inventiva y la ética humana. Puede emplearse y adaptarse a la gran mayoría de los campos en los que se proyecta y desenvuelven las personas. Como ejemplos de esto pueden mencionarse:

- Edificios inteligentes: Refuerza la seguridad, permite mayor ficiencia en la administración energética, la logística, salud y educación, asistencia variada, y el control de mascotas.
- Ciudades inteligentes: Además de lo mencionado en el ítem anterior, la administración y gestión del transporte, tránsito, recolección de residuos, limpieza, obras de infraestructura, y estadísticas.
- Educación: Integración de aulas virtuales y presenciales, procesos de evaluación más eficientes con resultados en tiempo real, bibliotecas virtuales interrelacionadas, seguimiento personalizado y permanente en los procesos de aprendizaje, asistencias y estadísticas.
- Electrónica: Gerencia y monitoreo de los electrodomésticos y demás dispositivos a distancia e integrados.
- Salud: Atención y seguimiento personalizado en tiempo real de pacientes, enfermedades crónicas, diagnóstico a distancia, pulseras o dispositivos sensores con reporte y llamados de emergencia remotos, alimentación y estadísticas.

- Transporte: Ubicación y estado de los servicios públicos, autos inteligentes, control de tránsito, administración de semáforos y accesos a arterias urbanas, administración de mejor ruta personalizada, recomendación o limitación de velocidad, eficiencia logística y estadísticas.
- Recursos energéticos: Eficiencia en la producción y almacenamiento, previsiones, y estadísticas.

Esta tecnología revoluciona el entorno a la que es introducida, desde el hogar de las personas hasta las grandes industrias y entes estatales. Otorga a sus usuarios el acceso a una cantidad creciente e integrada de datos, que pueden incluir aspectos de seguridad, salud o la simple ubicación de algún transporte público en particular. Este radicalismo se ve potenciado por la digitalización y puesta en red de sensores junto a la "inteligencia" de dispositivos y la integración por medio de redes cada vez más veloces. Esta sistematización repercute sustancialmente especialmente en las grandes industrias que pueden administrar y regular una gran producción a través de un dispositivo que modula los esfuerzos como consecuencia a las distintas entradas de información con el que es suministrado (materia prima, energía necesaria, temperatura ambiente y de cada máquina, cantidad de obreros en planta, valor del dólar, etcétera).

En el ámbito militar ofrece, a simple vista, una herramienta invaluable para la administración de recursos para la defensa. Desde la asignación de un TAI (Tránsito Aéreo Irregular) -por su velocidad, posición, altura, rumbo- a cierta sección de Caza Interceptora en relación a las características, performances y ubicación de esta, hasta el despacho de elementos críticos por haber alcanzado el nivel mínimo de abastecimiento en cualquier estación o destacamento remoto. Pero quizás sea mas evidente en el control y seguridad de las unidades, en las que para el ingreso o acceso a determinadas áreas, se cuente con dispositivos de reconocimiento facial, tarjetas de identificación, horarios particulares, todo supervisado en tiempo real en continua interacción con la base de datos y con la respuesta inmediata o retén.

Este flujo de intercambio e integración de datos implica un gerenciamiento seguro de información con un alto grado de protección en tiempo real. Que va desde criminalística, pasan por la salud para finalizar en la vida privada de los individuos. Razón por la cual, grandes esfuerzos y recursos son ejercidos para asegurar los mismos, y grandes controversias surgen como consecuencia.

Por ser una parte de la Computación en la Nube, la Internet de las Cosas también se vale de las mismas medidas y consideraciones de ciberseguridad, pero configurándose como

uno de sus aspectos más sensibles y propensos a ser vulnerados por el tipo de información que integra, y porque la mayoría de los dispositivos son administrados por usuarios con niveles de conocimientos básicos o nulos respecto a la seguridad de la información.

A lo largo del capítulo se mencionaron algunas de las innovaciones ya presentes y de gran repercusión en la cotidianidad, las herramientas actuales y futuras. Son claros los horizontes tecnológicos que se avecinan y el estar a la altura de las circunstancias, según la situación lo amerite, representa una obligación ineludible para la seguridad del Comando y Control. Que en el estado del arte actual, ya es propenso a vulnerabilidades varias -al igual que cualquier otro ente-, y se hacen exponenciales con el advenimiento de los computadores cuánticos.

Puede ejemplificarse el impacto que representaría el envío masivo de ciertos elementos críticos, como vituallas o armamento, a un extremo del tan extenso territorio, diametralmente opuesto al real, por un ataque cibernético con tal objetivo. O también, el despliegue de aviones interceptores hacia un eco radar ficticio o falso, mientras ingresan sustancias ilícitas a granel por otro eje de avance distinto y/o se encubre la ubicación real de los incursores. Las consecuencias en crisis o contexto bélico, pueden ser nefastas y determinantes.

CAPÍTULO II

"Procesadores Cuánticos"

"Si piensas que la tecnología puede solucionar los problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

Bruce Schneier

El presente capítulo versa plenamente respecto al eje de la temática. La inminencia de los computadores no tradicionales y sus augurios deberían tener carácter prioritario en las agendas, previsiones y medidas en el campo de la ciberseguridad. Porque más allá de las ventajas que estas nuevas tecnologías ofrecen, la actitud estratégica nacional y su decantamiento a nivel operacional y táctico, determina la posición defensiva con las que las mismas son aproximadas.

La radicalidad del cambio que conlleva el desarrollo de estas innovaciones deberán encontrar contrapartidas de seguridad acordes ya instaladas e instauradas, para que al momento de ser impuestas en el entorno ciberespacial, no avasalle con las estructuras, arquitecturas y sistemas sensibles de los distintos y tan variados protagonistas y participantes. Por es-

to, no puede y no debe hacerse caso omiso, o restarle importancia a cuanto esfuerzo pudiera abocarse a tal tarea. La indolencia o posposición por considerarlo temporalmente lejano o por la dificultad de la cuestión pueden acarrear resultados terminantes.

Funcionamiento y capacidades

Ignacio Kleinman Ruiz en su trabajo "Computación cuántica: Aplicaciones prácticas que la computación clásica no puede solucionar" acertadamente resume los aspectos básicos para cimentar una noción respecto a la computación cuántica y sus capacidades. Que, articulado con "Preparando la confiada internet para la era de la computación cuántica – La amenaza a la seguridad de la información puede ser más inminente de lo que crees" de Deborah Golden, Colin Soutar, Itan Barmes, Scott Buchholz, y Caroline Brown para Deloitte Insights, permite arribar a un concepto único y abarcativo respecto a esta tecnología y la seguridad que implica.

Cabe destacar, antes de proseguir con el correspondiente desarrollo, que las investigaciones respecto a esta tecnología se están produciendo por entes privados, estatales e híbridos. Y que la variedad de versiones, modelos y experimentaciones agregan a este diverso entorno ciertas características peculiares que impiden la comparación entre los distintos ejemplares. Pero más allá de lo expuesto, comparten un gran fundamento y sobre el cuál se desarrollan las distintas configuraciones mencionadas. No se realiza una explicación exhaustiva de la mecánica sobre la cual versa esta novedad por no aportar mayores luces a la temática en cuestión y a los objetivos perseguidos.

Ya respecto a la base común referida, su concepto y fundamentos, determina que los procesadores cuánticos se configuran como un paradigma verdaderamente diferente a los electrónicos. En primera medida porque se fundamentan en el uso de Qubits, término que deriva de quantum bit, en vez de los populares Bits; que posibilitan nuevos algoritmos y consecuentemente favorecen otras prestaciones.

En los procesadores actuales el bit asume valores de 0 o 1 únicamente, y lo hace mediante la entrega o no de impulsos eléctricos. Por el otro lado, en los cuánticos, el qubit puede representar, 0 y 1 por separado y/o 0 y 1 en simultáneo por el fenómeno llamado superposición coherente -propio de la ley de mecánica cuántica-, lo que arroja 4 resultados en vez de 2 (00, 01, 10 y 11); en otras palabras, las capacidades del computador cuántico son exponenciales respecto al digital y, además, lo hace en forma isócrona (00, 01, 10, 11 y 00, 01, 10, 11). A modo de ejemplo comparativo, un procesador cuántico de sólo 30 qubits equivaldría a un

procesador convencional de 10 teraflops, estos son millones de millones de operaciones por segundo, cuando en la actualidad una computadora personal estándar alcanza los 5.

Por las características de la mecánica fundamental de esta tecnología, ejemplificadas por Erwin Schrödinger y su hipotético gato[1], la problemática radica en la oportunidad en que los valores son medidos para poder extraer sus resultados. Ya que, según esta teoría, un 0 puede ser un 1 al mismo tiempo y sus estados no son conocidos hasta ser censados. Ante tal desafío, Peter Shor en el año 1994 desarrolló un algoritmo que permitió, por medio de la probabilidad -única forma para poder discriminar entre los estados posibles-, determinar el estado de las partículas cuánticas arrojando mediciones de estas, que luego, son sujetas a cierta corrección de errores para obtener el valor perseguido. Luego, en el año 1996, Lov K. Grover postula su algoritmo que simplifica la extracción de estos valores.

Para explicar la razonable paradoja que significa la proliferación un sistema de procesamiento de información muchísimo más complejo, obtener resultados concretos, y que este sea rotundamente superior en prestaciones en comparación con la simpleza del computador electrónico, aparece el entrelazamiento de qubits. Esto significa que funcionan como un conjunto en el que la excitación o los efectos sobre unos, repercuten sobre los otros, lográndose extraer los resultados esperados en un tiempo exponencialmente menor por la sinergia y cooperación entre ellos.

Para lograr que los qubits se comporten según la voluntad de su operador, pueden ser manipulados aplicando varias técnicas y durante varias etapas. Particularmente aquí, es donde aparece la ramificación de los distintos modelos, oportunamente mencionados, que esta tecnología revista. Empero, todos ellos deben cumplir ciertas normas básicas y comunes: primero que los qubits deben estar totalmente estables y controlados para su medición; luego, que estén dispuestos a realizar los algoritmos ingresados; y por último, que sus resultados sean proclives a ser corregidos.

Entre los sistemas que comparten el fundamento pero que operan en forma disimilar pueden mencionarse, principalmente: la trampa de iones, circuitos superconductores, vacantes de diamantes, NRM (resonancia magnético-nuclear) y los sistemas ópticos (fotónicos). Aunque cada modelo presenta sus ventajas y desventajas, los ópticos, ofrecen ciertas características que lo distinguen del resto, ya que pueden ser manipulados a muy altas velocidades; y que, a su vez, el proyecto a futuro y las posibilidades de desarrollo son más esperanzadoras

1 Hace referencia a un felino dentro de una caja, que puede estar vivo y muerto al mismo tiempo, demostrando un estado conocido como superposición cuántica, y que para determinar su estado resta comprobarlo.

con innumerables aplicaciones y utilidades que pueden ir desde la concepción de redes hasta tecnologías multidimensionales.

Futuro

Los avances que se registran hasta el día de la fecha, tal cual fue referido, son efecto de la interacción de aportes de diversa índole como estados, empresas, tecnologías y ciencias. La sinergia del aporte financiero, la inteligencia artificial, el desarrollo de nuevos algoritmos, nuevo y más potente hardware, y estructuras informáticas, hacen que en los últimos tiempos se prospere en forma vertiginosa y los horizontes se hagan cada vez más próximos y promisorios.

Existe en la actualidad una verdadera competencia para alcanzar la supremacía cuántica en cuanto actor involucrado se considere. Este frenesí se basa en el radicalismo y disrupción que esta tecnología promete. De todos estos se destaca, nuevamente, IBM por ser la pionera en querer comercializarla (QaaS: Quantum as a Service), aunque irónicamente lo ofrece de manera gratuita a través de la nube y no como herramienta en sí, sino como una plataforma para familiarizarse.

Esta mencionada drasticidad pronostica una verdadera revolución tal cual fue referido. Todas las previsiones apuntan al rotundo cambio de paradigmas, sistemas y hasta el mismo modo de vida de la sociedad. Solo basta con imaginar los resultados que podrían surgir por la simple combinación entre esta tecnología y la inteligencia artificial, desde la representación de la mejor combinación de transportes -en tiempo real- para ir al trabajo hasta encontrar la cura a enfermedades mortales o insanables. Pero, por sobre todo, se espera que den respuesta a problemas matemáticos hasta ahora sin solución, o comprobación, como el de Goldbach[2] o Collatz[3].

Por la capacidad de procesamiento que ofrece esta tecnología, todos los sistemas físicos y químicos con gran número de elementos que se interconectan e interactúan de formas distintas para luego modelar comportamientos o resultados para cada una de esas relaciones propias y únicas, pueden ser simulados casi en su totalidad; además de hacerlo en cuestión de segundos, con una inversión económica significativamente inferior al método tradicional y sin la necesidad de experimentaciones o comprobaciones de campo. Quizás se logre algún

2 Todo número par mayor que dos puede escribirse como la suma de dos números primos.

3 Cualquier número entero positivo, si es par puede dividirse entre 2; si es impar, es multiplicado por 3 y luego se le suma 1, sucesivamente. La repetición del proceso con los resultados obtenidos, inevitablemente se llega a 1.

compuesto químico que mitigue el cambio climático, o el descubrimiento de energía limpia e inagotable. Las posibilidades son verdaderamente colosales.

Pero no todo son ventajas, más aun si se considera que esta novedad será introducida en un sistema o entorno bien cimentado y establecido, con numerosos años de historia que lo formaron, lo condicionaron y afianzaron. Este ambiente es caracterizado por la interacción y convivencia equilibrada de seguridades y amenazas, donde una acción es correspondida con una reacción en forma casi inmediata. Que por ser de dominio popular, la mayoría de los individuos tiene algún conocimiento o pericia al respecto que les permite desenvolverse sin grandes riesgos, o en todo caso, ocasionales.

A nivel mundial, los protagonistas del desarrollo de esta innovación estiman la propagación de estas capacidades para antes del año 2030. Por esto, el establecimiento de un ambiente seguro es una prioridad y una urgencia. Siendo una de las áreas o elementos de mayor vulnerabilidad y preocupación para los estudiosos del tema, es la criptografía. Esta se utiliza para proteger cualquier información, como ser: comunicaciones, discos completos, particiones, carpetas y archivos, incluyendo la información que se transmite de un sistema de cómputo a otro. Entre las disciplinas que la fundamentan se destacan la matemática discreta, la teoría de los grandes números y la complejidad algorítmica.

Por otro lado, para realizar la vulneración a estos sistemas, se utilizan primariamente algoritmos que por estadística y probabilidad dan con el código de cifrado; también puede mencionarse el método de fuerza bruta, pero por la demora que implica el análisis de número a número es únicamente empleada en casos puntuales. Pero si se considera el empleo de computadores cuánticos, aun mediante la fuerza bruta el cifrado se rompe en cuestión de segundos.

Proactivamente, el NIST (National Institute of Standards and Technology), como todos los entes y organismos de tecnología significativos, se encuentra en la búsqueda, estudio, análisis y evaluación de algoritmos de clave pública que puedan resistir un ataque por procesador cuánticos. En la actualidad, sólo resaltan dos conceptos o metodologías, la criptografía cuántica y la postcuántica. Mientras que la segunda se basa en el uso de problemas tan difíciles de procesar que no puedan ser descifrados ni por estos procesadores, la primera reposa en algoritmos y protocolos propios y derivados de esta tecnología. Lo que naturalmente revela un dilema, el de elucubrar protocolos y algoritmos cuánticos orientados a la seguridad sin contar aún o dominar cabalmente esta ciencia.

Además, por tratarse de una tecnología en desarrollo, no existe actualmente regulación alguna, legislación o tratado que limite o controle los efectos y alcances de esta. Agra-

vándose la situación por tratarse de entes públicos, privados y mixtos, y de nacionalidades varias. Por esto, se optó por protocolo, el desconectar la propia terminal de la red de datos en forma automática ante cualquier comunicación o enlace con algún ordenador de estas características (killswitch).

Por todo lo expresado en el apartado, por un lado los computadores cuánticos son motivo de alegría y de dicha por las venturas y posibilidades que pueden ofrecer, un verdadero cambio a la forma de vida. Pero, por otro lado, la gravedad que representa la conexión de un solo ordenador cuántico a la red mundial es un tema de suma prioridad y preocupación. El acceso a datos sensibles, comunicaciones, procesos, sensores y terminales operativas, entre otros factores, pueden vulnerados en cuestión de segundos y sus consecuencias, quizás, nefastas.

CONCLUSIÓN

"La ciencia de hoy es la tecnología del mañana"

Edward Teller

El presente trabajo se fundamenta principalmente en una recopilación bibliográfica y documental respecto a las herramientas del Comando y Control en las que se vale la conducción para contribuir mediante su tarea a la misión de la Defensa Nacional, en su estado actual y tendencias; y la relaciona y contrasta con el advenimiento de los ordenadores cuánticos y las vulnerabilidades que ellos suponen. Que más allá del ventajoso potencial de tal tecnología, la disparidad entre las capacidades de procesamiento hacen imperativas las previsiones de seguridad.

Para tal objetivo, se han detallado dos conceptos en boga y de suma trascendencia, la Computación en la Nube y la Internet de las Cosas. Ambas utilidades son actualmente explotadas tal como fue referido, pero más aún, su tendencia es a proliferar en gran forma. Estos conceptos se encuentran en pleno desarrollo, y las aplicaciones y beneficios que prometen suponen un cambio sustancial en la vida de las personas.

Primeramente, se trata Cloud Computing, mencionándose la arquitectura sobre la que se sostiene, la manera en que está integrada y su modo de funcionamiento. Además, se refiere también a las aplicaciones y ofertas que esta modalidad entrega a la vida cotidiana y especialmente al Comando y Control actualmente. Y más aun, se establece una prospección a futuro de las capacidades y promesas que esta tecnología pretende alcanzar.

En segundo lugar, se expone respecto a Internet of Things, y particularmente en relación a la manera en que se basa, interrelaciona e integra con la Computación en la Nube. Se describe la forma de su diseño, de empleo y las prestaciones que hoy en día ofrece al Comando y Control y a la sociedad. También se hace mención al estado del arte que esta herramienta avizora y los cambios que ambiciona.

Luego, se describe el estado al presente de la computación cuántica, una somera explicación en relación a su funcionamiento, donde se tratan los Qubits, la superposición y entrelazamiento cuántico, y la manera en que de ellos se obtiene la información. Se menciona los modos en los que esta novedad avanza y toma diferentes enfoques. Se explaya respecto a su actualidad y futuro -junto a las capacidades previstas-. Se hace referencia también al cambio de paradigmas que transitan los algoritmos y protocolos entre la computación cuántica y la clásica.

Esta tecnología, a su vez, lanza una batería de cuestionamientos y estudios que revolucionan las estructuras tradicionales en las que tan conforme descansa la sociedad toda. Donde los mencionados algoritmos y protocolos tal cual son conocidos son vilipendiados para elaborar nuevos, que se orienten hacia los nuevos desafíos y proyecciones, dando espacio también a lenguajes exclusivos de la novedad cuántica.

Se mantiene a lo largo de todo el trabajo, un continuo parangón entre esta tecnología y los procesadores tradicionales para una mejor referencia del lector. Esta necesaria confrontación hace posible dimensionar y asimilar dos conceptos y tecnologías, que aunque análogas en sus objetivos o fines, su morfología, operación y prestaciones son verdadera y sustancialmente desiguales. Además, predispone al necesario cambio de estructuras mentales en acompañamiento o sintonía a los tecnológicos.

Hasta aquí, se cumplen los objetivos parciales y general. Se describieron las herramientas en las que se vale el Comando y Control y la amenaza cuántica. Se explayó respecto a la disparidad de capacidades y la problemática que supone la incorporación de uno de estos ordenadores a la red global, y consecuentemente, las alarmas y preocupación que suscita en aquellos responsables de la seguridad de la información. Que en la actualidad no existe algoritmo o protocolo que resista el embate cuántico, y que el único modo de protección es el “killswitch”, es decir, la desconexión de la red de aquel ordenador que enlaza comunicación con alguno de estos procesadores. Así, llama la atención la simpleza con la que se logra inutilizar algún sistema por un tiempo determinado, sólo alcanza con establecer una conexión mediante un ordenador cuántico, y por protección, se desconectará.

Empero, no se detallan consideraciones que sean aplicables en la actualidad y que revisten trascendencia. En primera medida por no existir fehacientemente medidas de seguridad que se contrapongan a la vulnerabilidad ante tales ordenadores, y en segundo orden, porque las previsiones iniciales que parecen alzarse como referencia a la problemática, implican el desarrollo y dominio de esta tecnología.

En referencia a esto, y como de cierre del epílogo, se reconocen algunas recomendaciones reunidas en torno a la cuestión, y que -como fuera oportunamente mencionado- sienta las bases y representa la primer voluntad y esfuerzo en respuesta proactiva a las amenazas venideras. Que por la perspectivas que ostentan los computadores cuánticos, la impasividad ante tal situación no es otra cosa que la rendición de los sistemas que permiten el Comando y Control de las Fuerzas Armadas, y la gravedad de tal supuesto excede las palabras que puedan procurarse.

En primer lugar se refiere a generar y propagar la conciencia respecto a la gravedad de los riesgos a la seguridad que significa el advenimiento de procesadores cuánticos -fundamento de este trabajo-. Transmitir esta conciencia a todos aquellos que de alguna manera se relacionan con la temática, de cualquier ámbito o campo. Esto permitirá, a su vez, la predisposición para atender razones y direccionar esfuerzos de todo tipo para no relegarse en esta materia, desde la asignación económica hasta la priorización de los organismos de investigación y desarrollo del Estado Nacional o terceros. Es imprescindible, también, la actitud de vigilancia, ya que organismos encargados de la seguridad pueden lograr avances en el campo, y que por parsimonia se desconozcan.

Como derivación de lo anterior, es menester conocer, difundir y aplicar las recomendaciones que los organismos y entes entendidos promulgan al respecto. Es de dominio popular el hecho que la principal amenaza contra la seguridad de la información es el mismo operador, que por negligencia o desconocimiento, utiliza de forma incorrecta, se desentiende de procedimientos o relativiza la seguridad.

Como segunda medida podría mencionarse el romper con los paradigmas de la computación clásica. Sólo de esta manera se podrán contrarrestar o mitigar los efectos negativos que los ordenadores cuánticos significan para la privacidad y seguridad. Es necesario realizar una aproximación a la temática sin sesgos ni estructuras. Por el contrario, se considera imprescindible elaborar la arquitectura necesaria teniendo como base la mecánica o ciencia de la cuál esta tecnología emana, y no tratar de adaptar lo conocido y dominado. Quizás sea contemplable el desarrollo de protocolos y algoritmos no rígidos, que muten y fluyan según cier-

to patrón -o de forma aleatoria- y se vayan adaptando y evolucionando mediante credenciales, formatos de autenticación y modalidad de conexión.

Otras de las posibilidades es la de desarrollar en forma periódica sistemas y procesos de encriptación propios y distintos a los generalizados. Estos podrían ser elaborados y difundidos en forma regular y en un período de tiempo razonable de manera tal que cualquier intento de intrusión, primeramente, le implique descifrar el tipo de código o proceso de autenticación, para luego, afanarse en obtener la clave para su acceso. Esta es una tarea propia de Sísifo, pero al momento de reconocer una amenaza potencial, puede activarse un protocolo de emergencia que automáticamente cambia a un proceso de encriptado e identificación diferente, dificultando aún más la incursión.

En cuarto lugar, establecer protocolos o procedimientos de seguridad para cada componente que integra el sistema a proteger y que sean resistentes al primer encuentro con un ordenador de estas características. Y, sobre todo, mantenerlos actualizados, recomendación que nunca puede desestimarse. Que, aunque muchos componentes poseen medidas de seguridad, no son todos y no tienen internalizado el procedimiento de killswitch, por ejemplo, la UEFI (interfaz unificada de firmware extensible)[4].

En quinto orden, puede utilizarse el análisis de la interacción de la comunicación o conexión entrante; de esta manera, poder discriminar el ancho de banda, latencia, el hardware de enlace, sistema operativo, programas o aplicaciones, protocolos, llaves criptográficas, y por sobre todo, el tiempo. Como se ha descripto, la velocidad de los ordenadores cuánticos sobrepasan en gran medida a los tradicionales, por ende, la respuesta a las interrogaciones será inmediata -aun simulando configuraciones ficticias-, mientras que en los clásicos tal proceso demoraría en comparación.

Este humilde trabajo espera considerarse como el punto de partida de una gran cantidad de trabajos subsidiarios, derivados, concurrentes e idealmente concluyentes. Las posibilidades y los campos que se abren respecto a la protección de los elementos o herramientas en las que se basa el Comando y Control son inmensos. Como ejemplo de esto puede mencionarse la seguridad de la representación visual de los elementos desplegados tanto en la superficie como por debajo y encima de ella, el sistema integrado de situaciones logísticas a nivel conjunto, o de las bases de datos. Pero aún más sensible, la protección todos los medios de comunicación, la eventual automatización de procesos, la criptografía en general, y de objetivos de valor estratégico.

4 Incluye bases de datos con información de la plataforma, inicio y tiempo de ejecución de los servicios disponibles listos para cargar el sistema operativo.

Bibliografía

Allende López M. (2019), *Tecnologías Cuánticas: una Oportunidad Transversal e Interdisciplinar para la Transformación Digital y el Impacto Social*. Banco Interamericano de Desarrollo. Recuperado de: https://publications.iadb.org /publications/spanish/document/Tecnolog%C3%Adas_cu%C3%A1nticas_Una_ oportunidad_transversal_e_interdisciplinar_para_la_transformaci%C3%B3n_digital _y_el_impacto_social.pdf

Brumfiel G. (2019*), Is the Future Quantum?* Entrevista en audio. Recuperado de: https://www.npr.org/2021/03/25/981315128/is-the-future-quantum

Cingolani E. (2015), *Computación Cuántica: Un Nuevo Paradigma*. Universidad Abierta Interamericana, Buenos Aires, Argentina. Recuperado de: https://fisica2-uai. wikispaces.com/file/view/Computacion+Cuantica+Nuevo+Paradigma.pdf

Evans D. (2011), *Internet de las Cosas - Cómo la Próxima Evolución de Internet lo Cambia Todo*. Cisco Internet Business Solutions Group. Recuperado de: https://www.cisco.com /c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Felipe Rojo A. (2020), *Computación cuántica: Análisis y Ejecución de Algoritmos Cuánticos*. Pontificia Universidad Católica Argentina, Facultad de Ingeniería y Ciencias Agrarias. Recuperado de: https://repositorio.uca.edu.ar/bitstream/ 123456789/11211/1/ computacion-cuantica-analisis-algoritmos.pdf

Garrigós Candela, E. (2022). *Supremacía Cuántica: ¿El Fin de la Seguridad Clásica?* Universitat Politècnica de València, Escuela Técnica Superior de Ingeniería Informática. España, Valencia. Recuperado de: https://riunet.upv.es/bitstream/handle/ 10251/185282/Garrigos%20-%20SUPREMACIA%20CUANTICA%20EL%20FIN %20DE%20LA%20SEGURIDAD%20CLASICA.pdf?sequence=1&isAllowed=y

Giles M. (2019), *Explainer: What is a Quantum Computer?* MIT. Estados Unidos, Massachusetts. Recuperado de: https://www.technologyreview.com/2019/01/29/ 66141/what-is-quantum-computing/

Golden D., Soutar, C., Barmes, I., Buchholz, S., Brown, C., (2021), *Preparing the Trusted Internet for the Age of Quantum Computing*. Deloitte Insights. Reino Unido. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/ risk/deloitte-nl-risk-di-quantum-series-article-1.pdf

IBM, *What is Quantum Computing?* Recuperado de: https://www.ibm.com/topics/quantum-computing

Joyanes Aguilar, L. (2011), *Computación en la Nube e Innovaciones Tecnológicas - El Nuevo Paradigma de la Sociedad del Conocimiento*. Universidad Pontificia de Salamanca para la Facultad de Ingeniería-UNA de Paraguay. Recuperado de: https://www.academia.edu/5313180/Computaci%C3%B3n_en_la_Nube_e_ innovaciones_tecnol%C3%B3gicas

Kleinman Ruiz I. (2019), *Computación Cuántica: Aplicaciones Prácticas que la Computación Clásica no Puede Solucionar*. Universidad Carlos III. España, Madrid. Recuperado de: https://www.researchgate.net/publication/337758188_Computacion _cuantica_Aplicaciones_practicas_que_la_computacion_clasica_no_puede_solucionar

Krawczyk, H. (2014), *Public-Key Cryptography – PKC 2014*. IBM TJ Watson Research Center. Estados Unidos, Nueva York. Editorial Springer.

Moret Bonillo V. (2013). *Principios Fundamentales de Computación Cuántica*. Universidad de La Coruña. España, La Coruña. Recuperado de: https://enginyeriainformatica.cat/ wp-content/uploads/2016/05/PRINCIPIOS-FUNDAMENTALES-DE-COMPUTACI %C3%93N-CU%C3%81NTICA.pdf

Museo Histórico Militar de Burgos (2010). *Proyecto Enigma: "Máquina Enigma, Código Resuelto"*. Recuperado de: https://ejercito.defensa.gob.es/Galerias/Descarga_pdf /Unidades/Madrid/Ihcm/2018/20180201-video-enigma-burgos-dossier.pdf

Oliver C., Suman V. (2021*), Why Quantum Computing is a Big Deal?* Kearney. Recuperado de: https://www.kearney.com/communications-media-technology/article/-/insights/why-quantum-computing-is-a-big-deal

OTECH (2022), *Un Dispositivo Fotónico Cuántico Tardó Microsegundos en Realizar una Tarea en la que una Computadora Convencional Pasaría 9,000 Años*. México, Hidalgo. Recuperado de: https://otech.uaeh.edu.mx/noti/index.php/ computacion-cuantica/un-dispositivo-fotonico-cuantico-tardo-microsegundos-en-realizar-una-tarea-en-la-que-una-computadora-convencional-pasaria-9000-anos/

Mell P., Grance T., *Effectively and Securely Using the Cloud Computing Paradigm*. NIST, Information Technology Laboratory. Estados Unidos, Maryland. Recuperado de: https://csrc.nist.gov/CSRC/media/Presentations/Effectively-and-Securely-Using-the-Cloud-Computing/images-media/fissea09-pmell-day3_cloud-computing.pdf

Nasser Darwish M. (2014). *Computación Cuántica*. Universidad de La Laguna. España, Tenerife. Recuperado de: https://www.mundotec.com.ar/Computacion-Cuantica.pdf

Rúa Vargas J., Branch B., John W. (2009). *Estado del Arte de la Computación Cuántica*. Universidad Nacional de Colombia. Colombia, Medellín. Recuperado de: http://www.redalyc.org/articulo.oa?id=133113598026

Salazar J., Silvestre S. (2017), *Internet de las Cosas*. České vysoké učení technické v Praze Fakulta elektrotechnická. República Checa, Praga. Recuperado de: https://psm.fei.stuba.sk/pages/95/LM08_F_ES.pdf

Saniz Balderrama R. (2001), *Computación Cuántica*. Universidad Católica Boliviana. Bolivia, Cochabamba. Recuperado de: http://www.scielo.org.bo/pdf/ran/v1n2 /v1n2a06.pdf

Sun Tzu (2003), *El Arte de la Guerra*. Biblioteca Virtual Universal. Recuperado de: https://biblioteca.org.ar/libros/656228.pdf

Targhi, E. y Unruh, D. (2016), *Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transform*. Universidad de Tartu. Estonia, Tartu. Recuperado de: https://doi.org/ 10.1007/978-3-662-53644-5_8

Wallden, P. y Kashefi, E, (2019), *Cyber Security in the Quantum Era*. Recuperado de: https://dl.acm.org/doi/pdf/10.1145/3241037