HABLANDO DE CIBERSEGURIDAD

Conversaciones con Miguel Gutiérrez Rodríguez

Omar Pérez Salomón

EBOOK

HABLANDO DE CIBERSEGURIDAD

Conversaciones con Miguel Gutiérrez Rodríguez

Omar Pérez Salomón

Edición
Dulce María García Medina

Diseño de cubierta
Heinz Benítez Jiménez

Diseño de interiores y composición
Heinz Benítez Jiménez

Corrección
Oday Enríquez Cabrera

© Omar Pérez Salomón ®, 2021
© CITMATEL ®, 2021

ISBN 978-959-315-173-3

CITMATEL
Avenida 47 No. 1802 entre 18-A y 20,
Playa, La Habana, Cuba. CP. 11300.
Teléfono: (537) 204 3600
comercial@citmatel.com
www.editorialcitmatel.com
www.libreriavirtualcuba.com

PRESENTACIÓN

El desarrollo mundial de las Tecnologías de la Información y la Comunicación (TIC) y la transformación digital en curso, están empujando a las empresas, profesionales y sociedad toda, a cambiar su manera de pensar, actuar y trabajar.

Los pasos indetenibles en la internet de las cosas, Industria 4.0, Inteligencia artificial, Analítica de datos y la implantación de nuevas tecnologías, requieren un cambio de visión de la seguridad tradicional, que tome como premisas la elevación de la ciberseguridad frente a las amenazas, ataques y riesgos a los que se exponen las TIC, su gestión acorde con los estándares y buenas prácticas en seguridad y potenciar la preservación y el desarrollo del capital humano asociado a la actividad.

Según el informe de seguridad Kaspersky 2020, durante el año 2020, 10.18 % de los equipos de los usuarios en el mundo sufrieron, al menos una vez, un ataque web de la clase *malware*.

Las soluciones de esta empresa neutralizaron 666 809 967 ataques lanzados desde recursos de internet ubicados en diversos países del mundo, encabezados por los Estados Unidos; registraron 173 335 902 URL maliciosas únicas en las que se activó el antivirus web; y en 668 619 equipos de los usuarios se neutralizaron intentos de ejecución de programas maliciosos diseñados para robar dinero mediante el acceso en línea a cuentas bancarias.

En ese período se detectó un promedio de al menos un programa malicioso en 28.65 % de los equipos, discos duros o medios extraíbles pertenecientes a los usuarios de Kaspersky[1].

El tema de la Covid-19 también estuvo presente en los ataques de *phishing* bancario, en las falsificaciones de mensajes, en el pago de impuestos y en el robo de datos personales a nivel internacional.

[1] Boletín de seguridad Kaspersky 2020. Disponible en www.kaspersky.com

En el plano externo, los países más poderosos del planeta se han propuesto mantener la supremacía en el ciberespacio y en el control del espectro radioeléctrico. La lucha por el dominio de la próxima generación de la tecnología de comunicaciones móviles, la denominada 5G, y el control de los contenidos y servicios que se brindan *on line*, son ejemplos de ese empeño imperial.

La carencia de normas y regulaciones de ciberseguridad facilita la escalada de los incidentes, limitando las posibilidades de actuación de los organismos internacionales en este contexto.

Es notorio que en los últimos años se ha producido un aumento considerable del uso de las TIC e internet para fines contrarios a la paz y la seguridad internacional, delictivos y de desestabilización política.

En la VII Cumbre de las Américas, celebrada en Panamá en 2015, el General de Ejército Raúl Castro Ruz denunció esta situación:

> No puede aceptarse que menos de una decena de emporios, principalmente estadounidenses —cuatro o cinco de siete u ocho—, determinen lo que se lee, ve o escucha en el planeta. Internet debe tener una gobernanza internacional, democrática y participativa, en especial, en la generación de contenidos. Es inaceptable la militarización del ciberespacio y el empleo encubierto e ilegal de sistemas informáticos para agredir otros Estados[2].

Varios países, a los cuales se ha sumado Cuba, han abogado porque estas cuestiones sean discutidas en el marco multilateral de las Naciones Unidas, con vistas a avanzar hacia el establecimiento de un marco internacional justo, democrático y participativo, que permita dar una respuesta efectiva a los retos y amenazas, iniciativa que no se ha podido concretar por la oposición de los Estados Unidos y sus aliados.

El trascendente propósito de informatizar la sociedad cubana carecería de sentido, si olvidáramos desarrollar la seguridad de las TIC y la defensa del ciberespacio nacional; para lo cual se ha creado un sistema de trabajo que incluye a los operadores de redes de telecomunicaciones, proveedores de servicios, aplicaciones y productos, usuarios de las TIC y las entidades encargadas de la dirección, el monitoreo, control y la supervisión de la seguridad informática, así

[2] Discurso del General de Ejército Raúl Castro Ruz, en la VII Cumbre de las Américas, Panamá, 11 de abril de 2015. Disponible en www.cubaahora.cu

como de las actividades relacionadas con la vigilancia tecnológica, la alerta temprana y la gestión de incidentes.

Las medidas adoptadas en nuestro país para la protección del ciberespacio nacional comprende seis ámbitos de actuación: organizacional, tecnológico, jurídico, gestión del capital humano, cooperación internacional y comunicación institucional; y hoy más que nunca requieren de un perfeccionamiento, teniendo en cuenta que los in cidentes de ciberseguridad y los programas malignos detectados crecieron en el año 2020 en relación con el anterior.

La actualización constante de los planes de formación y capacitación de los profesionales y del personal vinculado a la ciberseguridad, constituye cuestión clave del trabajo en esta actividad. Existen seis universidades con planes de estudio en la materia en pregrado, posgrado y técnico superior universitario.

Entre los años 2019 y 2020, la Oficina de Seguridad para las Redes Informáticas de Cuba (OSRI) emitió más de 400 reclamaciones internacionales hacia equipos de respuesta a incidentes de varios países desde donde se originaron ciberataques contra el nuestro que, además de las afectaciones ocasionadas, denigran el prestigio internacional de la nación.

En términos potenciales, los ciberataques podrían afectar los servicios de telecomunicaciones y las infraestructuras críticas del país, provocando interrupciones en las aplicaciones y plataformas informáticas que soportan el proceso de informatización de la sociedad, así como la pérdida o daños a la información y los datos que se preservan en estas.

Los últimos años se han caracterizado por el incremento de las acciones subversivas contra nuestro país, empleando las redes sociales digitales, que tienen como objetivo promover una imagen de ingobernabilidad, crisis social, descrédito institucional e incentivar conductas de enfrentamiento, indisciplina social y actuación delictiva, todo lo cual impone nuevos y complejos desafíos a la seguridad del ciberespacio nacional.

Es en este escenario que se presenta una visión desde Cuba, de disímiles aspectos relacionados con la ciberseguridad, redactados con un lenguaje comprensible para personas ajenas a esta activi-

dad. Se exponen, de manera íntegra, las entrevistas que realicé por espacio de un año en medios como *Cubadebate* y *La pupila insomne*, a Miguel Gutiérrez Rodríguez, experto en sistemas informáticos y ciberseguridad, que fungió como vicepresidente de Tecnologías en las empresas Correos de Cuba y Desarrollo de *Software* (DESOFT), director de la OSRI de nuestro país y director general de Informática del Ministerio de Comunicaciones.

Así, las causas y condiciones que facilitan los incidentes de ciberseguridad y su gestión, las medidas para fortalecer la protección del ciberespacio nacional de Cuba, la guerra cibernética en entornos digitales, el *status quo* de la gobernanza de internet y las violaciones y uso inadecuado del espectro radioeléctrico nacional, aparecen junto a otras temáticas en la información ofrecida por el entrevistado.

También se aportan datos y declaraciones muy apreciables referidas al modo de actuación para afrontar de forma adecuada un incidente de ciberseguridad, la protección a las infraestructuras críticas, migración a plataformas de código abierto, las normas jurídicas aprobadas en el país, las noticias falsas o *fake news* y la manipulación en el tema internet en Cuba, entre otros.

Mis aportes y preguntas aparecen en cursivas y las respuestas del entrevistado en redondas, para mayor comprensión del lector.

Esperamos que este libro tenga un impacto positivo en especialistas y lectores en general, contribuya a promover un mayor y mejor uso de las TIC, y a lograr una cultura social en ciberseguridad.

Omar Pérez Salomón.

INICIOS DE LOS EVENTOS DE CIBERSEGURIDAD

Primeros incidentes

¿Cuándo aparecen los primeros incidentes de seguridad?

Los incidentes de seguridad en los sistemas informáticos aparecen desde que comenzó el uso de estas tecnologías[3]. En 1947, los creadores de la computadora electromecánica Mark II informaron del primer caso de error en un ordenador causado por un insecto. El equipo sufrió un fallo en un relé electromagnético y durante la investigación se encontró una polilla que provocó que ese relé quedase abierto. Una de las programadoras, al registrar el incidente en la bitácora habilitada, pegó en ella el insecto con cinta adhesiva y se refirió a él como un *bug* (bicho) para describir la causa del problema[4].

El reemplazo de las válvulas electrónicas por el transistor bipolar y la integración a gran escala de los procesos en pequeños chip de silicio permitieron disminuir el tamaño de los equipos, aumentar su potencia y la capacidad de procesamiento de datos, así como disminuir los precios de los mismos. ¿Qué repercusión tuvieron esos adelantos en la seguridad informática?

Esta evolución tecnológica, positiva por supuesto, trajo consigo que se incrementaran de manera considerable los sitios donde los datos y el *hardware* estuvieran expuestos a diversas amenazas[5].

[3] García Pierrat, Gonzalo: *Administración de incidentes de seguridad informática,* La Habana, 2014, p. 8-13. La idea de este texto surgió en la Oficina de Seguridad para las Redes Informáticas, como parte del proyecto ALBACERT, a raíz del convenio bilateral Cuba-Venezuela, que pretendía crear en cada país del ALBA un equipo de respuesta a incidentes de ciberseguridad, y donde a Cuba le correspondía la formación y capacitación en esta materia.

[4] Ibídem.

[5] Ibídem.

A partir de ese momento se comenzaron a interconectar las computadoras para compartir datos, formando redes de diferentes tipos y dimensiones en las entidades. A finales de la década del ochenta estas redes comenzaron a conectarse con otras y surgió gran variedad de dispositivos de acceso portátil e inalámbrico. De tal manera se introdujeron nuevos factores de riesgo, posibilitando una vía para potenciales accesos no autorizados.

¿Cuál se considera el primer ataque a la infraestructura computacional de internet?

A finales de 1988 se estimaba que estaban conectadas a internet unas 60 mil computadoras. El 2 de noviembre de ese año, un programa informático atacó la red y afectó durante horas cerca del 10 % de todos los ordenadores ubicados en los Estados Unidos, incluyendo los del Centro de Investigación de la NASA. El autor fue Robert Tappan Morris, estudiante estadounidense de 23 años. A ese programa malicioso se le denominó "gusano Morris" (Morris *worm*) y se considera el primer ejemplo de *software* malicioso (*malware*) que afectó a internet[6].

Creo que el juicio a Morris derivó en la primera condena por la ley de fraudes informáticos de 1986 en los Estados Unidos.

Así es. Morris fue procesado, y en el juicio realizado en enero de 1990, la fiscalía argumentó que se trató de un ataque contra el Gobierno de los Estados Unidos y el jurado federal lo declaró culpable. De nada valió que los abogados de Morris aseguraran que intentaba ayudar a la seguridad de internet. Este primer ataque a la infraestructura computacional de internet trajo como consecuencia la creación por la Agencia de Investigación de Proyectos Avanzados de Defensa (ARPA) de los Estados Unidos, del primer equipo de respuesta a emergencias computacionales (CERT por sus siglas en inglés), ubicado en la universidad Carnegie Mellon, en Pitsburgh, Pensilvania. Después, muchos países comenzaron a crear estructuras similares y a establecer los contactos entre ellas[7].

[6] Ibídem.
[7] Ibídem.

¿Qué casos tuvieron connotación internacional a inicios del presente siglo?

Hay otro caso de un gusano informático, detectado en mayo de 2000 en Filipinas, que infectó a unos 50 millones de ordenadores en el mundo, el 10 % de las máquinas con conexión a internet en ese momento.

Afectó al Departamento de Defensa de los Estados Unidos, la CIA, al Parlamento británico y a varias empresas. Se calculó que los daños causados sobrepasaron los 5 mil millones de dólares. Como en esa época Filipinas carecía de leyes sobre delitos informáticos, no se pudo juzgar al culpable[8].

En el año 2004 circularon seis familias de organismos malintencionados, casi todos vinculados con los *spammers* (creadores de *spam*), o con el robo de información bancaria. Sasser, considerado el gusano más rápido de la historia, fue capaz de comprometer entre 100 mil y 200 mil computadoras en los primeros 10 minutos de su propagación, con capacidad para duplicar la cantidad de nuevas víctimas cada 8.5 segundos. Estaba dirigido a Windows 2000/XP; los infectaba automáticamente con el propósito de buscar direcciones IP y, a través de FTP, transferir el gusano a otros equipos. En el año 2015 resultó una novedad la creación de códigos destinados a afectar teléfonos móviles inteligentes.

Comportamiento en Cuba

¿Cómo ha evolucionado la seguridad informática en las entidades estatales cubanas en los últimos años?

En 1988 se detectó el primer virus informático proveniente del exterior, nombrado Vienna.648. En 1991 se reveló un virus desarrollado en nuestro país, el cual fue identificado como TERMINATOR.A. Tuvo como características que se replicó en el sistema operativo MS-DOS, teniendo como blancos a ficheros ejecutables.COM, que fueron destruidos durante la propagación, al sobrescribir sus códigos.

[8] Ibídem.

En este último caso, cuando se ejecutaba una aplicación infectada, solo lo hacía el virus hospedado y no el código del programa original, por lo que los usuarios apreciaron que algo extraño sucedía, siendo muy bajo su nivel de propagación. Otra de sus características es que contenía una condición de activación para destruir los primeros 32 sectores del disco activo[9].

En 1992 fue identificada una segunda variante, TERMINATOR.B, que se propagaba adicionando su código al inicio del fichero, mientras guardaba cifrado el código del programa original. El creador de ambos fue el primer autor confeso de programas malignos elaborados en Cuba.

El destructivo virus KILL_CVS, reportado en 1999, que tomaba como anfitriones a los ficheros .COM, intentó borrar de las computadoras al programa antivirus de factura nacional: CVS.EXE.

El virus macro WM.Mortal Kombat, fue el primero de su tipo de los destinados a nuestro país. Escrito en lenguaje Word Basic de Microsoft Word, infectaba a los documentos versiones 6.x y 7.x cuando eran abiertos. A partir de 2001 comenzaron a detectarse aplicaciones Windows de 32 bits con acciones malignas, creadas en Cuba o para Cuba.

En el año 2004 se reportaron 306 nuevos programas malignos, casi uno diario. Esa cifra superó la cantidad de 247, valor obtenido de la suma de los totales de los años 2001, 2002 y 2003.

En la cuenta virus@segurmatica.cu se recibieron más de 100 mil mensajes reportando programas malignos en ese período. Se mantuvo la tendencia de que los caballos de Troya fueran los más reportados, entre los que se incluyeron los *spywave*, los utilizados para crear las redes robots, los portadores y descargadores de códigos malignos y los que realizan ataques *phishing*. (Tabla 1; Cuadro 1).

[9] Guadis Salazar, Edgar: *Evolución de los programas malignos desarrollados en Cuba o para Cuba*, Rev. *Tino,* No. 46, 27 de octubre de 2015.

Tabla 1. Portadores de códigos malignos por año

Año	Mensajes portadores de códigos malignos	Mensajes spam
2002	1 de cada 11	1 de cada 16
2003	1 de cada 2.5	1 de cada 33
2004	1 de cada 1.4	1 de cada 212

Fuente: http://www.segurmatica.cu

Cuadro 1. Cantidad de programas malignos detectados hasta 2004

Programas malignos	Cantidad
Virus	376
Caballo de Troya	289
Gusanos	229
Exploits	20
Jokes	19
Total	**933**

Fuente: http://www.segurmatica.cu

Aunque a nivel de las personas jurídicas, en los últimos años, se aprecian algunos avances en la seguridad informática[10], aún son insuficientes. En el año 2013, los controles realizados en 421 entidades por la OSRI determinaron que 44 % tenían su seguridad informática vulnerable o muy vulnerable. En 2018 fue en 32.43 % de los 772 centros controlados.

Para que se tenga una idea de las consecuencias de las violaciones y vulnerabilidades que existen en las redes, les pongo solo dos ejemplos que ilustran el fenómeno.

En mayo de 2013, la OSRI recibió un reporte de una de las redes más grandes del país, donde se notificaba la detección de conexiones inusuales desde su red hacia los servidores de un sitio del sector de

[10] El término seguridad informática tiene igual significado que el de seguridad de las TIC, el cual está relacionado con la confidencialidad, integridad y disponibilidad de la información que se genera, procesa y almacena por los terminales y se transmite por las redes de datos.

la cultura. Las investigaciones realizadas determinaron que se trataba de un ataque informático, donde desconocidos tomaron el control de los servidores del sitio con el objetivo de ofertar servicios ilegales de navegación por internet a 25 CUC mensual, y buscar nuevas víctimas mediante la exploración de las redes nacionales.

Se determinó que esos mismos atacantes vulneraron y llegaron a controlar los sistemas informáticos de más de 50 entidades. Los atacantes descargaban desde un sitio en Canadá los programas que utilizaban para vulnerar la seguridad de las redes, y mostraron un alto grado de organización que los convirtieron en una amenaza al empleo seguro de las tecnologías de la información en nuestro país.

En ese mismo año, desde un hotel en Varadero, se realizó un ataque hacia un centro de investigación ubicado en el exterior, debido a la utilización inadecuada de los servidores del hotel por el administrador de la red, que permitió se alojara un virus informático que realizaba este tipo de actividades. En tal caso se puso en riesgo la seguridad nacional.

Dentro de las categorías de incidentes de seguridad informática más reportados en 2018 estuvo la explotación de vulnerabilidades. ¿Qué afectaciones provocaron las mismas?

En ese período se detectaron unas 500 direcciones IP con vulnerabilidades. La más significativa estuvo relacionada con la ejecución remota de código, si un atacante enviaba mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1).

La explotación de esta vulnerabilidad se alertó desde el año 2017 por la OSRI, debido a que esta permite la infección de equipos computacionales por un *malware* del tipo “WannaCry” que, tras instalarse, bloquea el acceso a los ficheros del ordenador afectado y como es típico en este tipo de virus, solicita un rescate para permitir el acceso y podría afectar, a su vez, al resto de los ordenadores vulnerables de la red a la que pertenece.

El servicio más afectado por las vulnerabilidades fue el SMB, que utiliza un protocolo de red, el cual permite compartir archivos, impresoras y otros elementos, entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows.

Está claro, como alegan muchos especialistas, que es imprescindible migrar a aplicaciones nacionales de código abierto, priorizando las infraestructuras estratégicas del país. Aunque en otros momentos se hicieron intentos por concretar el propósito, hay que reconocer que se avanzó poco. Hoy tenemos mejores condiciones; existe un cronograma de migración con un seguimiento permanente por parte del Ministerio de Comunicaciones. Considero que una de las instituciones que más progresó fue la Aduana General de la República, y es un referente a seguir.

CAUSAS Y CONDICIONES QUE FACILITAN LOS INCIDENTES DE CIBERSEGURIDAD Y SU GESTIÓN

Tratamiento a las vulnerabilidades de los sistemas informáticos

La identificación de las vulnerabilidades del sistema y el establecimiento de medidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades, permite disminuir los incidentes de ciberseguridad[11]*. En este sentido, ¿cuáles son los tipos de vulnerabilidad conocidos?*

Como se refleja en el artículo 9 del Decreto No. 360 de julio de 2019 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio[12] Nacional, la vulnerabilidad se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema.

En el citado texto de Gonzalo García Pierrat se plantea que, en correspondencia con su naturaleza y la manera en que se producen, se distinguen diferentes tipos de vulnerabilidades:

---

[11] La ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinadas a garantizar la protección y el uso legal del ciberespacio. En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes, el fortalecimiento de la resiliencia (capacidad de tolerar adaptarse a condiciones adversas y recuperarse de las afectaciones provocadas por incidentes, manteniendo la continuidad de su funcionamiento sin detrimento importante en su capacidad de cumplir las funciones principales del sistema), y la recuperación ante ataques y otras afectaciones.

[12] El ciberespacio es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones que interactúan entre sí y con personas, y en el que la información se crea, procesa, almacena y transmite.

- Vulnerabilidad física: se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo. Por ejemplo, ventanas sin rejas, cercado perimetral deficiente y falta de compartimentación.

- Vulnerabilidad natural: grado en que el sistema puede verse afectado por desastres naturales o ambientales que puedan dañarlos como inundaciones, incendios, rayos, terremotos, fallos eléctricos, polvo, humedad y temperatura excesiva.

- Vulnerabilidad del *hardware* y el *software*: algunos dispositivos pueden ser más vulnerables que otros. Ciertos fallos o debilidades del *software* del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. Aquí se incluyen todos los errores en los sistemas operativos u otros tipos de aplicaciones que permiten atacarlos. Un ejemplo frecuente de este tipo de vulnerabilidad se observa en los dispositivos magnéticos utilizados para las copias de seguridad, que obliga en la mayoría de los casos, a mantener más de una versión por si se producen fallos.

- Vulnerabilidad de los medios o dispositivos: se refiere a la posibilidad de robar o dañar los equipos que forman parte de la infraestructura computacional, incluyendo sus componentes y medios removibles, por ejemplo, discos, dispositivos USB y otros.

- Vulnerabilidad por emanación: los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen equipos y medios de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida, por lo que este tipo de vulnerabilidad cobra mayor importancia cuando se procesa información de mucho valor que requiere un acceso fuertemente restringido.

- Vulnerabilidad de las comunicaciones: la conexión de las computadoras a redes extiende la vulnerabilidad del sistema. Se incrementa el nivel de riesgo a que está sometido, al aumentar la cantidad de personas que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones, no importa si se emplean enlaces alámbricos o inalámbricos.

- Vulnerabilidad humana: el personal que administra y utiliza el sistema puede representar la mayor vulnerabilidad. Toda la seguridad del sistema descansa sobre su administrador, que tiene acceso al máximo nivel y sin restricciones. Los usuarios del sistema también representan un riesgo, ya que son los que pueden acceder al mismo, tanto de forma presencial como mediante conexión remota.

Los usuarios que posean baja preparación para el empleo de los sistemas, representan una vulnerabilidad que se manifiesta en una deficiente explotación y errores de operación[13].

¿Cómo las vulnerabilidades en los sistemas informáticos pueden dar lugar a un incidente de seguridad?

Las vulnerabilidades de cualquier sistema o aplicación adquieren su verdadera connotación en el momento en que pueden originar un incidente de seguridad, ya sea como resultado de un hecho accidental o intencional. En internet, varios sitios se dedican a buscar vulnerabilidades en los sistemas y publicarlas. Existen personas que desarrollan programas denominados exploit para generar incidentes de seguridad a partir de las vulnerabilidades, mientras que los fabricantes tratan de enmendarla a través de soluciones, conocidos como parches de seguridad. El problema está en que desde el momento en que la vulnerabilidad se conoce hasta que se aplica una solución, el sistema se encuentra expuesto a los ataques utilizando *exploit*, hechos especialmente para esa vulnerabilidad. Hoy el tiempo entre el descubrimiento de una vulnerabilidad y la aparición de una nueva técnica que explote la misma es muy corto[14].

[13] García Pierrat, Gonzalo (2014): *Administración de incidentes de seguridad informática*, pp. 23, 24, La Habana, Cuba.
[14] Ibídem.

¿En el caso de Cuba, cuáles son los aspectos que pueden convertirse en vulnerabilidades si no se le presta una debida atención?

A partir de nuestras condiciones considero que es imprescindible prestarle atención a las siguientes cuestiones:

- Implementación de las medidas de seguridad tecnológica, que acompañen de manera coherente los procesos de informatización del sector.

- Fortalecimiento de las estructuras organizativas que atiendan las funciones de la ciberseguridad.

- Separación física entre las redes.

- Preparación en temas de regulaciones vigentes o técnicas respecto a la ciberseguridad.

- Idoneidad en el personal que ocupa plazas de administración y supervisión de redes.

- Dar la prioridad necesaria a la conducción de la ciberseguridad.

- Elevar la percepción de riesgos.

- Analizar con rigor las causas y condiciones que pueden favorecer la ocurrencia de incidentes de ciberseguridad.

Los controles realizados por la OSRI a varias redes cubanas en el año 2019, dio como resultado que 30.4 % de las mismas obtuvieran una calificación de vulnerable o muy vulnerable. Si bien es cierto que existe una mejoría en relación con lo acontecido en años anteriores, es preciso aplicar con más rigor las medidas dirigidas a fortalecer la ciberseguridad.

Para que se tenga una idea de la evolución, basta decir que en el año 2013 los controles realizados en 421 entidades determinaron que 44 % tenía su seguridad informática vulnerable o muy vulnerable.

La vulnerabilidad más notificada fue el MS17-010, que afecta a la versión 1.0 del protocolo SMB de la plataforma Windows, permitiendo la ejecución de códigos de manera remota en el sistema vulnerable. Se hizo famosa a nivel mundial, al ser publicada por la organización Shadow Brokers y luego, por ser explotada por el *ransomware* WannaCry, para introducirse en distintos sistemas de todo el mundo.

Amenazas de ciberseguridad a que están expuestos los sistemas informáticos

No es posible comprender los fundamentos de la gestión de incidentes de ciberseguridad sin abordar las amenazas a que están expuestos los sistemas informáticos. ¿Cómo se clasifican las amenazas que ponen en peligro los sistemas informáticos?

En el Decreto No. 360 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, en su artículo 6, se define que la amenaza es la situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole, y representa los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

En dependencia de cómo se originan las amenazas, se pueden clasificar en accidentales o intencionales. Las primeras pueden ser producidas por causas naturales: inundaciones, rayos, terremotos, altas temperaturas, elevada humedad y presencia de polvo; laborales o sociales: surgen de acciones de las personas en las que no hay intención, como es el caso de borrar o modificar información por falta de entrenamiento o de conciencia sobre la seguridad. Las amenazas intencionales son provocadas por personas que pretenden de manera deliberada, acceder o dañar el sistema con motivos y objetivos diversos[15].

Por sus efectos o consecuencias, las amenazas pueden ser pasivas o activas. Las pasivas son aquellas que de materializarse no implican ninguna modificación a la información contenida en el sistema ni cambios en el estado del mismo. Es el caso del robo de información sin que esta se altere en lo más mínimo y que siga estando disponible para las personas y procesos con acceso legal a ella.

Las amenazas activas suponen la alteración de la información contenida en el sistema o cambios en el estado del mismo. Por ejemplo, la modificación de un programa que provoque que en lo

[15] García Pierrat, Gonzalo (2014): *Administración de incidentes de seguridad informática*, pp. 25-30, La Habana, Cuba.

adelante el sistema funcione de modo diferente, dando resultados distintos a los esperados[16].

También, cuando analizamos los efectos y consecuencias, las amenazas se pueden agrupar en:

- Interrupción: al producirse se interrumpe de algún modo el funcionamiento del sistema o se hace inaccesible o inútil y por tanto, se afecta su disponibilidad. Ocurre cuando se destruye algún dispositivo o se satura la memoria o el máximo de procesos en el sistema operativo, por solo poner dos ejemplos.

- Interceptación: tiene lugar cuando una persona, programa o proceso consigue acceder a una parte del sistema a la que no está autorizada y por lo general afecta la confidencialidad. Son difíciles de detectar pues, generalmente, no alteran la información o el sistema. Se da cuando se interceptan las conexiones telefónicas para capturar datos de una red, o se copian archivos o programas de forma ilícita.

- Modificación: una parte no autorizada no solo consigue acceder, sino que altera algún elemento y por tanto, afecta a la integridad. Por ejemplo, el cambio de valores en una base de datos, la alteración de un programa para que se comporte de forma distinta, o la modificación del contenido de los mensajes transmitidos en una red.

- Generación: se produce cuando una parte no autorizada inserta, por algún motivo, objetos falsos en un sistema (mensajes ilegítimos en una red, adición de registros a un archivo o añadir código en un programa), afectando la integridad[17].

En ocasiones confundimos el término de riesgo con el de amenaza a la hora de evaluar los factores que inciden sobre los sistemas informáticos.

Es cierto, con frecuencia tendemos a confundir ambas expresiones. En el propio Decreto No. 360, en el artículo 8, se identifica como riesgo a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización.

[16] Ibídem.
[17] Ídem.

El riesgo cuantifica la probabilidad de que una amenaza se materialice, causando un daño a los sistemas informáticos. Indica cuán probable es una amenaza y se expresa en valores numéricos, por lo general entre cero y uno, cero, cuando no es posible que la amenaza se produzca y uno, cuando hay evidencia para su materialización.

Para graficar lo anterior, consideremos la siguiente situación: las empresas o instituciones están expuestas a la amenaza de que se produzcan ataques para robar información. La probabilidad de que esto ocurra (riesgo) es muy baja, entre 0.2-0.3 para las que tienen dos redes (una interna sin conexión a internet y otra con conexión a la red de redes) y muy alta, mayor de 0.7 en las instituciones que poseen una sola red para todas las operaciones de la entidad.

¿Cuáles son las principales amenazas a que están expuestas las redes informáticas a nivel mundial?

En el sector bancario financiero existe un aumento de ciberataques dirigidos al robo de credenciales, espionaje en el comercio electrónico, ingeniería social asociada al comercio y ubicación de proveedores y de efectivos en bancos y a las criptomonedas.

En este sentido, se están utilizando programas para recopilar datos financieros y habilitar el retiro remoto de dinero de tarjetas de pago, cuentas bancarias en línea y cajeros automáticos, módulos de robo de información, *ransomware* y troyanos bancarios.

También se aprecia un incremento de ataques a datos expuestos en la nube y el empleo de plataformas y redes sociales para el robo de datos personales.

La industria del *malware* se desarrolla y ataca los sistemas operativos que sustentan la 4G y la 5G, la internet de las cosas, las tecnologías de la robótica, los programas vinculados con la inteligencia artificial y la Big Data.

Los ataques en la modalidad de *ransomware* tuvieron un aumento exponencial en los años 2019 y 2020, al igual que la explotación de las redes sociales para promover contenidos nocivos, noticias falsas, difamar, buscar liderazgo y capacidad de convocatoria.

Modalidades más empleadas en los ataques a los sistemas informáticos

¿Cuál es el patrón de conducta seguido por los atacantes en los ataques a los sistemas informáticos?

Un ataque[18] interno ocurre cuando usuarios legítimos de un sistema actúan de forma no autorizada o irresponsable. Los externos se producen con frecuencia, con el empleo de las posibilidades de acceso remoto destinadas a usuarios autorizados.

En correspondencia con el blanco elegido para ser atacado, los ataques pueden ser dirigidos o no dirigidos. En el caso de los primeros, estos se realizan sobre un blanco determinado de antemano, a partir de un interés específico, y en el caso de los no dirigidos, sobre un sistema al que se le haya detectado alguna vulnerabilidad que posibilite la agresión. En ambos casos, el atacante cumple un patrón de conducta, recorriendo determinadas etapas para lograr su objetivo:

- Reconocimiento: búsqueda de información sobre la entidad o sistema a atacar.

- Exploración (escaneo): identificación de sistemas operativos empleados, bases de datos, puertos abiertos y otros.

- Enumeración: servicios que se encuentran en ejecución.

- Entrada al sistema: mediante la explotación de vulnerabilidades existentes en servidores o aplicaciones.

- Escalada de privilegios: una vez dentro, tratar de obtener privilegios de administración.

- Mantener el acceso: instalar una puerta trasera para poder acceder de forma fácil en un futuro.

- Saltar a otros sistemas: utilizar los accesos obtenidos para acceder a otros sistemas.

- Limpieza del rastro: ocultar o borrar las evidencias del ataque.

[18] Se denomina ataque al intento de acceso o acceso a un sistema o una red informática o terminal, mediante la explotación de vulnerabilidades existentes en su seguridad.

Durante un ataque no dirigido, la secuencia de acciones es similar, comenzando por una búsqueda aleatoria de vulnerabilidades, que son explotadas para lograr el acceso[19].

El enfrentamiento exitoso a los ataques dirigidos a los sistemas informáticos, transita por el establecimiento de contramedidas que eviten que se exploten las vulnerabilidades que posean los mismos.

Creo que la identificación de las vulnerabilidades del sistema es vital para aplicar las técnicas de protección que eviten que un ataque tenga éxito. Como ejemplo positivo se puede mencionar que los portales institucionales de gobierno a todos los niveles, han recibido en menos de un año un número significativo de ataques y un mínimo ha sido exitoso.

Hay otros ejemplos, con menos condiciones de seguridad, donde estos ataques sí han tenido éxito. En el proceso investigativo, que siempre se hace, se identificaron fallas de seguridad.

Se han registrado casos de ataques internos por violación de las medidas de seguridad, lo cual es también un problema internacional. En ese sentido se han detectado pérdidas de información vital para las entidades, a partir de la introducción de dispositivos externos (memorias flash, discos externos y otros) por usuarios legítimos.

¿Cuáles son las herramientas más utilizadas por los atacantes para obtener información sobre el blanco seleccionado?

El ataque a una red informática estará casi siempre precedido de una intensa actividad de exploración que, en muchos casos, puede no ser advertida, durante la cual el atacante busca información sobre la topología, estructura y composición de las redes, la profundidad y solidez de las defensas y los probables puntos débiles de las mismas[20].

[19] Ibídem.
[20] Ibídem.

De manera general se utilizan las herramientas siguientes:

- Protocolo SNMP: se emplea para examinar la tabla de ruteo en un dispositivo inseguro, con el fin de conocer los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.

- Programa TraceRoute: puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico escogido como blanco del ataque.

- Protocolo Whois: servicio de información que provee datos acerca de todos los sistemas de nombres de dominios (DNS: Domain Name System) y el administrador responsable para cada dominio.

- Programa Nslookup: para acceder a los servidores DNS, a fin de obtener una lista de las direcciones IP y sus correspondientes nombres.

- Protocolo Finger: puede revelar información detallada acerca de los usuarios de un servidor específico (números telefónicos, tiempo y última sesión y otros).

A partir de la información obtenida, el agresor podrá iniciar acciones con el objetivo de lograr el acceso a algunas de las computadoras exploradas y poner en peligro a toda la red[21].

Como es lógico, los directivos de las empresas y entidades no pueden dominar los detalles técnicos citados, para eso están los especialistas en informática y en ciberseguridad; pero sí deben tener una cultura general en estas cuestiones. En la misma medida que avance la informatización y automatización de los procesos de una organización, debe avanzar la ciberseguridad; son como las dos alas de un pájaro.

[21] Ibídem.

¿Qué comportamiento tuvieron estos ataques a nivel internacional en el primer semestre de 2020?

Según datos ofrecidos por la empresa rusa de seguridad informática, Kaspersky Lab (Fig. 1), en el primer semestre de 2020, el porcentaje promedio de mensajes masivos no deseados, *spam*[22], en el tráfico global de correo fue de 52.39 %.

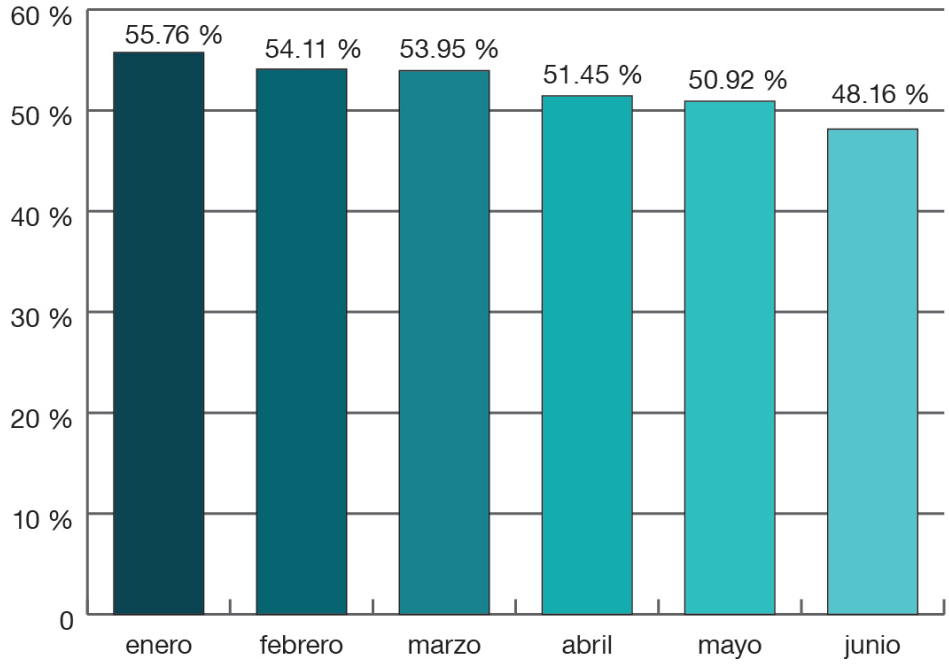


Fig. 1. Gráfico de la empresa rusa Kaspersky Lab.

Rusia (18.52 %) y Alemania (11.94 %) ocuparon los primeros lugares en el *ranking* de fuentes de *spam*. Le siguen Estados Unidos (10.65 %), Francia (7.06 %), China (7.02 %), Países Bajos (4.21 %), Brasil (2.91 %), Turquía (2.89 %), España (2.83 %) y Japón (2.42 %).

El país con la mayor proporción de usuarios atacados por *phishing*[23] en el primer trimestre de 2020 fue Venezuela (17.56 %), después

[22] Ídem

[23] Ataques que utilizan ingeniería social y recursos técnicos para robar credenciales de la identidad de consumidores. El término *phishing* proviene de la palabra inglesa *fishing* (pesca), haciendo alusión a que los usuarios (víctimas) "piquen el anzuelo" y den sus credenciales de acceso.

Portugal (13.51 %), Túnez (13.12 %), Francia (13.08 %) y Brasil (12.91 %). Cuba tiene 5.5 %.

En el primer semestre de 2020, el mayor número de ataques por *phishing* recayó en la categoría Tiendas en línea (19.42 %), el segundo lugar fue ocupado por Portales globales de internet (16.22 %); Bancos (11.61 %) pasó al tercer lugar y Redes sociales (10.08 %) al cuarto. (Fig. 2).

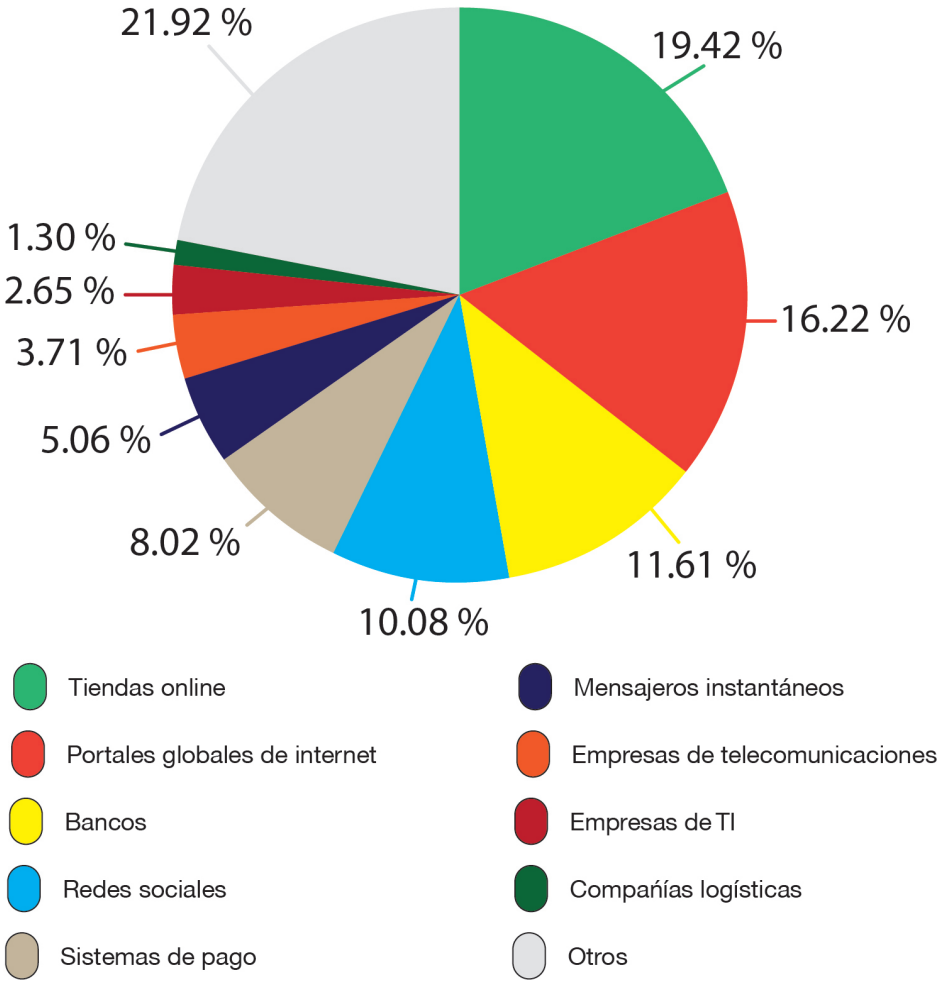


Fig. 2. Comportamiento de los ataques por *phishing* en el primer semestre de 2020.

En el caso de los programas maliciosos, ¿cómo se comportaron en el tráfico de correo en el segundo trimestre de 2020?

El *malware* Trojan.Win32.Agentb, con una participación del 13.33 %, resultó ser el más popular en el tráfico de correo. En el segundo lugar está Trojan-PSW.MSIL.Agensla.gen (9.40 %); en el tercero Exploit.MSOffice.CVE-2017-1188 (7.66 %). El cuarto puesto lo ocupó Hoax.Script.Scaremail.gen (3.93 %), mientras que en el quinto lugar está el Worm.Win32.WBVB.vam (2.57 %) (Fig. 3).

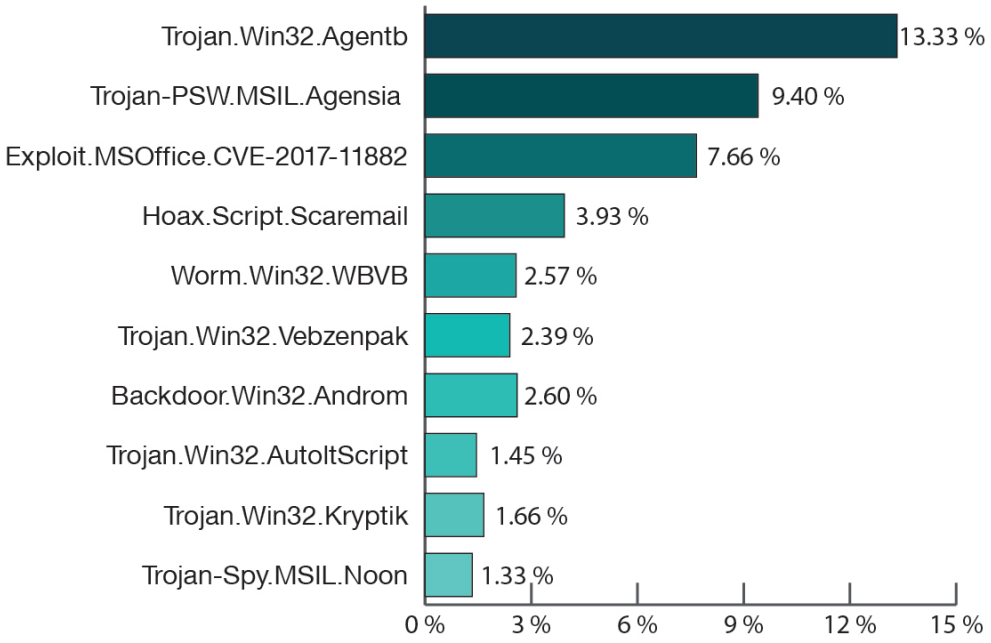


Fig. 3. Programas maliciosos en el tráfico de correo, segundo trimestre de 2020.

Cuba también ha recibido ataques en la variante de envío de mensajes masivos no deseados. ¿Qué características han tenido?

Entre enero y julio de 2019 en nuestro país, se reportaron más de 70 incidentes de este tipo, 68 % recibidos desde el exterior. Coincide que varios fueron dirigidos hacia redes de sistemas vitales para el funcionamiento del país como bancos, termoeléctricas, el sector de la ciencia, recursos hidráulicos y la del operador de telecomunicaciones, ETECSA.

¿Qué se establece en el Decreto 360/2019, de la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional sobre el envío de mensajes masivos?

En el artículo 49 de esta norma se plantea que queda prohibido el envío de mensajes masivos que no contengan, sea falso u oculto, el asunto y dirección o ubicación física o electrónica, número telefónico, identidad u otro medio de identificación del emisor que impidan a los destinatarios o receptores notificar su voluntad de no recibir más mensajes o no incluyan mecanismos que permitan al receptor manifestar su voluntad de no recibirlos; afecten el uso seguro y la calidad de las redes de telecomunicaciones de Cuba o de otros países o de los servicios que se prestan a través de estas; y posean un contenido que transgreda lo establecido en la legislación vigente cubana o los tratados, convenios o cualquier otro instrumento jurídico de carácter internacional de los que la República de Cuba es Estado parte.

¿Qué medidas deben acometer los operadores y proveedores para enfrentar los mensajes que contengan las características referidas anteriormente?

A los operadores y proveedores cubanos corresponde bloquear el envío, recepción o transmisión de los mensajes masivos dañinos que se cursan por sus redes y utilizan sus servicios; suspender temporalmente, hasta un mes, las comunicaciones entre sus redes y las que se establecen con las redes de operadores o proveedores extranjeros que no adopten las medidas necesarias para impedir el tráfico de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, dar cuenta al Ministerio de Comunicaciones; y suspender temporalmente, hasta un mes, el servicio prestado a los usuarios responsables del envío de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, dar cuenta al Ministerio de Comunicaciones, a los órganos del Ministerio del Interior o de la Fiscalía General de la República.

En los contratos suscritos por los operadores y proveedores entre sí y con sus usuarios, se incluye una cláusula sobre la responsabilidad derivada del envío de mensajes masivos dañinos a través de las redes de telecomunicaciones con utilización de las TIC o de los

equipos terminales de telecomunicaciones que son objeto de control por el Ministerio de Comunicaciones y, ante su incumplimiento, se le aplican las medidas previstas en la legislación vigente.

¿Qué se instituye en el artículo 53 del Decreto 360/2019, acerca de la responsabilidad por el envío de mensajes masivos dañinos?

En tal sentido, dicho artículo expone que, es responsable del envío de mensajes masivos dañinos toda persona natural o jurídica que directamente los envíe; los genere a través de los equipos de telecomunicaciones de otras personas; los transporte o intermedie en su difusión o trasmisión o haya incidido en su contenido, si mediante sus medios técnicos lo hubiese conocido y no evita su transportación, difusión, trasmisión, envío y reenvío; y cree, venda, preste, intercambie o realice cualquier tipo de recolección o transferencia de listas de direcciones de correo electrónico, números telefónicos u otro medio de identificación del emisor que haya sido realizada sin la autorización o consentimiento de su titular o del operador o proveedor de los servicios y sean conformadas para el envío de mensajes masivos dañinos.

Modo de actuación para afrontar de manera adecuada un incidente de ciberseguridad

¿Qué características tuvieron los incidentes que afectaron los sistemas informáticos cubanos en el año 2020?

En general, hubo un incremento de los incidentes en el año 2020 en relación con el año 2019, también fueron más las reclamaciones internacionales enviadas desde nuestro país y las recibidas. (Fig. 4).

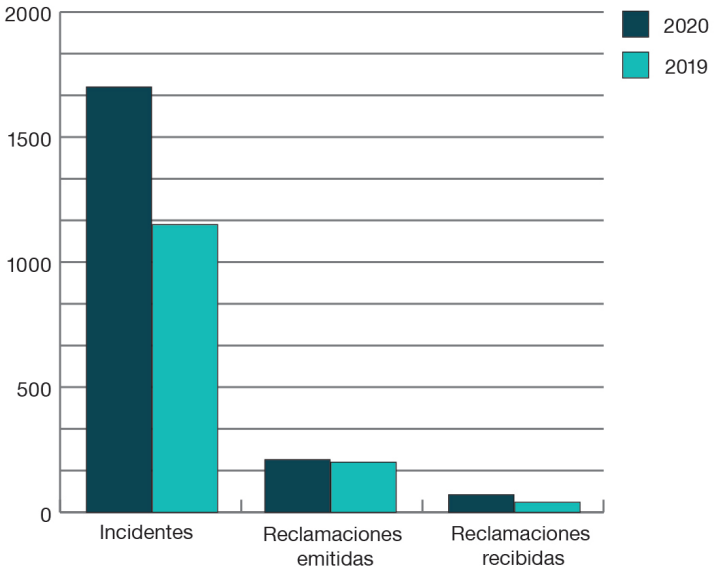


Fig. 4. Comportamiento de los incidentes en el año 2020.

Las categorías principales de incidentes ocurridas el año anterior fueron los troyanos, acciones no autorizadas sobre los sistemas, programas maliciosos, denegación de servicios y correos no deseados. (Fig. 5).

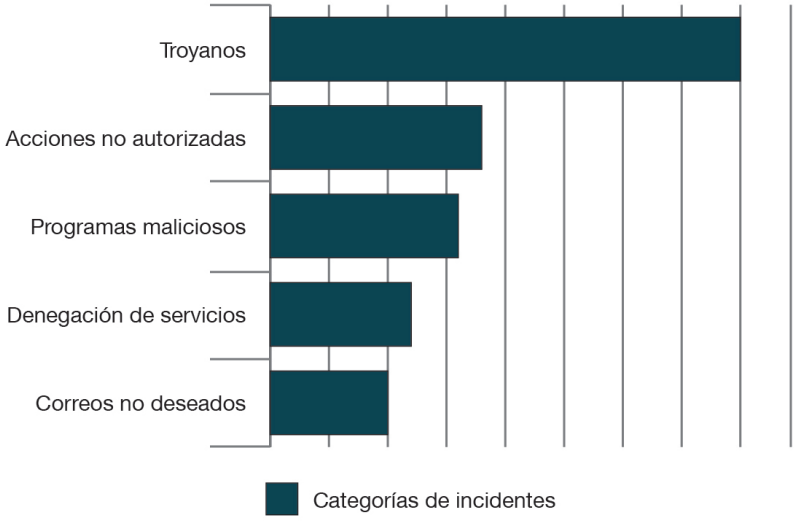


Fig. 5. Categorías de incidentes.

¿Cuáles son las reglas a seguir para minimizar la cantidad y repercusión de los incidentes de ciberseguridad?

La preparación para afrontar incidentes es vital si queremos reducir su impacto nocivo. En este sentido, es preciso definir con antelación una estrategia de respuesta a los mismos y tener en cuenta un grupo de reglas para lograr ese propósito. Entre ellas tenemos:

- Establecer y poner en práctica políticas y procedimientos para la gestión de incidentes.

- Evaluar de forma sistemática las vulnerabilidades del entorno.

- Comprobar con regularidad todos los sistemas y dispositivos de red para garantizar que tengan instaladas las revisiones más recientes.

- Establecer programas de capacitación sobre seguridad.

- Supervisar y analizar con regularidad el tráfico de red y el rendimiento del sistema.

- Comprobar los procedimientos de restauración y copia de seguridad.

- Actualizar los planes de medidas de ciberseguridad.

- Priorizar las capacidades de supervisión y monitoreo propias.

- Perfeccionar las estructuras especializadas en ciberseguridad[24].

¿Cuáles son las proyecciones de trabajo del Ministerio de Comunicaciones en lo referido a la gestión de incidentes?

Son varias las proyecciones; dentro de ellas tenemos: crear cultura de ciberseguridad en la población para el uso de las TIC; concluir la fase de aprobación de normas pendientes y capacitar a personas jurídicas y naturales, dada la transversalidad de la ciberseguridad; continuar incrementando la protección del ciberespacio nacional; perfeccionar la ciberseguridad en el ámbito tecnológico; incremen-

[24] García Pierrat, Gonzalo (2014): *Administración de incidentes de seguridad informática*, p. 41, La Habana, Cuba.

tar la capacidad de producción de herramientas propias; fomentar el desarrollo de las entidades especializadas; incrementar el control y fiscalización en materia de ciberseguridad; aplicar la legislación vigente en materia de contravenciones ante conductas violatorias e indisciplinas que generen incidentes cibernéticos o creen las causas y condiciones para su ocurrencia; aprovechar al máximo las posibilidades de la cooperación internacional y fomentar, de conjunto con los Organismos de la Administración Central del Estado, la capacitación y concientización de todo el personal y la población en general.

MEDIDAS PARA FORTALECER LA PROTECCIÓN DEL CIBERESPACIO NACIONAL DE CUBA

Protección a las infraestructuras críticas

En el artículo No. 46 del Decreto-Ley No. 370 sobre La informatización de la sociedad en Cuba, publicado en la Gaceta Oficial Ordinaria de 4 de julio de 2019, se definen las infraestructuras críticas de las Tecnologías de la Información y la Comunicación como aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

Teniendo en cuenta la definición citada, ¿cómo está organizada la protección de las infraestructuras críticas en nuestro país?

Como se plantea en el Decreto No. 360 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, se ha creado un Sistema Nacional de Protección de las infraestructuras críticas de las TIC que tiene un conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de las infraestructuras críticas de las TIC, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como un flujo de información que abarque a todos sus integrantes.

En este momento estamos actualizando el Catálogo Nacional y el plan para la protección de las infraestructuras críticas de las TIC, que tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en

coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

¿Mencione algunos de los sectores y actividades que poseen infraestructuras consideradas críticas?

En cualquier país existen sectores que son estratégicos por su impacto en la economía, la sociedad, la seguridad y en la defensa nacional. Entonces, sus redes informáticas e infraestructura se consideran críticas en el caso de la banca, telecomunicaciones, información y comunicación social, energía, recursos hidráulicos, transporte, determinadas industrias, los órganos de la defensa, entre otros.

En el decreto se estable que los jefes de estas entidades responden por la garantía de la confidencialidad, integridad y disponibilidad de los datos sobre infraestructuras críticas de las TIC a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada; además garantiza que el personal vinculado a las mismas esté capacitado para su utilización, posean compromiso político, ético y de responsabilidad social y material; así como que conozcan sus deberes y derechos específicos en relación con estas. También ejecutan las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten su funcionamiento.

¿Cuál fue el primer ataque cibernético conocido a una infraestructura crítica?

Es un hito cómo en la década del ochenta se utilizó por primera vez un arma cibernética, cuando la CIA introdujo un *software* defectuoso en el sistema de operación del nuevo gasoducto transiberiano, que debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia, a países de Occidente, causando grandes pérdidas económicas y contribuyendo al colapso de la URSS.

Así lo describió el Comandante en Jefe, Fidel Castro Ruz, en su reflexión, *Mentiras deliberadas, muertes extrañas y agresión a la economía mundial*[25]:

> El Dossier, bajo el nombre de Farewell, llegó a la Agencia Central de Inteligencia (CIA) de los Estados Unidos en agosto de 1981. Dejaba claro que los soviéticos llevaban años realizando sus actividades de investigación y desarrollo. Dada la enorme transferencia de tecnología en radares, computadoras, máquinas-herramientas y semiconductores de los Estados Unidos a la Unión Soviética, podría decirse que el Pentágono estaba en una carrera armamentista consigo mismo.
>
> El Dossier Farewell también identificaba a cientos de oficiales de casos, agentes en sus puestos y otros suministradores de información a través de Occidente y Japón. Durante los primeros años de la distensión, los Estados Unidos y la Unión Soviética habían establecido grupos de trabajo en agricultura, aviación civil, energía nuclear, oceanografía, computadoras y medioambiente. El objetivo era comenzar a construir "puentes de paz" entre las superpotencias. Los miembros de los grupos de trabajo debían intercambiar visitas a sus centros.
>
> Aparte de la identificación de agentes, la información más útil aportada por el dossier la constituía la "lista de compras" y sus objetivos en cuanto a la adquisición de tecnología en los años venideros. Cuando el Dossier Farewell llegó a Washington, Reagan le pidió al director de la CIA, Bill Casey, que ideara un uso operativo clandestino del material.
>
> La producción y transporte de petróleo y gas era una de las prioridades soviéticas. Un nuevo gasoducto transiberiano debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia, a través de Kazajstán, Rusia y Europa oriental hasta los mercados de divisas de Occidente.
>
> Para automatizar la operación de válvulas, compresores e instalaciones de almacenaje en una empresa tan inmensa, los soviéticos necesitaban sistemas de control sofisticados. Compraron computadoras de los primeros modelos en el mercado abierto, pero cuando las autoridades del gasoducto abordaron a los Estados Unidos para adquirir el *software* necesario, fueron rechazados. Impertérritos, los soviéticos buscaron en otra parte; se envió un operativo de la

[25] Fidel Castro Ruz: "Mentiras deliberadas, muertes extrañas y agresión a la economía mundial", *Granma Digital*, 18 de septiembre de 2007.

KGB a penetrar un proveedor canadiense de *softwares,* en un intento por adquirir los códigos necesarios. La inteligencia estadounidense, avisada por el agente del Dossier Farewell, respondió y manipuló el *software* antes de enviarlo.

Una vez en la Unión Soviética, las computadoras y el *software*, trabajando juntos, hacían operar el gasoducto maravillosamente. Pero esa tranquilidad era engañosa. En el *software* que operaba el gasoducto había un caballo de Troya, término que se usa para calificar líneas de *software* ocultas en el sistema operativo normal, que hacen que dicho sistema se descontrole en el futuro, o al recibir una orden desde el exterior.

Con el objetivo de afectar las ganancias de divisas provenientes de Occidente y la economía interna de Rusia, el *software* del gasoducto que debía operar las bombas, turbinas y válvulas había sido programado para descomponerse después de un intervalo prudencial y resetear –así se califica– las velocidades de las bombas y los ajustes de las válvulas, haciéndolas funcionar a presiones muy por encima de las aceptables para las juntas y soldaduras del gasoducto.

El resultado fue la más colosal explosión no nuclear e incendio jamás vistos desde el espacio. En la Casa Blanca, funcionarios y asesores recibieron la advertencia de satélites infrarrojos de un extraño evento en medio de un lugar despoblado del territorio soviético.

El Comando de Defensa Aeroespacial Norteamericano (NORAD por sus siglas en inglés) temía que fuera el lanzamiento de misiles desde un lugar donde no se conocía que hubiera cohetes basificados; o quizás fuera la detonación de un dispositivo nuclear. Los satélites no habían detectado ninguna pulsación electromagnética, característica de las detonaciones nucleares.

Otras infraestructuras críticas como las plantas nucleares de Irán o la red eléctrica de Venezuela han sufrido ataques cibernéticos.

Así es. La aparición del gusano Stuxnet hizo más lento el funcionamiento de los motores de enriquecimiento de uranio de la central nuclear iraní de Bushehr, con el objetivo de retrasar el programa nuclear con fines pacíficos de Irán; pero atacó además a redes de varios países. De los ordenadores infectados, 60 % se encontraban en ese país. Circuló en redes globales desde marzo de 2010 y el diario *The New York Times* hizo público el 16 de enero de 2011, opiniones de expertos militares y de inteligencia estadounidenses, donde refle-

jaron que la central nuclear de Dimona (al sur de Israel) se convirtió en un laboratorio para examinar y ensayar el virus Stuxnet.

Se trató de un ataque particular y sofisticado, perpetrado por un equipo con acceso a abundantes recursos financieros, un elevado nivel de preparación y un profundo conocimiento técnico diseñado para espiar sistemas infectados, inutilizar plantas y causar daños en ambientes industriales.

¿Computadoras conectadas a redes informáticas de Cuba también fueron infectadas?

El 13 de julio de 2011 se detectó la presencia del Stuxnet en redes cubanas. A partir de un estudio realizado por la empresa Segurmática, se conoció que este programa maligno instaló dos *drivers* o controladores, firmados de forma digital con un certificado de la compañía Realtek, significando que el autor tuvo acceso a la llave privada de ese certificado, un secreto supuestamente muy bien guardado. El análisis realizado sobre esta cuestión por la empresa estadounidense Symantec, situó a Cuba en el lugar 14 de los países con más ordenadores infectados.

¿Qué valoración le merece las afectaciones a la red eléctrica de Venezuela ocurrido en marzo de 2019?

En el artículo, "Venezuela bajo ataque: 7 apuntes sobre el *shock* eléctrico", publicado en el sitio *Misión Verdad*, se dan a conocer algunos elementos importantes de este sabotaje:

> Esta vez no hubo un ataque a subestaciones o a líneas de transmisión eléctrica, como se había ensayado en distintas ocasiones con anterioridad, según manuales de sabotaje de la CIA contra la Nicaragua sandinista de los ochenta, ya desclasificados.
>
> Cabe acotar que el *software* usado (llamado Scada) en el Sistema de Control Automatizado (SCA), que operativiza el funcionamiento de los motores, es el creado por la empresa ABB, que desde hace años no trabaja en el país.
>
> Esta empresa ABB, que en Venezuela trabajó como Consorcio Trilateral ABB (ABB Venezuela, ABB Canadá, ABB Suiza), diseñó un proyecto de modernización del Guri a finales de la década pasada,

durante el gobierno de Hugo Chávez, en el que describe a profundidad tanto el sistema atacado como la organización básica del Guri.

El analista geopolítico Vladimir Adrianza Salas, en entrevista con *Telesur,* relaciona el ataque con el consorcio. Explicó que el embalse del Guri requiere un sistema de control que técnicamente se llama sistema Scada, el cual no es otra cosa que un sistema de supervisión, control y requisición de datos que permite, desde la perspectiva informática, controlar todos los elementos de generación de energía.

Si saboteas esto, saboteas el funcionamiento. Pero para sabotearlo esto necesitas dos cosas: o debes tener acceso desde afuera o debes tener complicidad interna para modificar los procesos.

Precedentes de este tipo se encuentran en países atacados o presionados directamente por los Estados Unidos, como Irak y el Líbano, donde los apagones fueron sistemáticos y de forma consecutiva, uno tras otro durante decenas de horas.

Las réplicas en la interrupción del suministro de energía responderían a estas secuencias de ofensivas, que ya han sido experimentadas en otros contextos de guerra asimétrica e irregular.

Por supuesto, se impone estudiar al detalle estas experiencias y adoptar las medidas necesarias para impedir ataques cibernéticos de esta naturaleza o de otro tipo.

Migración a plataformas de código abierto

Fortalecer la ciberseguridad del país pasa necesariamente por ejecutar un programa de migración[26] *hacia plataformas de código abierto. Usted reconoció que en la migración a plataformas de código abierto se avanzó poco en los últimos años. ¿Qué le hace pensar que ese estado puede cambiar a partir de este momento?*

Estamos hablando sobre un tema muy complejo, teniendo en cuenta la falta de una cultura de ciberseguridad en directivos, especialistas y la población en general; insuficiente percepción de riesgos; la tendencia a rechazar cambios; la inexistencia de un repositorio de

[26] Sustitución ordenada del sistema operativo y de todas las aplicaciones propietarias que se usen en las computadoras, por otras de código abierto; cuyas evaluaciones previas hayan demostrado estabilidad, seguridad, interoperabilidad, así como su factibilidad de ser auditadas.

aplicaciones nacionales en *software* libre que cubra las necesidades existentes; la obsolescencia tecnológica, la diversidad de dispositivos (impresoras, lectores de código de barra, escáner) de una parte de los medios de cómputo del país, entre otros problemas.

Los cambios no se lograrán de la noche a la mañana; pero pretendemos que en tres años los órganos y organismos de la Administración Central del Estado, y las infraestructuras de entidades estratégicas, migren hacia una distribución de sistema operativo en código abierto de producción nacional, que cumplan con los estándares de calidad y seguridad que necesitan las entidades. Esto nos permitirá crear las condiciones para con posterioridad avanzar en el sistema empresarial y el resto de las organizaciones.

El Decreto Ley de la Informatización de la sociedad cubana y el Decreto de Seguridad de las TIC, así como una norma específica para este proceso, establecen las indicaciones generales para el mismo.

El reto es grande, si tenemos en cuenta que la Aduana General de la República inició su proceso de migración en 1999 y lo concluyó en lo fundamental, en 2010; pero creo que podemos lograrlo con el concurso de todos y la conducción de los máximos dirigentes en cada lugar.

¿Qué acciones se deben ejecutar en lo inmediato para avanzar en el objetivo?

Ahora mismo estamos evaluando con las entidades desarrolladoras cómo incrementar la producción de programas y aplicaciones informáticas compatibles con sistemas operativos de código abierto, que respalden la implementación del proceso de migración hacia plataformas de este mismo tipo. Se impone tener un repositorio con estas aplicaciones.

También debemos garantizar la capacitación del personal cuando estas aplicaciones sean desplegadas, la asesoría técnica, así como su sostenibilidad y evolución.

En el orden práctico, tenemos que aprovechar algunas aplicaciones que ya se utilizan en varias entidades y promover su uso. Hay que concretar el proceso de formación o capacitación del personal sobre el desarrollo, implantación, administración, despliegue del

soporte técnico y utilización del sistema operativo NOVA, el paquete ofimático OpenOffice, navegador Firefox y cliente de correo Thunderbird, o sus similares, entre otros.

Aprovecho para informar que esta migración se realizará de forma ordenada y progresiva y donde sea imprescindible; coexistirá con los sistemas propietarios, siempre que satisfagan los requerimientos de seguridad y las necesidades de informatización de cada entidad.

En este proceso es importante tener en cuenta las experiencias de la Aduana General de la República, para evitar o minimizar los inconvenientes y las dificultades por las que ya pasó. ¿Cuáles son los aspectos más importantes de la migración en esta institución que como usted refirió duró unos once años?

La Aduana desde el año 1999 inició la migración hacia sistemas operativos, ofimáticos y herramientas de desarrollo sobre plataformas de código abierto. En la actualidad, ciento por ciento de las estaciones de trabajo utilizan el sistema operativo Ubuntu, lo que garantiza disponer de una seguridad relativamente alta e independencia tecnológica. Comenzaron con Ubuntu versión 6 y ya van por la 16.

Ahora tendremos la ventaja que habrá normas jurídicas que respalden el programa, a diferencia del año 1999. Y estoy seguro que algunas, cuando pase un tiempo, habrá que readecuarlas a la situación de ese momento.

Los directivos y especialistas de la Aduana consideran que un factor vital fue la participación de la máxima dirección de este organismo, en particular, del general de Brigada Pedro Ramón Pupo Pérez, que condujo con acierto desde el principio esta compleja transformación cultural y tecnológica. La capacitación sistemática del personal fue un elemento esencial para asimilar los cambios. También organizaron una migración para servidores por servicios; y en las máquinas de escritorios utilizaron variantes libres, en dependencia de sus condiciones técnicas. Para transitar de Windows a Linux utilizaron la tecnología de virtualización.

En estos momentos trabajan en el fortalecimiento de la infraestructura tecnológica para mantener la vitalidad de los sistemas y lograr su

integración, de tal modo que se garantice el necesario equilibrio entre la facilitación de los servicios que ofrecen y la seguridad.

Se debe significar que existen otras entidades que han avanzado en el proceso con la ayuda de las universidades. La mayoría de los Organismos de la Administración Central del Estado (OACE), utilizan *software* libres en los sistemas operativos para la gestión de la red.

Desde el año 2005, la Aduana tiene una alianza estratégica con la Universidad de las Ciencias Informáticas (UCI), que ha permitido el desarrollo en código abierto de varios proyectos como el Sistema de Gestión Integral de Aduanas, que se vincula mediante intercambio electrónico de datos con operadores de comercio exterior, navieras, aerolíneas, operadores de puertos y aeropuertos, almacenes y autoridades en frontera; Ventanilla Única de Aduana, que posibilita a los usuarios externos que intervienen en el comercio exterior, realizar los trámites ante la Aduana y a la vez, recibir respuesta; pasarela para el intercambio de información Aduana-Inmigración; información adelantada de pasajeros, tripulantes y cargas, en correspondencia con los estándares internacionales y aplicaciones para móviles, para diferentes servicios aduanales.

Con la empresa Segurmática S.A. tienen contratados varios servicios como la licencia para los *software* antivirus Kaspersky para PC, servidores y la infraestructura de virtualización, y el Segurmática Antivirus versión para móviles; el de consultoría a sitios web y el de gestión de vulnerabilidades.

Habría que agregar la implementación de un grupo de medidas técnicas y organizativas que impactan en la seguridad y que, junto a lo anterior, permite minimizar los riesgos para la ocurrencia de incidentes de ciberseguridad.

Formación y preparación de especialistas en ciberseguridad

Una de las claves para resolver los problemas de seguridad cibernética está en la formación y preparación de especialistas en este campo. Un estudio sobre fuerza de trabajo en ciberseguridad, dado a conocer a finales de 2018 por el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2), reflejó que la falta de especialistas en esta materia era de casi 3 MM de profesionales en el mundo. ¿Qué resultados arrojó el estudio?

Para mantener la seguridad del ciberespacio, el factor más crítico está en las personas y en la capacidad para formar talentos de alto nivel y calidad. El estudio a que te refieres reflejó que en el mundo existen 2.93 MM de vacantes en puestos de ciberseguridad, aproximadamente 2.14 MM de profesionales en la región Asia-Pacífico, en parte, debido al crecimiento de estas economías y a las legislaciones de privacidad de datos y ciberseguridad que se vienen adoptando.

América del Norte es la segunda región en déficit de profesionales, llegando a 498 mil; y América Latina presenta una carencia de 136 mil especialistas.

También destaca que 48 % de los entrevistados afirmó que sus organizaciones planean aumentar el equipo de ciberseguridad en los próximos 12 meses, y que las áreas en que los profesionales de este sector sienten que necesitarán un mayor desarrollo o perfeccionamiento en los próximos años son: seguridad en la nube, prueba de penetración, análisis de inteligencia de amenazas e investigación forense.

En el caso de China, uno de los países con mayor crecimiento de la industria informática y de los internautas, ¿qué comportamiento ha tenido este asunto?

En el gigante asiático, la economía digital representó 34.8 % del PIB del país en 2018. Mientras que este sector creció 20 %, el PIB aumentó entre 6-7 %.

En los últimos años, la industria de seguridad de la información de China ha crecido de manera considerable. En 2017, los ingresos registrados fueron de 41 500 MM de yuanes, un aumento de 22 % en relación con 2016.

En la actualidad existen 800 MM de internautas; en 2006 había 70 MM. Se estima que hoy China genera un cuarto de los datos del mundo, y hay que destacar que una tercera parte de los delitos que ocurren en ese país son ciberdelitos.

En este contexto, no cuentan con suficiente personal calificado en temas de ciberseguridad y se considera que el déficit es de 700 mil especialistas.

Potencian el concepto de que la base de la seguridad cibernética son los recursos humanos bien preparados. En tal sentido, trabajan en dos líneas fundamentales: educación universitaria y capacitación de habilidades a corto plazo.

Existen 29 universidades que tienen carreras vinculadas con la ciberseguridad y esta materia figura en el contenido educativo de todos los niveles de enseñanza.

¿Cuál es el escenario cubano en este ámbito?

Tenemos en varios sectores estratégicos especialistas muy bien preparados en seguridad cibernética; pero nos sucede, como a la mayoría de los países, que nos faltan profesionales en esta materia.

Sin embargo, no estamos cruzados de brazos. En la Universidad de las Ciencias Informáticas (UCI) se estudia el Técnico de nivel superior en Seguridad Informática. En el curso 2020-2021 comenzó la carrera de Ingeniería en Ciberseguridad; además, tenemos como curso de posgrado una especialidad en ciberseguridad en varias instituciones cubanas.

Por supuesto, tenemos que aplicar otras medidas, como diseñar un programa para trabajar con los talentos del sector e introducir la asignatura de Seguridad Informática en los diferentes niveles de enseñanza de la educación, como parte de las medidas aprobadas por el Consejo de Ministros, para fortalecer la ciberseguridad.

En los próximos años crecerá la demanda de puestos de seguridad informática y se precisa construir un sistema de educación y capacitación de talentos que dé respuesta al desarrollo de nuestro país en el uso de las TIC y el acceso a internet.

Normas jurídicas relacionadas con la ciberseguridad en Cuba

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) en Cuba y la defensa del ciberespacio nacional, precisan de una actualización y adecuación a los tiempos actuales de las normas jurídicas relacionadas con estos asuntos vitales.

El Decreto No. 360/2019 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, forma parte del paquete de normas jurídicas que acompaña el programa de informatización de la sociedad cubana y la defensa del ciberespacio nacional. ¿Por qué ha sido importante su aprobación?

Resulta necesario aprobar normas jurídicas que respalden los avances y proyecciones del programa de informatización del país, la investigación, el desarrollo, la asimilación tecnológica de forma sostenible y, por supuesto, la soberanía de la nación.

Pero, paralelo con su aplicación, es necesario crear en la sociedad una cultura de ciberseguridad, fortalecer la disciplina en todos los que utilizan estas tecnologías y elevar la percepción de los riesgos que generan, si no la empleamos correctamente.

¿Cuáles son los objetivos de este decreto y con quién está relacionado el término Seguridad de las TIC?

Lo primero que quisiéramos apuntar es que el decreto es de aplicación a los órganos y organismos del Estado y el gobierno, las organizaciones empresariales y demás entidades estatales, incluidas las fuerzas especializadas en seguridad informática, el sector no estatal y las personas naturales.

El objetivo general es elevar los niveles de seguridad, en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de gestionarlos.

Además, tiene los objetivos específicos siguientes:

1 . Proteger el ciberespacio nacional y preservar la soberanía sobre su utilización.

2 . Establecer la seguridad de las TIC y los servicios y aplicaciones que soportan.

3 . Establecer la seguridad de las infraestructuras críticas de las TIC, con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.

Es importante referir que el término Seguridad de las TIC está relacionado con la confidencialidad[27], la integridad[28] y la disponibilidad[29] de la información que se genera, procesa y almacena por los terminales y se transmite por las redes de datos.

¿Qué premisas de la seguridad de las TIC se tienen en cuenta para la informatización de la sociedad y la defensa del ciberespacio nacional?

Resulta necesario comprender que en las condiciones actuales es imprescindible elevar la soberanía tecnológica en beneficio de la sociedad, la economía, la seguridad y la defensa nacional; contrarrestar las agresiones cibernéticas; salvaguardar los principios de seguridad de nuestras redes y servicios; así como defender los logros alcanzados por el Estado Socialista.

Nuestro país en diferentes foros internacionales ha manifestado su posición a favor del uso pacífico y legítimo de las TIC, así como de las múltiples oportunidades que ofrece el ciberespacio para el desarrollo social y económico de las naciones subdesarrolladas.

[27] La confidencialidad implica que solo quienes estén autorizados puedan acceder a la información y con ello, se minimice la posibilidad de que sea empleada por nuestros enemigos para sus agresiones.

[28] Garantizar la integridad significa que la información no sea alterada o destruida y por tanto, mantenga el valor de uso para el que se le destina.

[29] La disponibilidad de la información implica tanto su búsqueda y obtención, como su diseminación, de forma tal que todo usuario autorizado que la necesite pueda acceder a ella de manera oportuna.

Este decreto pretende actualizar las normas jurídicas sobre esta temática y contribuye a dar una respuesta efectiva a los vacíos legales que existen sobre la ciberseguridad, de tal manera que facilite el funcionamiento estable y seguro de los servicios que brindamos sobre internet.

Entonces, constituyen premisas de la seguridad de las TIC para la informatización de la sociedad y la defensa del ciberespacio nacional, las siguientes (Fig. 6):

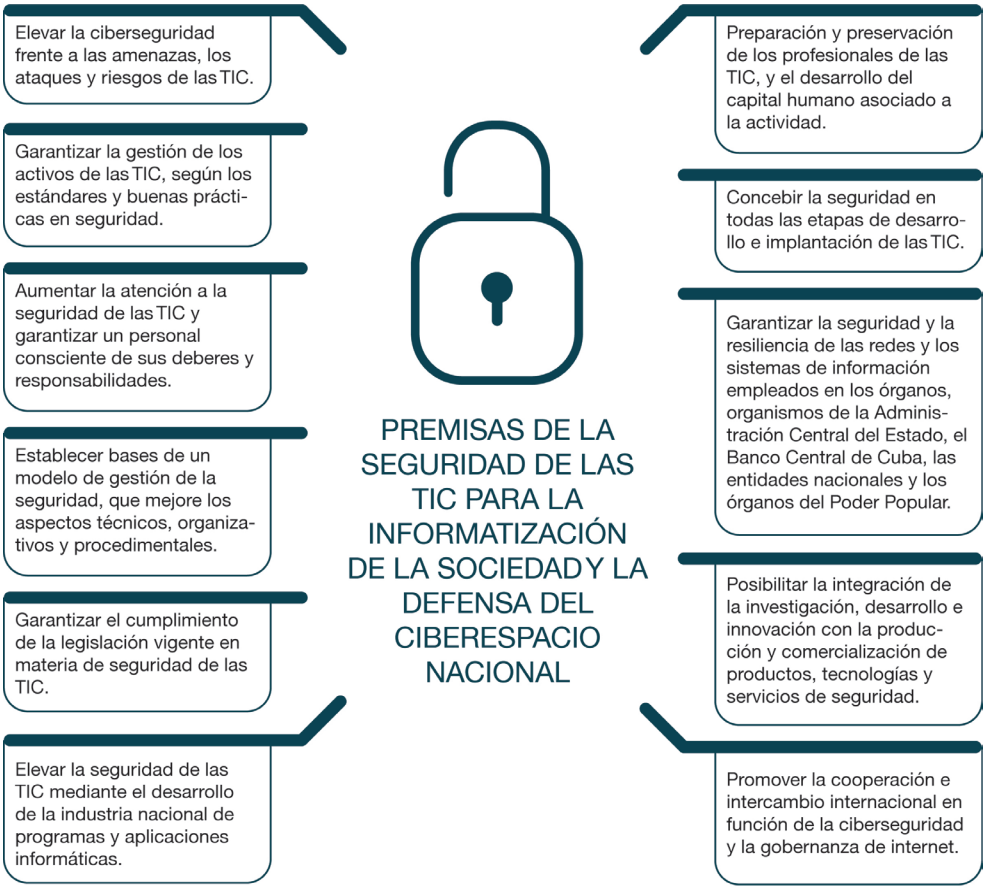


Fig. 6. Premisas de la seguridad de las TIC.

¿Quiénes integran el Sistema de Seguridad de las TIC en Cuba?

El Sistema de Seguridad de las TIC[30] se constituye a partir de las estructuras, procedimientos y otros componentes de seguridad existentes en las instituciones del país que posean o utilicen las TIC, e incluye (Fig. 7):

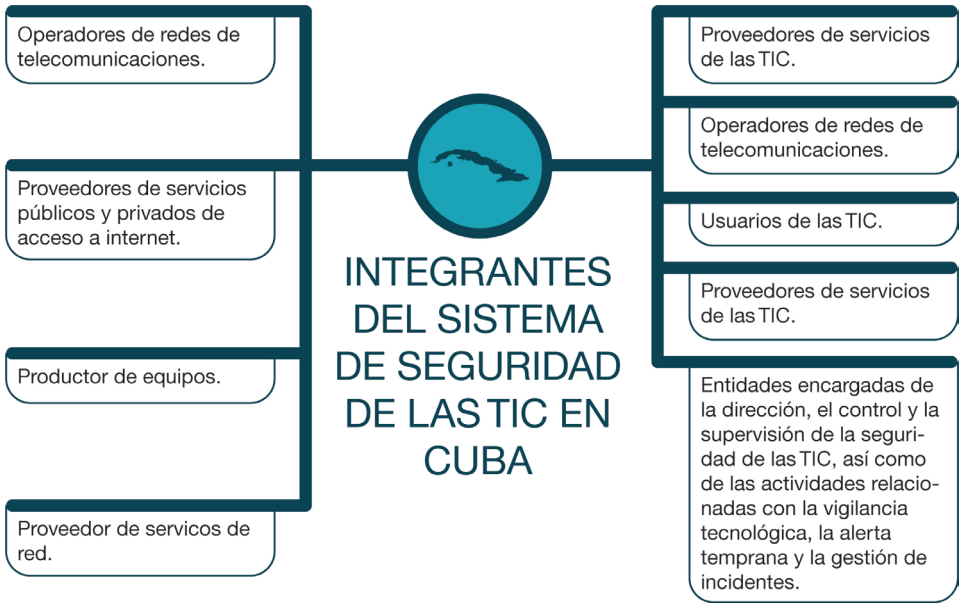


Fig. 7. Sistema de seguridad de las TIC.

En este sentido, cada entidad que haga uso de las TIC debe diseñar, implantar, gestionar y mantener actualizado un sistema de seguridad en correspondencia con los elementos a proteger y los riesgos a los que estos se exponen. Además, debe elaborar su plan de seguridad de las TIC, tomando como base la metodología establecida por el Ministerio de Comunicaciones en la Resolución No. 129/2019, como parte de las normas jurídicas que se han puesto en vigor.

[30] Es el conjunto de medios humanos, técnicos y administrativos que, de manera interrelacionada, garantiza diferentes grados de seguridad informática, en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

Segurmática, una empresa cubana de ciberseguridad

En la actualidad, el desarrollo de malware o software malicioso es una industria muy productiva en la que los ciberdelincuentes aprovechan las vulnerabilidades y debilidades en la configuración de los sistemas, así como la ingeniería social para lograr sus objetivos.

La industria de productos de seguridad ha tenido que adaptarse a estos cambios para buscar más efectividad y proactividad. Se caracteriza por grandes inversiones en investigación en aprendizaje automático e inteligencia artificial, capital humano, infraestructura de sensores y sistemas de inteligencia de amenazas.

Una noticia publicada en el sitio de Segurmática, el 1.º de noviembre de 2019, da cuenta de ataques por phishing, dirigidos a equipos de las Naciones Unidas, Cruz Roja, UNICEF, Programa Mundial de Alimentos y diversas organizaciones de ayuda humanitaria. También sobre las afectaciones ocasionadas por el virus Dtrack que puede hackear cualquier cosa, desde cajeros automáticos hasta plantas nucleares.

Lo cierto es que para que los atacantes tomen el control sobre las redes internas de la organización objetivo, es necesario que existan debilidades de seguridad como pobre manejo de contraseñas, falta de monitoreo del tráfico, uso de soluciones antivirus inadecuadas, entre otras fallas.

En este contexto, la empresa cubana Segurmática, constituida en febrero de 1995 y única de su tipo en Cuba, desarrolla productos y soluciones de seguridad informática avanzados, así como, brinda servicios y consultoría especializada a entidades nacionales y extranjeras, para contribuir a fortalecer la ciberseguridad del país.

¿Cuáles son los principales servicios que ofrece Segurmática?

En febrero de 2020 Segurmática cumplió 25 años, y hay que decir que su cartera de servicios ha crecido de manera sostenida. Recuerdo que la primera versión de Segurmática Antivirus (SAV32) salió en 2006 y la que tenemos hoy ha evolucionado mucho en calidad y

alcance, sin dejar de reconocer sus limitaciones y los aspectos que hay que seguir desarrollando y mejorando.

Con 60 trabajadores como promedio, de ellos 75 % dedicados a las actividades técnicas, comerciales y al desarrollo, alcanzan una productividad de más de 76 000 pesos por trabajador.

Aunque se le conoce en lo fundamental por sus programas antivirus, los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos, alertas de antivirus informáticos, escaneo de puertos, consultoría remota a sitios web, red interna y de cara a internet, actualización de parches, gestión de incidentes, recuperación de información borrada, elaboración y revisión de planes de seguridad informática, configuración segura de servicios de red, soporte técnico, adiestramientos, custodia de material informático y dictamen de sistemas contables y financieros.

También utiliza como distribuidores de sus productos a los Joven Club, Desoft, Eicma, Sitrans, Info y Aicros. Es socio comercial de Kaspersky Lab.

¿Qué dictaminan en el caso de los sistemas contables y financieros?

Hay todo un proceso para ir sustituyendo los sistemas contables financieros importados por nacionales; pero en cualquier variante, la seguridad de los que tenemos en funcionamiento en nuestras empresas, unidades presupuestadas y demás instituciones, es vital y necesaria la certificación de los que se utilizan en el país.

Por eso es importante el servicio que brinda pues, entre otras cuestiones, verifica si cuentan con claves de acceso robustas (8 caracteres como mínimo) y requisitos de complejidad; la transmisión de las claves en texto claro en el proceso de autenticación; el acceso a las opciones del sistema en correspondencia con los perfiles de usuario; los mecanismos de seguridad que evitan la modificación, destrucción y pérdida de los ficheros y datos, y el acceso a los mismos que esté compartimentado y controlado.

Asimismo, el diseño sobre bases de datos robustas y los mecanismos de salva; mecanismos de alerta si se intenta modificar su códi-

go ejecutable; utilización de mecanismos de cifrado para proteger la información primaria que gestiona; el cambio periódico de la contraseña; el bloqueo de la cuenta de usuario tras varios intentos fallidos de conexión; las opciones de salva y restaura, restringidas solo al usuario administrador del sistema; el registro de las acciones realizadas por los usuarios, por al menos un año y si tiene implementados mecanismos de seguridad orientados a impedir la exportación de datos susceptibles de ser modificados sin emplear las funcionalidades del sistema.

Como se aprecia, es riguroso el dictamen, hay aspectos que son invalidantes para obtener un resultado positivo y se realiza a partir de una lista de chequeo.

Muy pocos países cuentan con un antivirus nacional. ¿Qué situación tiene hoy el Segurmática Antivirus?

Aunque tenemos muchas insatisfacciones aún, nuestro antivirus continúa ganando usuarios en el panorama nacional y se trabaja por incrementar las computadoras protegidas tanto en las personas jurídicas como en las naturales.

Al cierre de 2018 protegió el 12.1 % del total de computadoras del país, 156 591 máquinas de personas jurídicas y 15 325 en las naturales; al cierre de 2019 fue 13 %.

En el caso de los equipos móviles protegidos con Segurmática Seguridad Móvil se inmunizó al cierre de 2018 apenas 2 % del total de los usuarios del servicio de datos móviles. Al concluir 2019 fue de 2.3 %. Como observamos, es mucho el trabajo a realizar en esta actividad.

Por otro lado, se trabaja en el reconocimiento del *malware* a través de inteligencia artificial, en sistemas de telemetría para Android, que servirán de base para el antivirus en la nube; se incrementa el número de cadenas de identificación de programas malignos; se ha mantenido la generación de cuatro actualizaciones diarias, incluyendo además la identificación heurística y genérica; se han establecido alianzas con las universidades; y se creó una unidad docente en la Universidad de Ciencias Informáticas (UCI).

¿Cuál es el sistema para recolectar las muestras de virus?

Son diversas las vías. Como dijera Niurka Edith Milanés Sarduy, directora general de la Empresa de Consultoría y Seguridad Informática, Segurmática, en entrevista concedida al Canal USB del sitio *Cubadebate*, el 3 de septiembre de 2019:

> No podemos acceder a sitios donde hay muestras frescas debido al bloqueo. Un ejemplo de ello es Virus Total, pues el .cu está bloqueado para descargas en ese repositorio, al ser de Google, y esto dificulta la obtención de muestras diarias de *malware*. No obstante, tenemos un sistema de vigilancia tecnológica que busca constantemente dónde se publican las muestras de *malware* que más afectan a nivel internacional. Si pueden afectar a las redes nacionales, las muestras son introducidas rápidamente en la próxima actualización.
>
> Por otra parte, contamos con otras opciones como la OSRI, cuando le notifican alguna incidencia de programa maligno; también los propios usuarios reportan a través de nuestro correo virus@segurmática.cu, cuando tienen otro antivirus instalado en su PC.
>
> Ningún antivirus es ciento por ciento seguro. Siempre hay algún programa maligno que se escapa. Y los atacantes cada día van usando mecanismos más sofisticados. Al cierre de julio de 2018, recibimos por esa cuenta 301 reportes y en 2019 tuvimos 567 al cierre de igual período, lo que te dice que hemos crecido. De esos reportes, 50 % lo resolvimos antes de siete días, muchos de manera inmediata. En dependencia de la complejidad, puede demorar un poco más.
>
> A pesar de las limitaciones, tenemos una base de datos de programas malignos de más de cuatro teras, gracias al acceso desde Cuba a determinadas muestras internacionales.

¿Qué se está proyectando desde el punto de vista de desarrollo tecnológico?

Teniendo en cuenta que fortalecer la ciberseguridad es una prioridad, en los próximos años debemos incrementar los servicios orientados a brindar soluciones integrales de seguridad de las TIC y proteger de manera efectiva el ciberespacio nacional.

En esta estrategia, Segurmática juega un papel muy importante por ser una de las contadas empresas de seguridad informática que tenemos hoy. Por tanto, se están ejecutando acciones para la cap-

tación y retención de especialistas, intensificar la colaboración con universidades y centros de investigación para los proyectos de I+D+i, concretar inversiones en la infraestructura de red y desarrollo, y dar solución a la certificación de *drivers*.

Específicamente, en lo referido a los productos, se trabaja a corto y mediano plazos en el Segurmática Antivirus para Windows, versión 2.0; Segurmática Seguridad Móvil, versión 2.0 con funcionalidad de *firewall*; Seguridad Antivirus para Linux, versión 1.0 con interfaz gráfica; desarrollo de la protección de URL del motor Antivirus; desarrollo de driver MTP para el control de dispositivos; prevención de fuga de datos (DLP); desarrollo de defensa proactiva y *antirransomware* (*driver* y servicio) para el motor Antivirus e incorporar motor de Android identificación de *malware* por inteligencia artificial, entre otras acciones.

Todas permitirán la creación de una *suite* de seguridad para protección de red y navegación, que permitirá una mayor integración de los productos y servicios de Segurmática.

Por último, debemos referir que existe una proyección para potenciar el comercio electrónico en la empresa con la venta en línea a través de la tienda Superfácil de Citmatel y en las plataformas EnZona y Apklis, incluir las renovaciones como una opción en Transfermóvil e incorporar dentro de los productos la opción de comprar licencias.

GUERRA CIBERNÉTICA EN INTERNET Y LAS REDES SOCIALES DIGITALES

CID 201, un ejemplo de soberanía tecnológica en Cuba

En estos días que tanto se ha hablado de los aportes de la ciencia cubana al enfrentamiento a la Covid-19, y lo que representa en la soberanía tecnológica, es justo recordar un hecho que, en nuestra opinión, fue el punto de partida del uso de la informática en función del desarrollo y la soberanía tecnológica del país.

El 18 de abril de 1970, de la mano de Fidel Castro, se puso en funcionamiento la primera computadora digital cubana, denominada CID 201, todo un acontecimiento para un pequeño país, que ya recibía los primeros embates del bloqueo económico, comercial y tecnológico más largo e inhumano de la historia.

¿En qué contexto para la ciencia cubana surge la idea de construir una computadora cubana?

Hay que decir que los primeros intentos para introducir la computación en Cuba fueron en las universidades, en momentos en que no había suficiente información ni medios sobre esta tecnología. Ya en los países desarrollados se estaba empleando la computación como un medio de formación y como un instrumento para la economía.

En la década del sesenta comenzaron a crearse los centros de investigación vinculados con las universidades. Entonces, entre las investigaciones que se hicieron a través de las universidades estaban los proyectos para desarrollar la computación y construir computadoras. En realidad, ya en esa época cada vez era mayor la conciencia entre los profesores y los intelectuales sobre la necesidad de producir estos medios, de generar conocimientos y potenciar su empleo.

Por aquellos años, los Estados Unidos tenían un monopolio casi absoluto de la informática, y nuestros aliados socialistas no tenían mucho desarrollo en el campo de la computación.

Ya en esta etapa, el Gobierno de los Estados Unidos había impuesto un feroz bloqueo al país, que se declaró en febrero de 1962, lo que dificultó o casi imposibilitó el acceso a esta tecnología. Basta decir que la adquisición de medios de cómputo resultó en extremo difícil, pues siguieron paso a paso las gestiones de Cuba para adquirir estos equipos, tratando de evitar con ello el desarrollo de la informática en nuestro país.

En el período de 1959 hasta 1968, solo fue posible comprar un equipo, Elliot 803B, con fines de investigación científica, que adquirimos sin los periféricos fundamentales. Esta era una máquina de segunda generación, con limitaciones en su capacidad de procesamiento de datos y en sus posibilidades de explotación, debido a las mismas circunstancias ya apuntadas.

Debo mencionar que el 26 de julio de 1968 se puso en explotación la primera computadora analógica cubana, nombrada SILNA999, construida en la Universidad Central Martha Abreu de Las Villas con piezas reutilizadas, para la enseñanza y aprendizaje. Participaron varios profesores de este centro docente, dirigidos por Felipe Ramón Argüelles y Héctor Onofre Salvador Gallardo. Se ponía de manifiesto el interés por dotar a nuestros futuros hombres de ciencia, de esta importante tecnología.

¿Y cuándo se puso en funcionamiento la primera computadora digital cubana?

El 18 de abril de 1970 se terminó la primera computadora digital, la CID-201, de tercera generación, que marcó el inicio de una serie de desarrollos de medios técnicos de computación. Al mismo tiempo que se realizaba la tarea de diseño y ejecución fue programado el *software* correspondiente.

Se creó un pequeño colectivo, fundamentalmente a partir de alumnos y profesores de la hoy Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE), encabezado por el ingeniero Luis Carrasco, y con la decisiva participación del ingeniero Orlando Ramos

(Fig. 8), quienes luego fundarían el Centro de Investigaciones Digitales (CID), adscripto a la Universidad de La Habana, que trabajarían en ese proyecto.

Fig. 8. Luis Carrasco y Orlando Ramos. Foto tomada del libro *Estrellas en la frente* del autor.

Fue elaborado un estudio para determinar en qué actividades se podía utilizar el equipo; se hizo el modelo matemático y después se diseñó la computadora adecuada. Se partió del criterio de utilizar los elementos y los medios que se correspondieran con el más alto nivel de la técnica del momento, es decir, circuitos integrados.

Si hablamos de soberanía, creo que el principal aporte estuvo en el *know how*, en el cómo hacerlo. Se concibió un álgebra que simplificó el análisis y el diseño; se desarrolló un *software* al que nombraron LEAL (Lenguaje Algorítmico), creado por dos matemáticos de la Universidad de La Habana y un programa de aplicación para jugar ajedrez.

El colectivo diseñó, adquirió los componentes —en Europa y Japón—, fabricó y puso en marcha la computadora en menos de un

año. Se logró gracias a un esfuerzo extraordinario en ese período, en que se trabajaba casi las veinticuatro horas del día. Un papel decisivo en la motivación del colectivo fue la presencia muy frecuente de Fidel, su atención personal, su aliento y apoyo constante, y de José Millar Barruecos, entonces rector de la Universidad de La Habana.

Ese 18 de abril, el Comandante jugó ajedrez con la máquina por más de una hora, hasta que al final le dio jaque mate.

La primera CID 201 fue instalada en el central Camilo Cienfuegos, con el objetivo de controlar el tráfico ferroviario durante la zafra azucarera; después se fabricó la CID 201A, similar desde el punto de vista electrónico a su antecesora, que permitió iniciar el uso masivo de la computación en el país. (Fig. 9).

Fig. 9. Primera computadora digital CID 201.

¿Qué otros desarrollos se alcanzaron a partir de la primera computadora digital cubana?

La efectividad del primer modelo de computadora permitió aumentar la escala de producción, comenzando por una cifra de cinco. Estas incluían algunas mejoras con respecto a la CID-201 y fueron denominadas CID-201-A, que se utilizaron en otras ramas de la economía, entre ellas, la industria azucarera, la textil, el cálculo científico, la gestión económica y los deportes.

Posteriormente, se desarrollaron la CID 202 con fines investigativos, la CID-201-B, las minicomputadoras CID-300-10 y la CID-300/20, equivalentes a miembros de la serie PDP-11 de la Digital Equipment Corporation (DEC).

En la línea de videoterminales fueron desarrolladas la CID-701, CID-702, CID 7205, CID 7221 y la CID 7300 con un régimen gráfico.

Después se desarrolló la videoterminal gráfica VT- 7060, todas análogas a las videoterminales de la firma DEC. En 1984 se desarrolló la primera microcomputadora cubana CID 1408 de 8 bits y la CID-1417 de 16 bits, totalmente compatibles a la IBM-PC.

A mediados de los ochenta se dejó de fabricar computadoras, pues al Gobierno de los Estados Unidos le era más fácil bloquear la compra de microprocesadores que la de microcomputadoras, de las que había muchos fabricantes, mientras los microprocesadores solo eran fabricados por INTEL y dos o tres compañías más. Al cerrarse la línea de desarrollo de minicomputadoras, se reforzaron las de equipos médicos, automatización, videoterminales y teclados.

Se diseñaron y fabricaron equipos médicos de la más alta tecnología como los electrocardiógrafos CARDIOCID-BS y CARDIOCID-BB, el monitor DOCTUS VI, el oxímetro de pulso OXY-9800 y el ERGOCID, para pruebas de esfuerzos.

Por eso, detrás de los resultados científicos que se muestran hoy en el enfrentamiento a la pandemia que azota al mundo entero y en el uso de la bioinformática, están aquellas investigaciones, propiciadas por Fidel, que generaron la primera computadora digital cubana hace 50 años.

Algunos antecedentes de guerra cibernética

Varios ejemplos demuestran que Cuba ha estado expuesta en los últimos años a las diferentes modalidades de la guerra cibernética, entendida como los conflictos en que adquiere un rol determinante la informática y las comunicaciones. ¿Puedes mencionar algunos?

En la década de los noventa del siglo pasado se produjo un gran número de estudios por institutos de investigación y "tanques pensantes" de los Estados Unidos, sobre la viabilidad de llevar las Tecnologías de la Información y la Comunicación (TIC) al campo de batalla; sin embargo, con el advenimiento de la administración de George W. Bush y los acontecimientos del 11 de septiembre de 2001, estas concepciones recibieron un gran impulso al declarar el entonces secretario de Defensa, Donald Rumsfeld, que "internet sería el nuevo escenario de la guerra contra el terror". Hay que destacar que para el país del norte, organizaciones terroristas y países que patrocinan el terrorismo, son aquellos que no se someten a sus designios.

En la actividad ideológica es donde más acciones subversivas e injerencistas se han organizado y ejecutado contra Cuba. Muchas personas no conocen que dos días antes del ataque terrorista a las torres gemelas en New York, el 9 de septiembre de 2001, Cuba se convertía en el primer Estado acusado de planear ataques cibernéticos contra los Estados Unidos, cuando en la audiencia del Comité selecto del Senado sobre Inteligencia, que trató el tema de "la amenaza mundial", el entonces director de la Agencia de Inteligencia de Defensa, almirante Thomas R. Wilson, identificó a la Mayor de las Antillas como un posible país "ciberatacante".

En febrero de 2006, el Departamento de Estado, encabezado por Condolezza Rice, crea el Grupo de Trabajo para la Libertad Global de la Red, que debía concentrarse en monitorear en especial a China, Irán y Cuba; y en julio del siguiente año se hace pública la decisión del presidente Bush, de crear un cuarto ejército en el país, el del ciberespacio, que estaría radicado en la base de la fuerza Aérea de Barksdale en Louisiana, con la misión de mantener la ventaja competitiva de las fuerzas armadas estadounidenses en un nuevo teatro de las operaciones militares.

La Administración Obama crea la figura del Ciberzar, para lo cual designó a un funcionario del gobierno de W. Bush, Howard Schmidt, con amplia experiencia en el campo de la seguridad y las TIC, tanto en el sector privado como en las agencias de inteligencia. Las funciones de este cargo están relacionadas con la coordinación de los esfuerzos gubernamentales para mejorar la ciberseguridad nacional en el ámbito militar y civil.

También resulta significativo que el 18 de abril de 2013, a solo cuatro días de las elecciones en Venezuela, varios sitios cubanos en internet, entre ellos, el portal Cubasí, recibieron un ataque de denegación de servicio que los afectó por varias horas.

Algunas redes cubanas se han utilizado desde el exterior para lanzar ataques cibernéticos a redes fuera de Cuba, aprovechando las vulnerabilidades que presentan, cuestión que en su momento se notificó a los países desde donde se originó el ataque, en correspondencia con los mecanismos existentes a nivel internacional.

Es conocido que el 19 de abril de 2010 se efectuó una conferencia sobre ciberdisidencia, organizada por la Fundación George W. Bush en el Southern Medhodist de la Universidad de Dallas, en Texas. ¿Qué se discutió allí?

La conferencia sobre ciberdisidencia inauguró el "Área de Enfoque sobre la Libertad Humana" del Instituto George W. Bush. El copatrocinador del evento fue Freedom House, una organización ampliamente beneficiada con el presupuesto del Gobierno de los Estados Unidos para la subversión en Cuba y vinculada a escándalos de uso indebido de esos fondos.

Según los documentos del Bush Institute, la conferencia tuvo como propósito utilizar las herramientas de internet y de la tecnología inalámbrica para los "disidentes" afines a Washington, en cuatro continentes. Evaluaron cómo contrarrestar el uso de esas mismas herramientas por los "enemigos de la libertad" en los países donde trabajan sus invitados: Cuba, Venezuela, Irán, Sudán, China y otros, e idearon un plan de acción para cumplir esos propósitos.

Creo que se impone que menciones las características de algunos proyectos subversivos que han empleado las TIC para cumplir sus propósitos como Commotion, ZunZuneo, Piramideo, entre otros.

En 2008, la CIA puso en práctica la operación Surf. Desenmascarada por Dalexi González Madruga, el agente Raúl de la Seguridad del Estado, esta operación consistía en la entrada de equipamientos y *software* para la instalación de antenas ilícitas para el acceso ilegal a internet.

En ella intervino Robert Guerra, propietario de la empresa Privaterra, en realidad un agente de los servicios especiales de los Estados Unidos para la guerra cibernética, quien contactó a Dalexi para la creación de redes ilegales de infocomunicaciones en nuestro país.

Le entregó en CD, *plugs*, navegadores y otros medios de lo más avanzado en *software*; le enseñó a entrar a sitios de la web sin acceso desde las conexiones nacionales, haciéndolo desde un servidor en el exterior y la forma de encriptar mensajes a través de aplicaciones capaces de emitir textos que en las ondas cibernéticas se transmitieran como algo similar al ruido.

Robert Guerra era el jefe del plan de agresión cibernética de la Freedom House, la misma organización CIA que desde hace varias décadas encubre operaciones de inteligencia contra Cuba, con financiamiento de la USAID y por medio de la NED. Este era un plan creado por el Centro para una Cuba Libre (Center for a Free Cuba), del agente CIA Frank Calzón.

Guerra habló como experto de la Freedom House en el evento convocado por esa organización junto con el Instituto George W. Bush, el 19 de abril de 2010, reunidos por un tema sugerente: el Movimiento Global de Ciberdisidentes, un producto propagandístico concebido y manejado por la CIA.

Commotion fue una herramienta desarrollada en 2011 por el Instituto de Tecnología Abierta (OTI) de la New America Foundation, un tanque pensante con sede en Washington DC, originalmente para uso militar, que consistió en la creación de redes inalámbricas independientes en forma de "malla" para enlazarse con el exterior, fuera de cualquier control gubernamental, lo cual permitía desinformar a los usuarios sobre la situación en su país y convocarlos a manifestaciones.

El Departamento de Estado estadounidense proporcionó 2.8 millones de dólares a un equipo de *hackers* y activistas comunitarios, y conocedores de programación, para desarrollar un sistema de redes que permitiera a personas afines a los intereses de Washington en diferentes partes del mundo, comunicarse sin interferencias de sus gobiernos por internet.

La red fue probada en la ciudad de Sayada, en Túnez, a través de académicos y expertos informáticos tunecinos que participaron en el levantamiento de 2011, que derrocó al presidente Zine al-Abidin Ben Ali.

Aunque en los planes de Washington estaba su aplicación en Cuba, no se conoce su entrada en funcionamiento en nuestro país.

El proyecto ZunZuneo, red social creada de manera secreta por agencias del Gobierno de los Estados Unidos para promover el "cambio de régimen" en nuestro país, y donde presumiblemente se realizaron acciones de ciberespionaje para robar la base de datos de la telefonía celular de Cuba, fue financiado por la USAID. Su objetivo era lanzar una red de mensajería que pudiera llegar a cientos de miles de cubanos usando "contenido no controversial": noticias de fútbol, música, parte del clima y publicidad. Cuando lograran su meta, enviarían mensajes de contenido político para incitar a los cubanos a crear convocatorias en red y concentraciones masivas para desestabilizar el país.

ZunZuneo, también conocido como el "*Twitter* cubano" bajo la apariencia de una red social inocente, encubrió una operación secreta financiada y dirigida por la USAID, que empleó empresas de fachada constituidas en secreto y financiadas desde bancos extranjeros a través de las nuevas tecnologías (vía teléfonos celulares y redes sociales), cuyo propósito era crear situaciones de desestabilización para provocar cambios en el ordenamiento político cubano.

En 2012, el proyecto captó más de 40 000 cubanos como suscriptores para compartir noticias e intercambiar opiniones. Esos suscriptores nunca supieron que el servicio fue creado por el Gobierno de los Estados Unidos, ni que había contratistas que recopilaban información privada de los usuarios con propósitos políticos.

Por último, Piramideo, similar a ZunZuneo, estaba a cargo de la Oficina de Transmisiones a Cuba (OCB), a la que se supeditan *Radio y TV Martí*. El mismo promovía la creación de una red de "amigos", ofreciéndoles la posibilidad de que una persona enviara a los miembros de su "pirámide" un sms masivo por el valor de un solo mensaje. El objetivo último era contar con una plataforma para la subversión y crear una especie de "canal de comunicación" entre los grupúsculos contrarrevolucionarios.

Manipulación en el tema internet en Cuba

¿Quién se ha enriquecido verdaderamente con el tema internet en Cuba?

Los avances del programa de informatización de la sociedad cubana en los últimos años y del acceso de los cubanos a internet tienen sin dormir a los centros de estudio e investigación, los servicios especiales y los medios de comunicación al servicio del imperialismo estadounidense. No se puede apreciar de otra manera cuando se lee el artículo, "El Gobierno cubano pasó de negarle internet a sus ciudadanos a enriquecerse con él", publicado por *The Washington Post*, el mayor y más antiguo periódico de Washington DC, la capital de los Estados Unidos.

Tras una atenta lectura, no es difícil la conclusión de que lo descrito denota una total desinformación y manipulación del autor acerca del acceso a internet en Cuba y una perversa mirada, sin mediar una investigación seria y profunda de la historia y desarrollo del acceso a la red de redes en nuestro país.

Otra vez *The Washington Post* nos hace recordar al escritor y periodista uruguayo Eduardo Galeano, quien expresó que cuando se trata de Cuba, los grandes medios de comunicación, "aplican una lupa inmensa que magnifica todo lo que allí ocurre cada vez que conviene a los intereses enemigos, llamando la atención sobre lo que pasa en la Revolución, mientras la lupa se distrae y no alcanza ver otras cosas importantes".

Entre esas cosas importantes que no alcanza a ver la lupa inmensa del *The Washington Post*, está que el Gobierno revolucionario cuba-

no, en medio de un brutal cerco económico y decenas de millones dedicados por el Gobierno de los Estados Unidos a la subversión, siempre ha estado al tanto de los adelantos de las tecnologías relacionadas con la información, la comunicación y las telecomunicaciones, para poner esos avances a disposición del desarrollo del país y de los sectores menos favorecidos de Cuba y el mundo.

Acusaban al Gobierno cubano de enemigo de internet y del uso de las TIC por sus ciudadanos, mientras el líder de la Revolución Cubana, Fidel Castro, fundaba en 1987 el programa de los Joven Club de Computación y Electrónica, que conjuga como ninguno las tecnologías con el conocimiento y la cultura, que en sus más de 32 años de trabajo ha preparado de forma gratuita más de 4.8 millones de cubanos y prestado importantes servicios a la comunidad, centros de salud, escuelas y otras instituciones, contribuyendo a que Cuba ocupe un lugar destacado entre todos los países en habilidades en el uso de las TIC.

Decían que Cuba era enemigo de internet; y ya en 1992, cuando los dueños de internet no permitían que la Mayor de las Antillas se conectara a esta red, surgió la red Infomed como un proyecto del Centro Nacional de Información de Ciencias Médicas, en aras de dar respuesta a la necesidad de facilitar el intercambio de información entre profesionales, académicos, investigadores, estudiantes y directivos del Sistema Nacional de Salud cubano.

Desde su surgimiento, Infomed se desarrolló bajo los conceptos de un modelo descentralizado de construcción colectiva, de lo cual da fe el desarrollo de los nodos en todas las provincias, la creación de dominios territoriales, el desarrollo de sitios y páginas web a todos los niveles, la incorporación sostenida de usuarios y la amplia producción de contenidos y servicios en momentos en que aún no existían los *blogs*, las *wikis* y demás vías que hoy se resumen en la idea de web 2.0. Por la calidad de su información, Infomed es uno de los sitios más consultados por profesionales de la salud en varios países de América Latina.

Trataron de sembrar la idea de que a los jóvenes se les excluía del acceso a las TIC y, sin embargo, en septiembre de 2002, la Universidad de Ciencias Informáticas (UCI), abrió sus puertas al primer curso académico con 2008 estudiantes procedentes de todos los municipios del país.

En estos 17 años, la UCI ha graduado a más de 14 500 ingenieros y en la actualidad tiene una matrícula superior a los 3000 estudiantes de pregrado.

Posee centros de desarrollo de *software* que se especializan en soluciones informáticas, desarrollo tecnológico e investigaciones asociadas. En más de 130 organismos y organizaciones del país están presentes los productos que se generan en esa institución.

Junto a la Ingeniería en Ciencias Informáticas, se estudia la carrera de Ingeniería Bioinformática, encaminada a la formación de profesionales que trabajen con herramientas para el análisis de datos en centros de investigación y salud del país. En el curso 2020-2021 se inició la carrera de Ingeniería en Ciberseguridad, que por cierto, se estudia en universidades de gran cantidad de países, pero que solo al iniciarse ahora en Cuba, molesta al periódico estadounidense.

Si estos tres ejemplos no bastaran, las cifras que incomodan, tanto a los representantes del imperio como para tratar de enmascararlas con manipulaciones, dan fe de los avances de Cuba en el sector de las telecomunicaciones y las TIC en los últimos años. El reconocimiento ya no es solo en las habilidades, sino también en el uso y acceso, sin desconocer que hay mucho que lograr en términos de tarifas más bajas, calidad en los servicios y ampliación del acceso.

Ahora no les queda más remedio que reconocer que sí hay acceso a internet; pero los ataques van dirigidos a otros objetivos. Las realizaciones alcanzadas en los últimos años en el acceso a internet han echado por tierra el estereotipo que han pretendido fabricar, ahora no pueden aducir que no hay acceso a la red y buscan otras falacias como que el Gobierno cubano se enriquece con internet.

Es pura hipocresía acusar al Gobierno cubano y por otro lado, callar que se impide el desarrollo económico de Cuba arreciando el bloqueo, que ha provocado daños en este sector en los últimos 10 años por más de 500 millones de dólares. Para alcanzar un desarrollo sostenido en el sector se necesita duplicar las inversiones, cuestión que impiden las sanciones aplicadas por el actual Gobierno estadounidense y que calla la prensa corporativa como *The Washington Post*, que para Cuba pretende disfrazarse de alternativa.

Es conocido y lo ha reiterado el ministro de Comunicaciones de Cuba, Jorge Luis Perdomo Di Lella, en varias comparecencias televisivas, que los ingresos provenientes de los servicios de internet se emplean para mantener la operación de la infraestructura de las telecomunicaciones del país, invertir para el desarrollo y aportarle a la economía para resolver otras necesidades de los sectores sociales y de la población afectados por el bloqueo. Las verdades dichas por el ministro de Comunicaciones en la Televisión Cubana, han derrumbado los estereotipos que se han empeñado en construir la propaganda pagada por el Gobierno estadounidense y la prensa corporativa a su servicio, y por eso aparecen artículos como el citado.

¿Quién se ha enriquecido verdaderamente con el tema internet en Cuba? Muchas agencias y personajes que han formado parte de un sinnúmero de fracasados proyectos provenientes del vecino del Norte, son los que en verdad se han hecho ricos con el abundante dinero aprobado por el Gobierno de los Estados Unidos para estos fines. Pregunten a los organizadores de ZunZuneo, Piramideo, a Alan Gross, a quienes escriben para la mal llamada *Radio Martí* y la telaraña de medios digitales que publican todo el tiempo propaganda disfrazada de periodismo contra la Revolución Cubana. Hagan verdadero periodismo alternativo: pregunten a las instituciones estadounidenses que financian cursos, publicaciones y eventos para usar internet contra la Revolución y veremos si entonces los publica *The Washington Post*.

Algo avanza internet en Cuba, y cómo molesta cuando se informa sobre ello, a pesar de las críticas, los impedimentos y las manipulaciones. Creo que se ajusta perfectamente a la interpretación que se deriva de ese artículo en *The Washington Post*.

Ataques en la red social *Twitter*

El 8 de enero de 2013, la red social Twitter suspendió, por tiempo indefinido, más de 900 cuentas pertenecientes a la organización cubana Joven Club de Computación y Electrónica. Este hecho coincidió con la cobertura que realizaban del recorrido conmemorativo de la caravana que condujo a Fidel Castro y otros miembros del Ejército Rebelde a La Habana en enero de 1959, luego del triunfo de la Revolución Cubana.

Las etiquetas #Cuba y #Caravana54 ocuparon lugares destacados durante varios días. La primera hasta el 7 de enero tenía 30 574 tweets y desde el 3 de enero se había posicionado entre las 20 etiquetas más populares.

El 18 de mayo de 2018, en medio de la intensa cobertura al accidente aéreo ocurrido en La Habana ese día, la red social Twitter bloqueó la cuenta del sitio Cubadebate, el medio de noticias que más visitas recibe. Un mensaje automático de Twitter explicaba que "su cuenta está temporalmente restringida porque ha presentado actividad inusual".

El 11 de septiembre de 2019, minutos antes de comenzar la comparecencia en televisión del presidente cubano Miguel Díaz-Canel Bermúdez y otros funcionarios del gobierno, para explicar las medidas para enfrentar la actual coyuntura energética del país, provocada por la intensificación del bloqueo del Gobierno estadounidense, la red social Twitter suspendió las cuentas de varios medios de comunicación de la Isla, entre ellos Granma y Cubadebate; la de otras instituciones, periodistas y funcionarios de varios organismos.

Si bien es cierto, que no es la primera vez que usuarios cubanos de Twitter reportan problemas para ingresar a sus cuentas y reciben mensajes que estas han sido bloqueadas, el caso lo distingue la masividad —más de 250 cuentas— y el matiz político ideológico de este hecho de guerra cibernética. Estos son solo algunos ejemplos de los ataques de Twitter en medio de eventos importantes para Cuba.

¿Existe algún otro antecedente donde la red social Twitter haya actuado a las órdenes del Gobierno estadounidense?

En su momento, varios medios de comunicación publicaron que durante las elecciones de 2009 en Irán, la entonces secretaria de Estado, Hillary Clinton, ordenó posponer un mantenimiento programado a los servidores de esta red social para permitir que supuestos activistas iraníes denunciaran el fraude de las elecciones, las manifes-

taciones del pueblo y la represión del gobierno de ese país. *Twitter* cumplió con el mandato del Departamento de Estado y pronto se supo que la mayor parte de los activistas que enviaban sus *tweets* se encontraban en territorio estadounidense, y que estas acciones provocaron unos 20 muertos.

Durante el Referéndum Constitucional en Cuba, los enemigos de la Revolución utilizaron *Twitter* para intentar que hubiese rechazo ciudadano y ofrecer al mundo una falsa imagen de oposición antigubernamental. Entre los principales implicados en esa tentativa se encontraba la Office of Cuba Broadcasting, oficina del Gobierno de los Estados Unidos a la que pertenece *Radio TV Martí*, que forma parte del Grupo de Trabajo sobre Internet en Cuba.

Pudiera referirse a lo acontecido el 11 de septiembre de 2019, minutos antes de iniciarse la transmisión en vivo de la comparecencia especial del presidente Miguel Díaz-Canel Bermúdez en el programa televisivo Mesa Redonda.

Como es conocido, en ese momento la red social *Twitter* inició el bloqueo numeroso y selectivo de más de 250 cuentas de medios de prensa y profesionales del sector, de algunos organismos y sus gestores de comunicación.

El objetivo de este ciberataque fue limitar el alcance e impacto en la opinión pública cubana e internacional de la información sobre la situación energética del país que el presidente Díaz-Canel realizaría en la *Mesa Redonda*, y sobre el plan genocida de la actual administración estadounidense contra el pueblo de Cuba.

También pretendían crear una situación que desviara la atención y el debate hacia otro tema, cuestión que se corroboró al día siguiente, cuando en el sitio *OnCuba* se publicó un artículo donde un directivo de *Twitter* justificó la suspensión masiva de las cuentas, argumentando que era por violación de las normas y condiciones del servicio de esa red social, utilizando un lenguaje muy técnico y poco comprensible para la mayoría del público.

¿Qué repercusión tuvo este ataque desde el punto de vista de la comunicación?

A pesar del bloqueo de estas cuentas, el volumen de contenidos generados con las etiquetas #Cuba, #NoMásBloqueo, #AquíNoSeRindeNadie fue numeroso, al ser usadas por casi 13 mil usuarios que generaron más de 76 mil mensajes.

Por solo citar un ejemplo, la etiqueta #Cuba alcanzó un número mucho más elevado de lo que se manifiesta a diario, pues se generaron más de 63 mil *tweets*, por más de 12 mil usuarios. Aquí por supuesto, no se pudo considerar las cuentas de *Cubadebate* y de *Granma*, que reúnen más de 700 mil seguidores.

Sin dudas, aunque lograron limitar no pudieron impedir que Twitter sirviera de plataforma para amplificar el mensaje de la Revolución.

Así es, y hay que destacar que otras redes sociales también se pliegan a este tipo de maniobras, sirviendo como plataformas para la subversión político ideológica y la desestabilización.

Noticias falsas o *fake news*

Desde siempre, las fuerzas reaccionarias han utilizado las noticias falsas o fake news con un interés político, en el sentido de manipular o falsear la verdad a través de la información.

En relación con Cuba, existen muchísimos ejemplos a lo largo de la historia; desde inventar en febrero de 1898 en la prensa estadounidense un falso ataque a un buque de ese país, el acorazado USS Maine, en el puerto de La Habana, para justificar la declaración de guerra de los Estados Unidos a España; pasando por las campañas de desinformación en torno a la Operación Peter Pan; sobre la existencia de una base de submarinos nucleares soviéticos en Cienfuegos en 1970; la presencia en la Isla de aviones MIG-23 en 1978, con el supuesto objetivo de bombardear los Estados Unidos con armas atómicas; acerca de la supuesta responsabilidad de Cuba en el auge revolucionario centroamericano impulsada por el gobierno de Ronald Reagan en 1981; hasta los supuestos

ataques sónicos en la embajada de los Estados Unidos en La Habana, inventado por el Gobierno de Donald Trump, para muchos, uno de los capítulos más inverosímiles en la incesante campaña de engaños, calumnias y fechorías contra la Revolución Cubana provenientes del vecino del Norte desde 1959.

El desarrollo de las Tecnologías de la Información y la Comunicación, de internet, las redes sociales digitales y de la telefonía móvil, han propiciado la circulación de las fake news, teniendo en cuenta que en las condiciones actuales, su principal ámbito de actuación es el mundo digital. En el caso de Cuba, ¿cómo influyen las noticias falsas en la seguridad del país?

Las noticias falsas o *fake news* circulan en cualquier tipo de medio: radio, televisión, prensa escrita; pero hoy la regla es que se difundan a través de los medios digitales, e incluyen cualquier reportaje, referencia, información, mensajes y datos que son total o parcialmente falsos en forma de texto, imágenes y audio.

Si bien es cierto que la comunicación social y el derecho de los ciudadanos de recibir información veraz se afectan con las *fake news*, en el caso cubano se emplean en lo fundamental con fines políticos, para crear un escenario que permitan acciones y medidas dirigidas a destruir la Revolución. Te referiste a algunos casos acontecidos en los últimos 60 años; pero ahora aparecen con mucha sistematicidad y llegan a muchas personas de la mano de las redes sociales digitales y de las plataformas móviles. Como diría el doctor en Lingüística Pedro Santander Molina, "podemos conceptualizar *las fake news* como un bulo mediado por lo tecnológico"[31].

¿Qué acciones se están ejecutando a nivel internacional para frenar la propagación de noticias falsas en línea?

Tenemos información que en más de 40 países se han aprobado normas jurídicas sobre este particular o se trabaja en su elaboración. En Singapur, por ejemplo, una ley aprobada en mayo de 2019 plantea que una persona no debe realizar ningún acto dentro o fuera de

[31] Santander Molina, Pedro: *¿Cómo combatir las fake news sin contribuir a su propagación?*, 25 de junio de 2019. Disponible en www.cubadebate.cu.

Singapur para publicar una noticia, sabiendo o teniendo razones para creer que es una declaración de hechos falsa y la comunicación de la declaración pueda ser perjudicial para la seguridad de Singapur; ser perjudicial para la salud pública, la seguridad pública, la tranquilidad pública o las finanzas públicas; ser perjudicial para las relaciones amistosas de Singapur con otros países; e influir en el resultado de una elección. Establece penalizaciones de hasta $735 000 para empresas y máximo de 10 años en prisión para individuos.

En Francia, una ley de diciembre de 2018, conocida como Ley Orgánica contra la manipulación de la información, está dirigida principalmente a la protección de las campañas electorales. Entre sus objetivos está detener la difusión de la información falsa durante los tres meses anteriores a una elección nacional. Las plataformas digitales como *Facebook y Twitter* están sujetas a obligaciones de transparencia. Cuando distribuyen contenido, deben nombrar a los anunciantes que lo financian y permitirles a las autoridades de Francia suspender los medios que intentan desestabilizar una votación.

En el caso de China, no hay una ley dirigida solo a las *fake news*, sino que el Estado chino declara que los crímenes de difamación, disturbios, negocios ilegales y extorsión son aplicables también al ciberespacio. La Ley de Ciberseguridad y Protección del ciberespacio establece que se debe proteger el ciberespacio de hechos de esta índole.

En Alemania entró en vigor en enero de 2018 una ley dirigida a compañías de medios sociales como *Facebook y Twitter,* para obligarlas a eliminar en un plazo de 24 horas discursos de odio. Se pretende agregar una enmienda que permita a los usuarios restaurar el contenido eliminado de forma incorrecta de la web.

Rusia trabaja en un proyecto de ley, donde las autoridades pueden bloquear sitios web que no eliminen la información sensible publicada; establece penalizaciones por difundir información que exhibe una falta de respeto flagrante para la sociedad, el gobierno, los símbolos oficiales del gobierno, la constitución u organismos gubernamentales de Rusia. Las multas se calculan en función de si el violador es un ciudadano, un funcionario o una entidad legal.

Por último, una ley australiana de 2019, penaliza a las compañías de redes sociales por la propagación de rumores y contenido de odio en sus plataformas. Si no eliminan la información de manera expedita, las empresas tendrán que pagar una multa considerable de hasta 10 % de sus ganancias anuales y los empleados podrían ser encarcelados por hasta tres años.

Y en el caso de Cuba, ¿existe alguna norma jurídica al respecto?

Exactamente, una norma para enfrentar las noticias falsas no existe en nuestro país. En el Código Penal vigente hay una tipificación de los llamados delitos contra el honor, que incluyen figuras como la difamación, la calumnia y la injuria, los cuales podrían invocarse en determinados casos. Creo que en el paquete de normas que se pondrán en vigor para implementar la Política de Comunicación Social este asunto se abordará.

Estudios realizados por instituciones extranjeras calculan que para 2022, 50 % de todas las noticias que circularán por la red serán falsas, entonces el desafío que tenemos también está en el orden ético, cultural y tecnológico. En el contexto de la lucha que libramos en el orden político, ideológico y comunicacional contra el imperialismo del Norte, no basta con entender cómo funciona este fenómeno, sino adoptar las medidas para fortalecer la protección y el uso legal del ciberespacio cubano.

La batalla de la izquierda en las redes sociales

El imperialismo estadounidense y sus lacayos de la derecha latinoamericana han utilizado las redes sociales digitales para mentir y crear escenarios favorables a sus intereses. No podía ser de otra manera si tenemos en cuenta que estas plataformas forman parte del poder mediático diseñado para aplastar a las fuerzas de izquierda y todo lo que huela a progreso para las grandes masas.

Jugaron su papel en los golpes de Estado de Paraguay-2014, Brasil-2016 y Bolivia-2019, en los resultados de procesos eleccionarios como el de Brasil en 2018 y en la demonización e intento de juzgar a líderes de izquierda como Lula y Rafael Correa.

Algunas redes sociales han estimulado también el fuego para atacar a Venezuela, Nicaragua y Cuba, y servido de base a múltiples campañas donde se repetían mentiras y falsedades con el objetivo de convertirlas en verdades.

En el caso de Bolivia, investigaciones sobre las cuentas de Twitter de varios de los personajes que lideraron el golpe de Estado confirman que se puso en marcha una operación de guerra cibernética, con el objetivo de inundar de propaganda, en contra de Evo Morales, las redes sociales digitales y hacer válida la matriz de opinión de que quería eternizarse en el poder, hacer fraude y que es culpable de la represión desatada contra el pueblo.

En esta campaña crearon más de 70 000 cuentas robots o falsas en Twitter, para seguir al líder golpista Luis Fernando Camacho, que utilizaban las etiquetas #EvoEsFraude, #BoliviaNoHayGolpe, #EvoDictador, entre otras.

En esos difíciles momentos, las fuerzas de izquierda de América Latina, que van más allá de partidos, y que tienen una expresión en los pueblos y movimientos sociales, no se cruzaron de brazos y en el orden mediático y de las ideas libraron una verdadera batalla en las redes sociales digitales. ¿Qué características tuvo la participación de las fuerzas de izquierda en las redes sociales digitales en los días iniciales del golpe de Estado en Bolivia?

Lo primero que pudiéramos decir es que las fuerzas revolucionarias de nuestro continente no tuvieron que emplear robots ni cuentas falsas en *Twitter* para defender la verdad y a Evo Morales, en los días más complejos del golpe de Estado. Más de 135 mil usuarios de esta red social, personas de carne y hueso, aportaron medio millón de mensajes denunciando el golpe.

A partir de la declaración del Ministerio de Relaciones Exteriores de Cuba, el 9 de noviembre de 2019, donde se denunció que sectores de la oposición boliviana, con el apoyo y conducción del Gobierno de los Estados Unidos y de oligarquías regionales, pusieron en marcha un golpe de Estado con el objetivo de escamotearle al pueblo boli-

viano el resultado electoral, se activó el activismo de la izquierda que llegó a generar el 10 de noviembre, 14 mil mensajes con la etiqueta #EvoNoEstásSolo y casi 8 mil con #NoAlGolpeEnBolivia. El 11 de noviembre se transmitieron más de 51 mil *tweets*, de ellos, unos 41 mil mensajes se publicaron con la etiqueta #NoAlGolpeEnBolivia.

Varias personalidades se manifestaron en *Twitter* en contra del golpe, como la premio Nobel de la Paz @RigobertMenchu: "Entristece e indigna ver las manifestaciones de odio contra los pueblos indígenas de parte de grupos oligárquicos como sucede en Bolivia y del que es víctima el presidente Juan Evo Morales Ayma y el pueblo boliviano. #EvoElMundoContigo #EvoNoEstásSolo #EvoPresidenteLegítimo"; el politólogo vasco @KatuArkonada: "Masiva movilización en Buenos Aires en rechazo al golpe de Estado en Bolivia. Compas la solidaridad es más importante que nunca, no dejemos solo a @EvoEsPueblo ni al pueblo boliviano #EvoNoEstásSolo", y el periodista y poeta @ Marco_Teruggi: "Honor y gloria a los caídos. ¿Qué pedimos? Justicia, esta noche en Cochabamba por los nueve muertos #GolpeDeEstadoEnBolivia #MasacreEnBolivia". (Fig. 10).

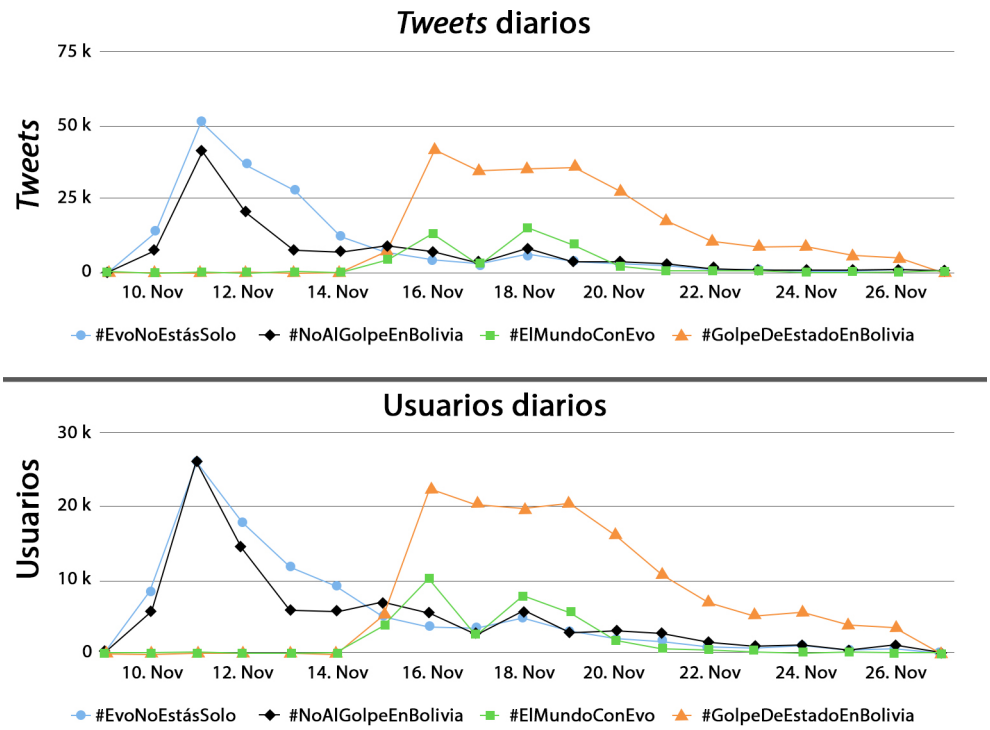


Fig. 10. *Tweets* y usuarios diarios.

Las manifestaciones que se han realizado en Chile, Colombia, Haití y otros países tienen su reflejo en las redes sociales digitales, aunque los grandes medios manipulen la realidad. Las fuerzas de izquierda no están dormidas, tienen que organizarse y unirse para enfrentar al neoliberalismo y movilizar a los pueblos de nuestra América. Como diría Fidel Castro:

> […] Qué difícil se le hace cada vez más al imperialismo engañar a una parte del pueblo latinoamericano todo el tiempo. Y llegará el momento en que no pueda engañar absolutamente a nadie de los pueblos latinoamericanos y del Caribe. Esas son las lecciones de la historia. Y mal anda un imperio cuando su arma más poderosa, la mentira, empieza a fallarle; cuando su instrumento más poderoso, cuando su garra más hiriente, que es la mentira, empieza a ser inofensiva, empieza a ser ineficaz, empieza a ser inútil […][32].

[32] Castro, Fidel: Discurso en la clausura del III Encuentro Continental de Mujeres, La Habana, 7 de octubre de 1988, *Granma*, 12 de octubre de 1988, p. 5.

¿Cómo están participando los cubanos en las redes sociales?

El acceso de los cubanos a las redes sociales es una realidad cada vez más visible. Estas plataformas permiten el acceso de la población cubana a contenidos y materiales audiovisuales de diferentes temáticas, y posibilitan la participación, con opiniones, criterios y propuestas.

Cuba fue el país de mayor crecimiento en dos categorías de conectividad digital en 2017, de acuerdo con el reporte *Digital in 2017 Global Overview* (Fig. 11): presencia en redes sociales—con más de 2.7 millones de nuevos usuarios y 365 % de incremento respecto al año precedente— y uso de móviles para acceder a las redes sociales —2.6 millones de nuevos usuarios y un aumento de 385 %[33]. A partir del año 2018, estas cifras se multiplicaron con la ampliación del acceso a internet desde las viviendas y la apertura del acceso a la red de redes desde los móviles.

En septiembre de 2017, 88 % de los cubanos que accedían a las redes sociales se conectaba a *Facebook*; pero al cierre de septiembre de 2018 era 46.5 %. El uso de *Youtube* creció considerablemente, de 3.59 % en septiembre de 2017 a 36.18 % en el propio mes de 2018[34]. Hoy *Youtube* es la red social con más accesos desde Cuba; pero se impone colocar más contenidos nacionales.

[33] Kemp, S. (2017): "Digital in 2017 Global Overview". We Are Social, Nueva York.
[34] https://statcounter.com/.

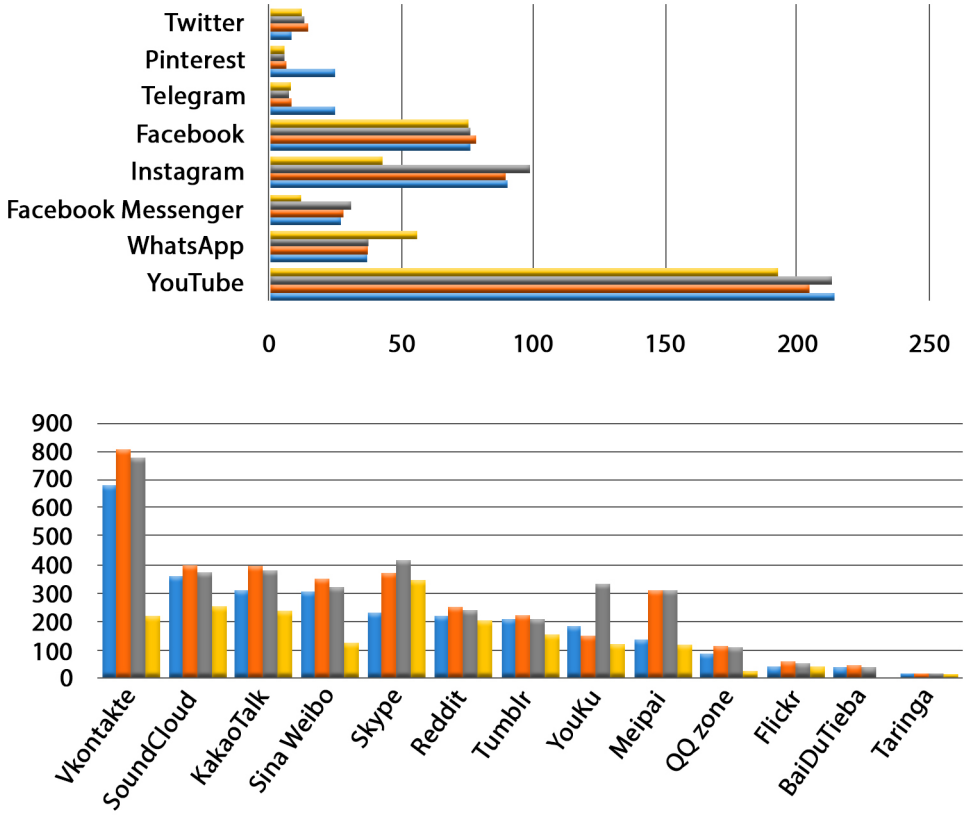


Fig. 11. Principales redes sociales.

Creo que en los últimos años ha crecido la masa crítica de revolucionarios cubanos que se enfrentan a los grandes medios de la información, divulgan la verdad de la Revolución y llevan la cultura a todos los confines del mundo con un sentido descolonizador. No es de extrañar que la etiqueta #VictoriaDeCuba se haya convertido en tendencia mundial en *Twitter* en noviembre de 2019, tras la votación de la Resolución Cubana contra el bloqueo de los Estados Unidos en Naciones Unidas, y que cada vez más cubanos participen en las redes de solidaridad e interacción creadas para dar a conocer la verdad de nuestros pueblos.

El bloqueo del Gobierno de los Estados Unidos afecta la protección del ciberespacio nacional cubano

Desde hace 60 años, el Gobierno de los Estados Unidos bloquea el acceso de Cuba a las telecomunicaciones y a tecnologías necesarias para su desarrollo. El equipamiento, plataformas y productos informáticos destinados a fortalecer la ciberseguridad del país, no escapan al cerco económico, financiero, comercial y tecnológico tendido sobre la Isla.

Basta citar que en los últimos 10 años el bloqueo ha ocasionado más de 500 millones de dólares de pérdidas al sector de las telecomunicaciones y las TIC. (Cuadro 2).

Año	*Valor (USD)*
2010	*61 240 43*
2011	*7 396 394*
2012	*66 766 000*
2013	*44 200 000*
2014	*34 200 000*
2015	*57 122 900*
2016	*59 208 700*
2017	*68 922 110*
2018	*64 144 319*
2019	*55 000 000*
Total	***518 200 853***

¿Cómo impacta el bloqueo económico, financiero, comercial y tecnológico en la ciberseguridad de nuestro país?

La política de hostilidad de los Estados Unidos hacia Cuba tiene repercusiones en la protección del ciberespacio nacional. En realidad, pasamos mucho trabajo para acceder a suministros de tecnologías y equipos producidos bajo licencia o utilizando componentes estadounidenses, lo que implica que haya que acudir a mercados lejanos, con sus correspondientes afectaciones monetario-financieras.

Las empresas que poseen equipos con menos del 25 % de componentes estadounidenses tampoco nos quieren vender, debido a las presiones que reciben. Eso es una realidad que vivimos en estos momentos y que retrasa algunos proyectos en marcha.

¿Puedes mencionar algún ejemplo que ilustre esta situación?

Es conocido que al proveedor chino ZTE le impusieron una multa de 1150 millones de dólares, supuestamente por violar las leyes del bloqueo, y estas presiones motivaron que se quedaran sin respaldo equipos de este fabricante, instalados en las redes de telecomunicaciones del país.

También te puedo decir que el costo por reparación a través de terceros, de tarjetas, módulos y equipos, como promedio, se duplica al no poderse realizar directo con algunos proveedores y fabricantes, cuando conocen que el cliente es cubano.

Agregaría que a Cuba se le niega el acceso a la información oficial de sitios tecnológicos de primera línea, lo que dificulta la autopreparación o capacitación a distancia de especialistas y técnicos.

¿Cómo se manifiestan las afectaciones del bloqueo del Gobierno estadounidense en la empresa Segurmática?

En primer lugar, Segurmática está imposibilitada de participar en el programa "Iniciativa de virus de Microsoft" (MVI). En el año 2017 se completó el formulario de solicitud y recibieron la notificación que debido a las restricciones del bloqueo, por el momento esto no era posible.

MVI permite que las organizaciones logren que sus productos funcionen e integren con Windows, y que compartan información sobre el panorama de amenazas en la red.

Sus miembros reciben acceso a las bibliotecas de Windows, como las utilizadas por Windows Defender Security Center, muestras, estudios de comportamiento de *malware* e invitaciones a eventos y conferencias relacionadas con la seguridad. Para una empresa como Segurmática, que desarrolla productos antivirus para Windows, que son empleados tanto por las organizaciones como por la población, es vital poder formar parte de programas como este.

Por otro lado, se dificulta la captura de muestras de programas malignos, cuestión que constituye la fuente fundamental para que los programas antivirus de Segurmática mantengan una actualización respecto al enfrentamiento a estos. Los especialistas deben mantener una vigilancia constante y obtener los insumos que dan sitios especializados en programas malignos y que incluyen análisis con diferentes productos. En varios sitios, a las direcciones de Cuba se les permite subir muestras; pero no su descarga hacia nuestros servidores.

Por último, el elemento fundamental del producto antivirus lo constituye su motor. Para los sistemas operativos Windows de 64 bit, es un requerimiento que el *driver* esté certificado digitalmente. En varios años, el producto Segurmática Antivirus no pudo activar la protección permanente en los sistemas operativos mencionados por no tener la posibilidad de firmarlo, siendo la empresa Microsoft su propietaria.

A pesar del escenario adverso, estamos buscando soberanía sobre la gestión de los códigos malignos en el país, en particular, fortaleciendo nuestro antivirus y evolucionando sus funcionalidades a una *suite* de seguridad, que integre varios servicios para la protección de los dispositivos, como lo demanda el proceso de informatización de la sociedad cubana.

Cuba en tiempos de coronavirus, su repercusión mediática

Varios grandes medios de comunicación capitalistas se han referido de manera positiva —algo inusual— a la estrategia y accionar de Cuba en relación con el enfrentamiento a la Covid-19.

Al consultar la prensa extranjera y agencias de noticias a principios del mes de marzo de 2020, predominaban los ataques dirigidos a demonizar a Cuba en la esfera de la cultura, la libertad de opinión y creación y los derechos humanos en general. Trataban de fijar la matriz de opinión de que había un "incremento de la represión" para "silenciar voces críticas", las "detenciones arbitrarias y las restricciones al movimiento".

Pero el anuncio de las autoridades cubanas sobre la política y las acciones que seguiría el país para prepararse y prevenir la pandemia del coronavirus, concitó de inmediato la atención de las agencias y los medios de prensa extranjeros y no les quedó más remedio, ante tanta evidencia, que reflejar la verdad.

¿Qué comportamiento tuvo el tema Cuba en los medios de prensa capitalistas en el mes de marzo de 2020?

La realidad es que la repercusión mediática internacional del tratamiento a la Covid-19 en Cuba, sepultó otros temas que eran fuente de ataques contra nuestro país, dejó aisladas las presiones a través de la alcaldía de Miami parta suspender los vuelos entre Cuba y la Florida, y silenció la campaña contra las misiones de colaboración médica.

A partir de marzo de 2020, Cuba fue reconocida en noticias, comentarios o menciones en más de 400 titulares, de unos 50 medios de todos los continentes, en un promedio diario de más de 15 países.

Estos medios publicaron las medidas que se aplicaron, sobre todo, en su naturaleza preventiva y universal, la normalidad y confianza que vive el país, destacaron la fortaleza de nuestro sistema y promovieron noticiosamente nuestros medicamentos para el tratamiento de la enfermedad.

Algunos abordaron la solidaridad y la solución del caso del crucero británico MS Braemar, el impacto positivo en la opinión pública internacional y el agradecimiento de las autoridades inglesas; la solidaridad, colaboración y el envío de brigadas médicas a distintos países, en especial, la región de Lombardía, la más infectada de Italia.

Medios muy posicionados difundieron titulares atrevidos como “¿Por qué los Estados Unidos se oponen a que países afectados por el coronavirus pidan ayuda a Cuba?” (CNN en inglés); “los cubanos lidian con la pandemia en medio de la escasez y el embargo estricto de los Estados Unidos” (NBC); “Cuba lo entiende mejor que nosotros”. (Rabble, de Canadá).

Varios medios progresistas y de izquierda, y hasta algún otro fuera de ese entorno, han destacado que lo que se hace en Cuba refleja

un alto nivel de gobernabilidad, en medio del incremento del acoso y la guerra económica de los Estados Unidos; lo contrastan con lo que algunos denominan "descalabro" de los servicios de salud en el capitalismo, sobre todo, en la Unión Europea y los Estados Unidos, convertidos ahora en epicentros de la pandemia.

¿Y en las redes sociales digitales?

Por otro lado, la labor de Cuba frente a la pandemia ha sido muy reconocida en las redes sociales digitales. Por ejemplo, a pesar de que *Twitter* ha eliminado buena cantidad de perfiles de revolucionarios cubanos, la etiqueta #CubaSalvaVidas fue tendencia a nivel mundial —lugar 15— entre el 11 y el 26 de marzo de 2020. En Argentina y Ecuador fue primer lugar, en Venezuela, segundo lugar, en México, tercero, en Perú el onceno y en Colombia el lugar veintitrés. Las etiquetas de la Revolución han tenido un mayor impacto que las matrices de opinión de la contrarrevolución.

En este período, los usuarios más retuiteados fueron el perfil de la cancillería cubana @CubaMINREX, @cubavsbloqueo y @dominiocuba.

Los mensajes más retuiteados fueron:

#CubaSalvaVidas ¡Qué grande es Cuba! Pese al criminal bloqueo sobre Cuba, la hermana nación da un ejemplo de solidaridad con el mundo enviando doctores a 38 naciones para combatir el coronavirus.

#GanamosConLaPrevención @NicolasMaduro

#CubaSalvaVidas. Mientras algunos países solo envían bombas, Cuba envía doctores por todo el mundo combatiendo las peores enfermedades y salvando vidas. #GanamosConLaPrevención

A cualquier parte que va el médico cubano está pendiente de la salud del ser humano, de la integridad. #CubaSalvaVidas

Imágenes más compartidas en las redes sociales (Fig. 12):

En el período que referíamos, del 11 al 26 de marzo de 2020, la etiqueta #Cuba, tuvo 88 9267 *tweets*, de 16 1528 usuarios y un alcance potencial de 433 801 815 seguidores. En 24 horas, como promedio, se enviaron 57 493 *tweets* por 17 296 usuarios, con un alcance potencial de 56 466 708 seguidores.

No obstante, algunos sitios contrarrevolucionarios continúan insistiendo, sin éxito, en descalificar las medidas adoptadas por el Gobierno revolucionario y la actuación de entidades estatales y los órganos del orden interior.

La imagen y el prestigio de Cuba se han fortalecido, y una muestra de ello es que se incrementaron los titulares que destacan las distintas demandas que se han producido para que el Gobierno estadounidense levante el bloqueo económico y el asedio unilateral contra nuestro país.

Si tuviera que resumir este momento, diría que el Gobierno los Estados Unidos y los medios contrarrevolucionarios están aislados y sin repercusión visible en los ataques a Cuba en tiempos de coronavirus.

STATUS QUO DE LA GOBERNANZA DE INTERNET

Control unilateral de los Estados Unidos sobre internet

Ya en la década del setenta, en diferentes eventos e investigaciones auspiciadas por la Organización de Naciones Unidas (ONU), se denunció el desbalance entre los países capitalistas desarrollados y los países del llamado Tercer Mundo, en lo referido a la información y la comunicación.

En el informe presentado en el coloquio sobre intercambio de información, celebrado en Florencia, Italia, en abril de 1977, se manifestó que "América Latina estaba invadida de tal modo por las instituciones económicas, políticas y de comunicación estadounidenses, que es legítimo hablar de dominación extranjera en beneficio de los Estados Unidos y considerar este fenómeno de dependencia como una amenaza"[35]*. Algo similar sucedía con los países africanos y asiáticos.*

Esta situación se agudizó con el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y el surgimiento de internet, que incrementó el control transnacional en el campo de la información y la comunicación. Pese a los esfuerzos de la ONU y de un grupo de países, no se han logrado aprobar instrumentos legales jurídicamente vinculantes, que permitan una regulación internacional de la red de redes.

¿Cuáles son los antecedentes que llevaron a poner en la agenda de análisis de la ONU lo relacionado con la gobernanza de internet?

[35] González-Manet, Enrique (1987): *La guerra oculta de la información*, Ed. Ciencias Sociales, p. 27, La Habana, Cuba.

Como es conocido, internet surgió en los Estados Unidos. Joseph Carl Robnett Licklider, designado por el presidente de ese país, John Kennedy, al frente de la Oficina de Técnicas para el Procesamiento de la Información (IPTO) de la Agencia de Proyectos de Investigación Avanzada (ARPA), del Departamento de Defensa, ideó interconectar a las universidades estadounidenses más importantes en una red de computadoras, que él llamaba *'Intergalactic Computer Network'*, la que después se llamaría ARPANET, la antecesora de internet.

La red ARPANET se creó en 1969 con cuatro minicomputadoras ubicadas en varias universidades de la costa oeste de los Estados Unidos, empleando el protocolo Network Control Protocol (NCP). La primera demostración pública tuvo lugar en la International Conference on Computer Communications (ICCC) en 1972.

El 1.º de enero de 1983, la ARPANET pasaba del protocolo NCP al TCP/IP, naciendo internet. Al año siguiente se introduce el sistema de nombres de dominios o Domain Name System (DNS).

La mayoría de los servidores raíces se encuentran en territorio de los Estados Unidos. En 1992, este gobierno asigna a la National Science Foundation (NSF) la coordinación y financiación de la parte no militar de internet y contrata a la empresa privada Network Solutions Inc. (NSI), para operar el DNS. Tres años después sacó del entramado a la NSF y se firmó un contrato entre el Departamento de Comercio y la NSI. De esta manera se crearon las condiciones para privatizar internet y cobrar el registro de los dominios.

Durante el gobierno de William Clinton se presentó un plan para la privatización del DNS, que provocó una fuerte oposición fuera y dentro de los Estados Unidos. Se creó la Corporación de Internet para la Asignación de Nombres, (ICANN), como una organización privada sin ánimo de lucro, bajo las leyes del estado de California; y es contratada por el Departamento de Comercio para gestionar recursos críticos de internet.

¿Qué decisión tomó la ONU ante esta situación?

Hay que decir que la Unión Internacional de Telecomunicaciones (UIT), organismo de la ONU, en 1996 —por cierto, el año en que

se le permite a Cuba acceder a internet— propone el traslado del servidor raíz de los Estados Unidos a Ginebra, Suiza. Esta iniciativa se acompañó por 80 gobiernos que firmaron un Memorando de Entendimiento (no vinculante), del cual fue depositario la UIT.

Por supuesto, el Gobierno estadounidense no estuvo de acuerdo y chantajeó a la UIT, al manifestar que no apoyaría la realización de una Cumbre Mundial sobre la Sociedad de la Información si no se olvidaba del Memorando.

Al final, la primera fase de la Cumbre Mundial de la Sociedad de la Información se celebró en Ginebra en diciembre de 2003, sin que se llegara a ningún acuerdo sobre la gobernanza de internet[36].

¿Cuál fue la posición de Cuba en la primera fase de la Cumbre Mundial de la Sociedad de la Información en lo que respecta a la seguridad internacional de la información?

La posición de Cuba se expuso en el informe presentado por la delegación cubana titulado, Cuba: Tecnologías de la Información y las Comunicaciones para todos:

> Es inadmisible que instrumentos del desarrollo como las Tecnologías de la Información y la Comunicación (TIC) sean utilizados sin control para producir armas cada vez más letales, incluidas las nucleares. No puede perderse de vista que cada vez más, bajo el pretexto de la lucha contra el terrorismo, se expanden conceptos como vigilancia e inteligencia tecnológicas, que enmascaran el espionaje masivo, quebrantan los derechos civiles, restringen los avances democráticos y reprimen a quienes disienten o se oponen a los designios imperiales.
>
> La comunidad internacional tiene el imperativo ético de detener e invertir la tendencia a la marginación de cientos de millones de personas del disfrute de los beneficios de la globalización y la interdependencia. El establecimiento de un Nuevo Orden Mundial de la Información y la Comunicación no es una aspiración utópica; es una necesidad impostergable para que los países en desarrollo y amplios sectores sociales en los propios países industrializados puedan

[36] Concepto que generalmente se refiere a la administración técnica de los recursos claves de internet a escala mundial, como los nombres de dominio y las direcciones IP. Sin embargo, sus implicaciones son mayores, pues incluye temas de política como la seguridad, la jurisdicción, el multilingüismo y aspectos de infraestructura como el acceso, la conectividad y los costos de interconexión.

enfrentar con éxito los planes de dominación política y cultural, diseñados en los principales centros de poder del capital transnacional[37].

Desde ese momento, el gobierno y las empresas monopólicas de internet de los Estados Unidos y sus aliados se han dedicado a evitar cualquier cambio al *status quo* de la gobernanza de internet que pudiese poner en peligro sus privilegios y preferencias en el dominio de la red de redes.

Estados Unidos evita cualquier cambio al *status quo* de la gobernanza de internet

El Gobierno de los Estados Unidos, sus aliados y las empresas hegemónicas de internet han evitado por todos los medios cualquier cambio al status quo de la gobernanza de internet promovido por la Organización de Naciones Unidas (ONU) y varios países subdesarrollados. ¿Qué sucedió, luego que en la primera fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), celebrada en Ginebra, Suiza, en 2003, no se llegó a acuerdo en el tema de la gobernanza de internet?

Los Estados Unidos y sus aliados no quieren poner en peligro los privilegios que han adquirido en el modelo colonizador predominante del uso de internet, y en el proceso de privatización y de comercialización de internet, así como en la banalización de productos, servicios y contenidos diseñados por sus centros de pensamiento, empresas subordinadas y medios de comunicación capitalistas.

Plantean que los gobiernos y las organizaciones intergubernamentales no deben inmiscuirse en la gobernanza de internet, pues funciona bien bajo las leyes del mercado y conducida por las grandes empresas como *Google, Facebook, Yahoo*, entre otras. Pretenden imponer su hegemonía y favorecer los intereses imperiales en el ciberespacio por encima de los de otros países.

Varias naciones, encabezadas por Rusia y China, realizaron propuestas que han tenido consenso entre los países subdesarrollados; pero

[37] Informe, "Cuba: tecnologías de la Información y las Comunicaciones para todos", presentado en la primera fase de la Cumbre Mundial de la Sociedad de la Información, celebrada en Ginebra, en diciembre de 2003.

los poderosos las han rechazado. Hay que destacar el papel jugado por nuestro país, en particular, la profesionalidad de los funcionarios del Ministerio de Relaciones Exteriores, en los intercambios realizados en diferentes organismos de la ONU.

¿Cuáles son las principales posiciones presentadas en diferentes foros internacionales?

En el año 2004 se creó el Grupo de Trabajo sobre Gobernanza de Internet (GTGI) de las Naciones Unidas para que elaborara un informe sobre el tema a ser presentado en la segunda fase de la CMSI. Propuesto en junio de 2005, recomendó internacionalizar la gobernanza de internet.

Durante la segunda cumbre celebrada en Túnez en 2005, las fuerzas interesadas en mantener el *status quo* en la gobernanza de internet, encabezadas por los Estados Unidos, lograron imponer su posición y evitaron que los documentos finales recogieran las recomendaciones del Grupo de Trabajo.

Las principales posiciones fueron:

- Mantener el estado actual (entidad privada —ICANN— controlada por el Gobierno de los Estados Unidos). Es apoyada por países desarrollados y el sector privado.

- Pasar el control a una organización intergubernamental, por ejemplo, la UIT dentro de la ONU, con participación del sector privado y la sociedad civil. Apoyada por países en desarrollo, liderados por China, Brasil, India y Sudáfrica.

- Pasar el control a una organización multisectorial, donde no solo participen gobiernos sino también, en igualdad de condiciones, el sector privado y la sociedad civil. Apoyada por algunos países y por la sociedad civil.

La Corporación de Internet para la Asignación de Nombres (ICANN) es vista como un sustituto del sector privado para el Gobierno estadounidense, porque actúa bajo licencia y ejecuta las decisiones de la Administración Nacional de Telecomunicaciones e Información (NTIA) del Gobierno de los Estados Unidos.

El 14 de marzo de 2014, la NTIA, subordinada al Departamento de Comercio de los Estados Unidos, anunció que renunciaría a sus responsabilidades en la gestión del sistema de nombres de dominio (DNS) para cumplir con el compromiso de privatización del DNS, realizado en 1998. Se dejó claro que no se aceptaría una propuesta que reemplace el papel de la NTIA con una solución encabezada por un gobierno o una organización intergubernamental.

La asignación de números de internet también es controlada por el Gobierno estadounidense a través de la ICANN, conforme a los términos de un contrato con el Departamento de Comercio de los Estados Unidos. De esta manera realiza la coordinación global de las direcciones IP, en coordinación con los Registros Regionales de Internet (RIR), mantiene la base de datos de nombres de dominio y administra los parámetros de protocolo.

Pronunciamientos de los países subdesarrollados en la Organización de Naciones Unidas, sobre ciberseguridad

Varios países subdesarrollados han promovido desde el año 1998 la discusión de asuntos vinculados con la seguridad de la información en organismos de la Organización de Naciones Unidas (ONU). ¿Qué temas relacionados con la seguridad de la información se pusieron a debate en la ONU y en el Grupo de Expertos Gubernamentales, surgido en 2003?

En 1998, Rusia introdujo en la Primera Comisión de la Asamblea General el proyecto de resolución A/RES/53/70 titulado “Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional”, el que fue adoptado sin ser llevado a votación.

La resolución pedía a los Estados miembros que promovieran el examen multilateral de los peligros actuales y posibles en el ámbito de la seguridad de la información, y los invitaba a que enviaran al secretario general sus opiniones sobre los criterios básicos relacionados con la seguridad de la información y la conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de

información y de telecomunicaciones mundiales, y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información.

En 2003, Rusia pidió al secretario general que preparara un estudio sobre los conceptos internacionales pertinentes, encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones, con la asistencia de un grupo de expertos gubernamentales.

Surgió así el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (GEG).

Ese primer grupo no logró consenso en los temas a debate. Los puntos de desacuerdo fueron el impacto y el uso de las TIC en la seguridad nacional y la esfera militar, y si se debían abordar los contenidos o limitarse solo a la infraestructura. En particular, en este último tema, no hubo acuerdo en si se debía tratar a los contenidos transfronterizos como un asunto de seguridad nacional.

¿Qué papel han jugado los grupos de Expertos Gubernamentales?

Un segundo grupo de Expertos Gubernamentales se estableció en 2009. Este grupo sí logró consensuar un informe sobre los temas sustantivos, recomendando realizar un diálogo sobre las normas para los Estados en el uso de las TIC, para reducir riesgos y proteger infraestructura crítica; adoptar medidas para la creación de confianza y la reducción de riesgos sobre el uso de las TIC por los Estados, incluyendo el intercambio de información sobre el uso de las TIC en los conflictos, intercambiar información sobre la legislación, estrategias, políticas y buenas prácticas nacionales en cuanto a la seguridad de las TIC; realizar acciones de capacitación para los países subdesarrollados y tratar de elaborar términos y definiciones comunes pertinentes en seguridad de las TIC.

En septiembre de 2011, China, Rusia, Tayikistán y Uzbekistán enviaron una carta al secretario general, anexando un Código Internacional de Conducta para la Seguridad de la Información.

En la carta introductoria, los países promotores de esta iniciativa, pidieron que se celebraran deliberaciones internacionales en el marco de las Naciones Unidas sobre tal código internacional, a fin de pro-

mover que se lograra cuanto antes un consenso sobre las normas y reglas internacionales que rijan las actividades de los Estados en el espacio de la información.

El Código de conducta estipulaba que todo Estado que se adhiera de forma voluntaria al mismo se compromete a 11 principios de actuación, entre los que se encuentran: no utilizar las tecnologías de la información y la comunicación, incluso en red, para realizar actividades hostiles o actos de agresión, plantear amenazas a la paz y la seguridad internacionales ni contribuir a la proliferación de armas informáticas o tecnologías conexas.

Con esta propuesta, los países proponentes tomaron la iniciativa de proponer medidas concretas de colaboración en el campo de la ciberseguridad en el ámbito multilateral de las Naciones Unidas.

El informe enviado por el tercer grupo de expertos en 2013 constituyó un paso de avance en relación con el anterior, ya que los expertos acordaron varias cuestiones sobre la pertinencia del derecho internacional en el ciberespacio:

> El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad, y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías.

Otro principio importante que refrendó este informe es el relacionado con la soberanía de los Estados al establecer que:

> La soberanía de los Estados y las normas y principios internacionales que de ella emanen son aplicables a la realización de actividades relacionadas con las tecnologías de la información y la comunicación por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio.

En enero de 2015 fue enviada al Secretario General de la ONU una nueva versión del Código internacional de Conducta para la Seguridad de la Información por los mismos países que la presentaron en 2011.

Según sus autores, la nueva versión tuvo en cuenta las observaciones y sugerencias formuladas por todas las partes. El nuevo texto incorpora la aplicabilidad del derecho internacional al ciberespacio, tal como antes lo había hecho el tercer grupo. También incorpora la

necesidad de elaborar medidas de creación de confianza destinadas a evitar riesgos de conflictos.

Asimismo, reafirma un acuerdo de la Cumbre Mundial sobre la Sociedad de la Información de que todos los Estados deben tener igual cometido y responsabilidad respecto a la gobernanza internacional de internet. Finalmente, reafirma del papel de las Naciones Unidas en el desarrollo de normas jurídicas internacionales para la seguridad de la información y la coordinación entre las organizaciones internacionales pertinentes.

La AGNU en 2013, decidió convocar a un cuarto grupo de Expertos Gubernamentales con la particularidad que añadió a su mandato la manera en que se aplica el derecho internacional al uso de esas tecnologías por los Estados.

El grupo fue extendido a 20. Su informe es más extenso que su predecesor de 2013. Entre las novedades que incluye está la recomendación que un Estado no debería realizar o apoyar de forma deliberada actividades en la esfera de las TIC que dañaran de manera intencionada infraestructuras críticas de otro; los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras críticas fueran objeto de actos malintencionados relacionados con las TIC; llamar la atención sobre la existencia de principios jurídicos internacionales establecidos, entre ellos, de ser aplicables, los principios de humanidad, necesidad, proporcionalidad y distinción y la atribución, o sea, que las acusaciones de organizar y cometer hechos ilícitos dirigidas contra los Estados deberían estar fundamentadas.

El informe se abstuvo de singularizar al artículo 51 de la Carta de las Naciones Unidas, que establece el derecho de los Estados a la legítima defensa en caso de una agresión.

En 2016 Cuba se incorporó al Grupo de Expertos Gubernamentales. ¿Cuáles son los temas planteados por la delegación cubana en estos foros?

La resolución de la AGNU A/70/455 de noviembre de 2015 solicitó al secretario general de la ONU la creación de un quinto grupo de Expertos Gubernamentales para que continúe estudiando estos

asuntos, con miras a promover un entendimiento común de las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, así como la manera en que se aplica el derecho internacional al uso de las tecnologías de la información y la comunicación por los Estados, además de las normas, reglas y principios de comportamiento responsable de los Estados, medidas de fomento de la confianza y creación de capacidad, como también promover el examen de conceptos internacionales encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

En nuestro caso, es imprescindible crear capacidades para preservar la soberanía en el ciberespacio y acceder a tecnologías que permitan alcanzar mayores niveles de ciberseguridad. Yo te diría que dentro de las prioridades está evitar que se aplique directa y totalmente el derecho internacional al ciberespacio, y estudiar la forma de aplicarlo, con regulaciones específicas, vinculantes entre los Estados miembros de la ONU y orientadas a evitar que el ciberespacio se convierta en un campo de batalla. Los países occidentales tienen capacidades ofensivas en este espacio, y así lo han demostrado en varias oportunidades. En particular los Estados Unidos, en su afán de dominación (entre otros países y organizaciones), tienen dentro de su doctrina responder a ciberataques de forma convencional, lo que resulta inaceptable. Por eso, estamos trabajando también en evitar reinterpretaciones nocivas del derecho internacional y la Carta de las Naciones Unidas, contrarias a sus principios y propósitos, que solo conducirán al incremento de los conflictos en el ciberespacio.

VIOLACIONES Y USO INADECUADO DEL ESPECTRO RADIOELÉCTRICO NACIONAL

Afectaciones a la soberanía y a los servicios de telecomunicaciones

El Estado cubano regula el uso y los beneficios de las telecomunicaciones en su territorio, conforme a lo estipulado en el artículo 16 de nuestra Constitución, a la práctica universal y a los convenios internacionales de los que Cuba es parte.

Las violaciones del espectro radioeléctrico[38] *cubano ha sido una práctica del Gobierno de los Estados Unidos desde 1959. ¿Qué impactos tienen estos hechos en la soberanía y los servicios de telecomunicaciones?*

Cuba ha denunciado en diferentes conferencias de radiocomunicaciones, organizadas por la Unión Internacional de Telecomunicaciones (UIT), organismo de la ONU, que los Estados Unidos han violado las normas internacionales en esta materia, al invadir el territorio cubano con frecuencias radioeléctricas enviadas desde su territorio y de otros países, que interfieren frecuencias de radio en ondas medias y FM, que se encuentran en servicio en la Isla.

El Reglamento de Radio Comunicaciones de la UIT, en su disposición 23.3, estipula que las transmisiones de radio en ondas medias deben ser concebidas como "un servicio nacional de buena calidad dentro de los límites del país que se trate". Por ejemplo, lo estipulado en este reglamento confiere un carácter ilegal a las emisiones de *Radio Martí*

[38] Parte del espectro electromagnético en el que sus límites de frecuencias se fijan convencionalmente por debajo de tres mil gigahertz (3000 GHz) y cuyas ondas electromagnéticas se propagan por el espacio sin guía artificial. Constituye un recurso natural limitado, inalienable, imprescriptible e inembargable, cuya propiedad exclusiva es ejercida por el Estado Cubano; que resulta imprescindible para el desarrollo de los modernos sistemas de radiocomunicaciones que integran las redes de telecomunicaciones nacionales e internacionales del país.

en los 1180 kHz, al utilizar esta frecuencia para enviar señales desde los Estados Unidos a Cuba.

Por su parte, las transmisiones de onda corta que realiza esta propia emisora, al utilizar 10 frecuencias, también son ilegales porque el contenido de esas emisiones contraviene lo legislado en la Constitución y Convenio de la UIT, cuando en su preámbulo se afirma que "las transmisiones de onda corta deben facilitar las relaciones pacíficas y la cooperación internacional entre los pueblos".

Además de las emisoras de radio comerciales, se han interferido importantes servicios como el de radionavegación marítima, las comunicaciones por radio de ambulancias y la de radioaficionados.

Pero el colmo de esta locura ha sido el uso de un globo aerostático a tres mil pies de altura, ubicado en un cayo de la Florida, y de un avión militar del tipo EC-130, perteneciente al Comando Solo de una Unidad de Guerra Psicológica de las Fuerzas Armadas de los Estados Unidos, para transmitir señales de radio y *TV Martí* a Cuba.

El despliegue de aviones para transmisiones ilegales constituyó una de las acciones más provocativas y peligrosas, teniendo en cuenta que una medida como esta solo se había tomado con anterioridad durante situaciones de guerra en Vietnam e Irak, y significó una clara violación de la soberanía cubana.

Lo peor es que continúan con esta práctica y cada semana se emiten hacia Cuba más de 1800 horas de programación anticubana, por 13 estaciones de radio en 21 frecuencias.

Recientemente se publicaron en la Gaceta Oficial de la República de Cuba dos resoluciones del Ministerio de Comunicaciones, la No. 98, que norma el empleo de redes de telecomunicaciones inalámbricas de alta velocidad en las bandas de frecuencias de 2.4 GHz y 5 GHz, y la No. 99, que reglamenta el funcionamiento de las redes privadas de datos. ¿Cómo pudiera afectar a la ciberseguridad del país el incumplimiento de algunos de los aspectos reflejados en estas normas?

El asunto estriba en que si no organizamos bien el uso de nuestro espectro radioeléctrico, que por demás es limitado, se pueden producir hechos que inciden en la ciberseguridad.

En los últimos años proliferaron en todo el territorio nacional redes alámbricas e inalámbricas que no han estado sujetas a ninguna norma jurídica. El desarrollo de las telecomunicaciones y la ciberseguridad del país requieren de ese ordenamiento. No se trata de eliminar o restringir servicios, todo lo contrario, ampliarlos, pero apegados al orden necesario para continuar avanzando. Sabemos que en muchas de esas redes se han cometido violaciones de la legalidad, pues se cobran determinados servicios y se han entrado al país equipamientos que por sus características técnicas requieren que el operador solicite una licencia para su explotación, por solo citar dos ejemplos.

Muchas instituciones estatales tienen redes privadas de datos por donde se ofrecen servicios vitales para la economía y la sociedad. Imagínate que se interfieran algunos de los servicios que da un hospital por su red privada: de consulta de algún caso médico o de seguimiento a un paciente postoperado; que se afecten los sistemas ubicados en los puntos de extracción de petróleo que miden los indicadores de este proceso, o los sensores que utiliza la Unión Nacional Eléctrica para medir el estado de los indicadores eléctricos, porque esos servicios usan la frecuencia de 5 GHz.

También se utilizan drones en 2.4 GHz y 5 GHz para diversos fines, incluido la cetrería robótica, que ya operan en dos aeropuertos del país y se va a ampliar a otros. Las afectaciones en el vuelo de uno de estos drones pudiera trascender nuestra frontera y eso hay que evitarlo.

No estamos hablando nada que sea ciencia ficción, son cuestiones reales que pueden acontecer si no somos previsores. Hace poco tiempo una persona instaló en su vivienda un equipo que puso fuera de servicio por varias horas las radio base de la telefonía celular de una cabecera municipal. Por supuesto, las consecuencias en el orden social y económico no se pueden subestimar.

Tampoco podemos olvidar las acciones de agentes encubiertos como Alan Gross, para darle acceso a internet ilegal a organizaciones contrarrevolucionarias de nuestro país.

Así es. Gross recibió medio millón de dólares de la empresa Development Associates International Inc. (DAI), que había logrado un contrato multimillonario con la USAID, agencia del Gobierno estadounidense con un largo historial de acciones subversivas fuera de los

Estados Unidos, con el objetivo supuesto de dar acceso a internet a la comunidad judía en Cuba y "romper el bloqueo informativo impuesto por el Gobierno cubano", mediante innovaciones tecnológicas como conexiones telefónicas, internet por satélite y telefonía celular, que darían servicio a las organizaciones contrarrevolucionarias en Cuba. Reclutó la ayuda de otros judíos estadounidenses para poder traer los equipos electrónicos, pieza por pieza y evitar los controles en los aeropuertos cubanos.

La idea era que la comunicación se transmitiera directamente al satélite, sin pasar por los servidores controlados por el operador cubano. Como es conocido, Alan Gross fue juzgado y condenado a 15 años de prisión y, tras cumplir cinco años de cárcel, fue puesto en libertad el 14 de diciembre de 2014.

No podemos ser ingenuos, el Departamento de Estado de los Estados Unidos creó el 7 de febrero de 2018 una Fuerza de Tarea en internet para Cuba, compuesta por funcionarios gubernamentales y no gubernamentales con el objetivo de "promover el libre flujo de información" y "ampliar el acceso a internet de los medios independientes" en Cuba, en respuesta a lo dispuesto en el Memorando Presidencial de Seguridad Nacional del 16 de junio de 2017, emitido por el presidente Donald Trump. Sabemos que han modelado la posibilidad de crear y potenciar este tipo de redes en Cuba.

En fin, estas dos resoluciones permitirán un uso adecuado del espectro radioeléctrico, fortalecer la ciberseguridad e incrementar los servicios en la red a tono con el objetivo de construir una sociedad de la información y el conocimiento centrada en la persona, en la que todos puedan crear, consultar, utilizar y compartir los contenidos y el conocimiento en la mejora de su calidad de vida.

Violaciones del espectro radioeléctrico de Cuba

Nunca antes en la historia se preparó con tanta meticulosidad y detalle una operación de guerra tecnológica y sicológica, que cuando el Gobierno de los Estados Unidos decidió en la segunda mitad de la década del ochenta, agredir el espectro radioeléctrico de Cuba, enviando señales de televisión con contenidos subversivos. Ya lo hacían desde los años sesenta a través de las ondas radiales.

En esa operación participaron el gobierno, el congreso, las fuerzas armadas y las agencias de inteligencia de ese país. Contrataron empresas tecnológicas y académicos de universidades y centros de investigación, que estudiaron y propusieron las mejores variantes técnicas.

Pero el resultado significó una rotunda derrota del imperialismo estadounidense en el orden tecnológico: a los pocos minutos de salir al aire la señal de TV Martí, el 27 de marzo de 1990, se interfirió, se tapó la señal como decimos los cubanos, y así ha sido durante 30 años.

Todos los esfuerzos se realizaban para llevar la televisión a lugares remotos y no había precedentes en la interferencia al poderío tecnológico de los Estados Unidos. En Cuba, en específico, las inversiones realizadas en la década de los ochenta permitieron extender la televisión a 90 % de la geografía cubana.

Este caso representó un problema de seguridad nacional, pues se intentó agredir el espectro radioeléctrico de Cuba y crear condiciones para una agresión armada, incitando en varios programas a la realización de actos terroristas. Se trataba, como definimos en un libro publicado hace uno años, de aplicar acciones de terrorismo en el éter.

¿Cuáles son los elementos esenciales de la etapa de preparación de la agresión televisiva contra Cuba?

Posterior a la salida de *Radio Martí*, elementos contrarrevolucionarios de origen cubano, protegidos por políticos de la administración Reagan, manifestaron su interés de emitir señales de televisión hacia Cuba.

Como antecedentes técnicos están las emisiones realizadas desde los Estados Unidos hacia Cuba, a partir del 30 de septiembre del año 1954 al 1957, por un avión cubano DC- 3 que sobrevoló a 3000 metros de altura y a una distancia de 80 kilómetros del litoral habanero, para trasmitir como primer programa una serie mundial de béisbol.

En 1962, Edward R. Murrow, entonces director de la Agencia de Información (USIA), trató con el presidente Kennedy la posibilidad de montar un canal de televisión con fines diversionistas hacia Cuba. Su plan consistía en emplear dos aviones DC- 6, a una altura de 18 000 pies, muy próximos a los límites aéreos de nuestra patria, pero el intento fue aplazado por considerarse riesgoso.

Durante el segundo semestre de 1985 circuló por primera vez ante el congreso el proyecto de trasmitir señales de televisión a Cuba. En mayo de 1986 sale a la luz pública por primera vez, el proyecto de *TV Martí*, cuando el representante por la Florida, Lawton Chiles, envió una misiva al director de la USIA promoviendo la idea de agilizar el sistema de televisión hacia Cuba; en ella Chiles señaló: "*TV Martí* facilitará al pueblo cubano otra fuente de información y noticias".

Decisivo fue el año 1988 para los promotores del proyecto subversivo. Contrataron cuatro firmas consultoras ingenieras para efectuar las investigaciones y dos compañías encargadas de los asuntos financieros y jurídicos.

Los estadounidenses, después de haber analizado otras variantes, llegaron a la conclusión que utilizarían un aerostato o globo cautivo, situado en Cudjoe Key, próximo a Cayo Marathon, a una altura de 10 000 pies, donde existían otros medios destinados a los servicios aduaneros de los Estados Unidos.

La señal se originaba en la ciudad de Miami, desde donde se trasladaba a un satélite que a su vez, la hacía llegar a una estación terrena en Cudjoe Key mediante una red de microondas, y de allí hacia un transmisor a bordo del aerostato que emitiría hacia Cuba.

El 1.º de octubre de 1988, la asignación de 7.5 millones de dólares para pruebas de la televisión enemiga se convirtió en ley al ser firmada por Reagan, lo cual representó una cínica violación de las leyes internacionales.

¿Cuáles fueron las variantes técnicas estudiadas por los especialistas estadounidenses para ejecutar la agresión televisiva?

Hay que decir que la contratación de las firmas consultoras para los estudios contó con la participación protagónica de Jorge Más Canosa, presidente de la organización contrarrevolucionaria, Fundación Nacional Cubano Americana (FNCA) y de la Junta Directiva de *Radio Martí*.

Los estudios realizados planteaban cuatro variantes para la transmisión de la eventual *TV Martí*.

1 . Torre transmisora de gran altura.

Las consultoras que realizaron los estudios técnicos concluyeron que instalar una torre de aire de entre 300 y 700 metros de altura en las cercanías de Key West no les proporcionaría señales de la intensidad deseada en La Habana. Estas torres de gran altura presentaban una serie de problemas mecánicos, y la experiencia indicaba que sus probabilidades de supervivencia en caso de huracanes, eran casi nulas.

2 . Barco portador de transmisores de televisión.

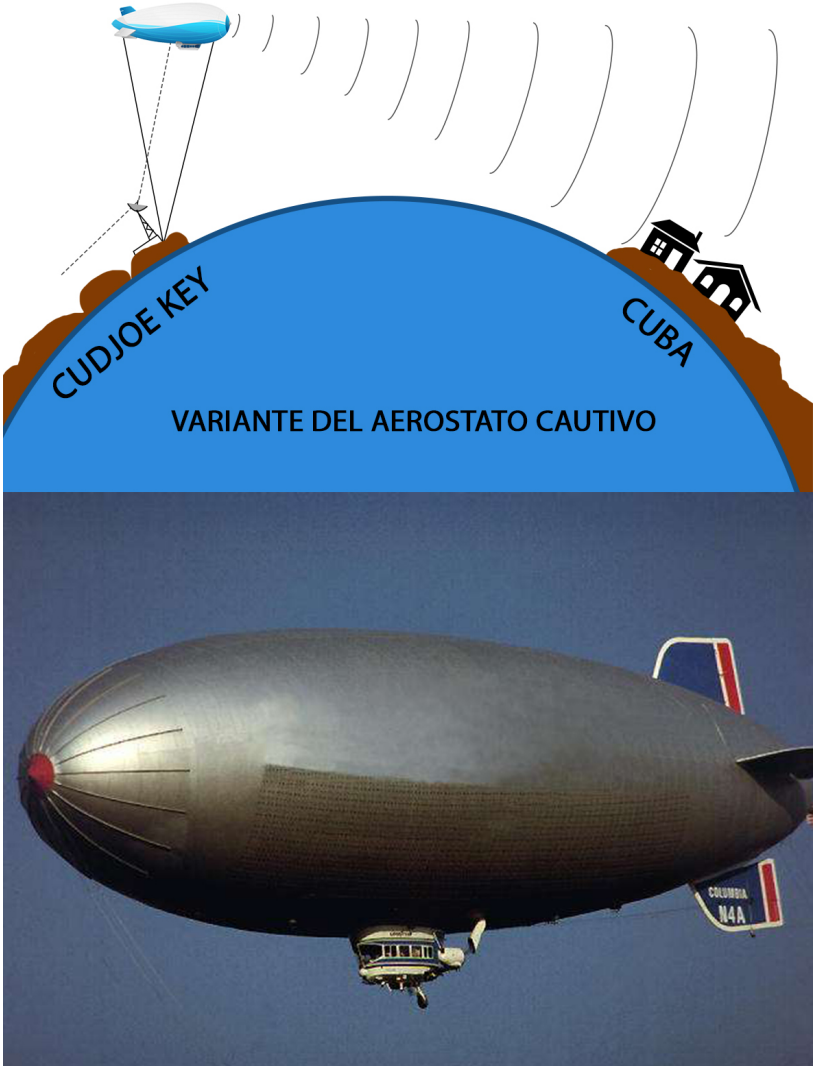
Esta opción tenía como inconvenientes fundamentales que su concreción violaba las leyes y acuerdos internacionales en el campo de las telecomunicaciones, y su continua exposición a la acción de elementos naturales podía entorpecer su funcionamiento debido a las condiciones meteorológicas y a la acción del mar sobre los equipos electrónicos, antenas y líneas de transmisión. Esta alternativa fue descartada casi de inmediato.

3 . Avión portador de transmisores de televisión.

Esta variante recibió mucha atención, debido a que una aeronave relativamente pequeña podía llevar a bordo un transmisor de televisión de mediana potencia y los elementos necesarios para reproducir señales ya grabadas.

Tenía como inconveniente el riesgo para la seguridad de millares de personas, al colocar una aeronave en el espacio aéreo internacional en las cercanías de rutas muy congestionadas, y la flagrante violación de las leyes y acuerdos internacionales sobre telecomunicaciones. También el costo de operación de esta opción era bien alto.

4 . El aerostato o globo cautivo. (Fig. 13).



En los estudios realizados, esta fue la variante más atractiva. El globo o aerostato cautivo, inflado con helio, estaría anclado en una zona militar restringida, en Cudjoe Key, para garantizar su protección. Mediante un cable de acero y cabrestantes, el artefacto podía ser manipulado con variaciones en su altitud desde la superficie hasta más de 4000 metros.

¿Cuándo salió al aire TV Martí y cuál fue su evolución posterior?

Las transmisiones se iniciaron el 27 de marzo de 1990 por el canal 13 de la televisión en VHF, desde el aerostato ubicado a una altura de 10 000 pies sobre el nivel del mar. A los pocos minutos la señal se interfirió.

A finales de 1993, la firma Hammett y Edison, Inc., comenzó a realizar estudios de ingeniería para *La Voz de América*, para evaluar la posibilidad de emplear los canales de televisión en UHF (canales del 14 al 69) en la transmisión hacia Cuba. El 20 de noviembre de 1997 comenzaron a transmitir en UHF, en pocos minutos para sorpresa del Gobierno estadounidense, la señal fue interferida con eficiencia.

Una nueva modalidad de las transmisiones de televisión se produjo el 20 de mayo de 2003, y luego a partir del 21 de agosto de 2004, al emplearse una aeronave militar del tipo EC-130J (Fig. 14), perteneciente al Comando Solo de una Unidad de Guerra Sicológica de las Fuerzas Armadas de los Estados Unidos. Comenzó una vez por semana por espacio de cuatro horas y media, y a partir de agosto de 2006 se realizaron a diario. Una vez más, los técnicos cubanos detuvieron la penetración de la señal televisiva proveniente de un transmisor instalado en aviones.

En julio de 2005, el huracán Dennis desapareció el globo cautivo y a partir de agosto de 2006, las transmisiones se realizaron utilizando un bimotor Gulfstream G-1, alquilado a una empresa aérea.

Estos vuelos se detuvieron en mayo de 2013, tras gastar una cifra considerable de dinero de los contribuyentes estadounidenses. Tales emisiones se sufragaban con un presupuesto aprobado por el Congreso estadounidense, que cada año fiscal preveía más de 30 millones de dólares para las transmisiones contra Cuba.

En septiembre de 2013, *The Washington Post*, publicó una noticia que daba a conocer que el avión utilizado en las transmisiones de la señal de la televisión anticubana se encontraba estacionado en un campo de aviación en la zona rural de Georgia, y se pagaba a un contratista 79 500 dólares al año para su custodia.

Fig. 14. Aeronave militar estadounidense, tipo EC-130J.

El 8 de julio de 2014, el Departamento de Estado anunció que los Estados Unidos finalizaba de manera oficial uno de los programas más ineficaces y muy criticados de la última década destinados a socavar al Gobierno cubano: la transmisión de la mal llamada *TV Martí* desde una aeronave.

En una noticia publicada en la revista *Foreing policy*, se reconocía que desde su lanzamiento el programa se vio afectado por un simple problema: cada día que el avión voló, fue bloqueada su señal de transmisión, lo que significó que los cubanos no podían ver los programas de televisión.

De esta manera se reconocía la derrota en el campo tecnológico del imperialismo yanqui que ya cumple 30 años.

Cuando Cuba humilló tecnológicamente a los Estados Unidos

Casi dos meses antes de que se pusiera en el éter la señal de TV Martí, ya estaban creadas las condiciones técnicas para enfrentar esta agresión. La respuesta cubana fue contundente, gracias a la pericia de ingenieros y técnicos cubanos que diseñaron, desarrollaron, construyeron y pusieron a punto los equipos, para lograr una interferencia efectiva, y así, propinarle una sonada derrota en el orden tecnológico al imperialismo yanqui, que en esos momentos festejaba el inminente desmerengamiento de la Unión Soviética y el campo socialista de Europa del Este.

¿Cuándo la parte cubana comenzó a tomar medidas para defenderse de la teleagresión?

Recordemos que los representantes estadounidenses Daniel Mica, Dante Fascell, Bill Nelson, Claude Pepper y Lawrence Smith, presentaron en 1987 una resolución concurrente ante el Comité de Relaciones Exteriores de la Cámara, con el objetivo de obtener 100 000 dólares para realizar estudios dirigidos a la teleagresión, la que fue aprobada poco después por el subcomité de Apropiaciones del Senado. Desde entonces, corrían rumores de estos preparativos.

Por nuestra parte, a principios de 1988 comenzó el monitoreo y observación de las señales de televisión del Sur de la Florida las 24 horas del día, y la búsqueda de información sobre compras de estaciones de televisión en nuestra área geográfica. Esto se mantuvo durante varios meses, tiempo que se aprovechó para adquirir más tecnologías y personal para cubrir los turnos de trabajo. Había canales como el 23, el 41 y uno con programación religiosa que eran los de mejor recepción.

En paralelo, se creó un grupo técnico con expertos de la Universidad Tecnológica de La Habana (CUJAE), del Ministerio de Comunicaciones, el Instituto Cubano de Radio y Televisión y de los Órganos de la Defensa.

¿Qué objetivos se trazó el grupo técnico?

Al principio no había ninguna información sobre las variantes que utilizarían, la posible frecuencia por donde transmitirían, nivel de señal ni el emplazamiento que usarían. Entonces, el grupo técnico tenía la misión de realizar análisis de las posibilidades del enemigo, de nuestras posibilidades de respuesta y estudios de propagación.

Nuestros especialistas, experimentados en producir señales de radiodifusión, tenían ante sí la paradójica tarea de diseñar o inventar un dispositivo para anular una televisión cuyas características desde el punto de vista técnico, eran por demás desconocidas. A estas complejidades se sumaba el hecho de que todo esto había que hacerlo con el mínimo de recursos, de manera que resultara en esos términos racional y no significara una contradicción con las limitaciones y los esfuerzos que se realizaban para mantener en el aire nuestra propia televisión.

¿Cómo fue posible que nuestros cálculos se acercaran hasta casi coincidir con la variante elegida por los estadounidenses?

Fue necesario considerar todas las opciones y variantes técnicas que podían imponernos, debido al alto nivel de secreto mantenido por los estadounidenses, sobre los elementos básicos del proyecto.

Ingenieros y expertos (Fig. 15) en diferentes momentos de un trabajo que se caracterizó por su alto rigor científico, fueron ponentes de distintas variantes que ayudaron a frustrar la agresión y preservar la soberanía de la patria.

No hubo una sola variante que no fuera explorada y cualquier idea, por insólita que pudiera parecer, fue examinada. El país fue obligado a prepararse para diversas alternativas, responder en cualquier canal y en cualquiera de las bandas. Esta circunstancia, naturalmente lo hizo todo más complicado, los estadounidenses aprovecharon todas las ventajas de que dispone el agresor, eligieron el canal, el día y la hora, las variables técnicas, todo con absoluta discreción.

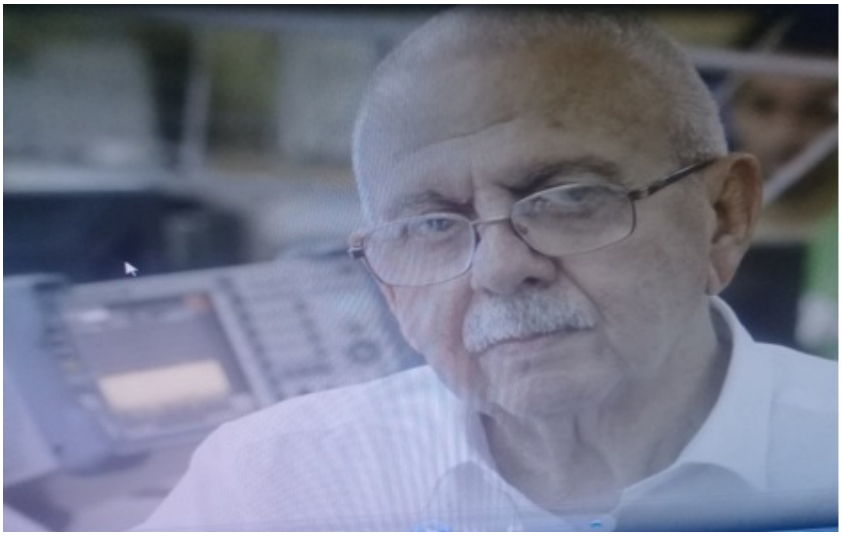


Fig. 15. Profesor Francisco Marante Rizo, miembro del grupo técnico que realizó los estudios para defender el espectro radioeléctrico cubano. Foto tomada del programa de televisión *La pupila asombrada*.

Los técnicos cubanos (Fig. 16) fueron dilucidando las intenciones del enemigo, y los cálculos se aproximaron hasta casi coincidir con los realizados por los ingenieros estadounidenses. Jamás nuestro país había enfrentado un reto semejante, talento contra talento, los ingenieros cubanos salieron vencedores.

Se hizo una prueba con un transmisor instalado en un lugar alto de La Habana, se ponía una película 15 minutos, y se estudiaba la cobertura en todos los municipios de la capital. Participaron alrededor de 60 personas. También se hicieron estudios en todas las zonas desde Pinar del Río hasta Matanzas, para definir dónde instalar los equipos de interferencia y sus características técnicas.

En el momento en que estaban identificadas las cuatro opciones posibles, se llegó a la conclusión, a través de rigurosos estudios y análisis científicos, que la variante más probable era el globo aerostático, pues era la alternativa que podía poner mayor nivel de señal en Cuba.

Se investigó todo sobre el funcionamiento de estos artefactos y así descubrieron una señal que al batirse con la señal original en un punto determinado del espectro, producía un efecto que rompía el sincronismo, destruía la información, y la imagen no se veía.

Posteriormente, se diseñaron y fabricaron los equipos de interferencia, se realizaron los trabajos de instalación y montaje en los puntos definidos con la cooperación de varias empresas del Ministerio de Comunicaciones.

Fig. 16. Los ingenieros Julio Ortega, Elio Borges y Sócrates Rojas (de derecha a izquierda), participantes directos en el enfrentamiento a la teleagresión. Foto tomada del periódico *Trabajadores*, 30 de marzo de 1990.

El día en que salió por primera vez la señal enemiga, fue detectada en el centro de monitoreo y exploración, y desde el puesto de mando se dio la señal para conectar los equipos de interferencia; todo esto se realizaba por voz vía radio en forma cifrada. Por cierto, comenzaron transmitiendo de 3:30 a 6:00 a.m., porque era el horario en que los transmisores cubanos estaban apagados.

Día tras día, durante las 24 horas, se mantenía un hombre en cada punto o instalación esperando por la señal emitida desde el puesto de mando para conectar los equipos de interferencia.

Los técnicos del Ministerio de Comunicaciones desarrollaron entonces un equipo al que llamaron de modo muy jocoso “Libertador”, por aquello de liberar a los compañeros que se encontraban en los puntos, después se bautizó con el nombre de Bolívar. De esta forma

se logró que automáticamente, vía radio se conectaran los equipos de los puntos.

En materia de inversiones, se han calculado los costos en una relación aproximada de uno a mil. Es decir, por cada millón gastado por los estadounidenses en la teleagresión, Cuba invirtió mil dólares. Muchos trabajos se realizaron recuperando equipos, otros fueron diseñados con múltiples propósitos y los gastos de proyectos y salarios fueron mínimos.

En los primeros momentos, como ya expliqué, la gestión de interferencia se realizó en condiciones de campaña. Después, cuando se conocieron todos los parámetros de funcionamiento de la señal enemiga, la interferencia se hacía en régimen automático, disminuyendo mucho los costos de mantenimiento, energía y operación.

El 20 de noviembre de 1997 surge una nueva escalada del enemigo al comenzar sus transmisiones en la banda de UHF, y de nuevo se dio una respuesta contundente al evitar en pocos minutos la penetración de la señal enemiga; en esta oportunidad, también con una nueva técnica desarrollada por el Ministerio de Comunicaciones. Cambiaron en varias oportunidades de canal con el objetivo de sorprendernos, siendo en vano dicho propósito.

El 20 de mayo de 2002, el enemigo intentó de nuevo sorprendernos y cambió el horario de transmisión para uno de mayor teleaudiencia, de 03.30-06.00 a 18.00-22.30; pero se quedaron en el intento, los especialistas y técnicos siempre atentos en la primera línea de combate, no permitieron que se recibiera ni un minuto la señal.

¿Y desde el punto de vista mediático qué medidas se adoptaron?

Se hizo una gran campaña internacional y nacional, casi al nivel del bloqueo. Se realizaron debates en los centros laborales y estudiantiles; y con extranjeros que visitaban el país. (Fig. 17).

Funcionarios cubanos visitaron los Estados Unidos y se reunieron con directivos y periodistas de medios de prensa de ese país; les explicaron las consecuencias que provocarían las transmisiones de televisión contra Cuba.

En ocasión de la visita de Mijail Gorbachov a Cuba, en abril de 1989, varias televisoras estadounidenses que cubrieron este acontecimiento, recibieron información sobre el proyecto de televisión anticubano, sus implicaciones para la soberanía nacional y el espectro radioeléctrico de Cuba. Participaron los periodistas Dan Rather de CBS, Tom Brokan de NBC y Peter Jennins de ABC, entre otros.

En los Juegos Panamericanos, celebrados en La Habana en agosto de 1991, también se les explicó a las cadenas de televisión de los Estados Unidos que vinieron a cubrir el evento.

Se hicieron grupos de trabajo para recorrer con la prensa extranjera las provincias desde Pinar del Río hasta Matanzas, con el objetivo de demostrarles que *TV Martí* no se veía y demostrar que Cuba había ganado el enfrentamiento.

La juventud cubana debe conocer que el proyecto de *TV Martí* puso muy tensas las relaciones con los Estados Unidos. Hubo amenazas de bombardear los puntos de interferencia y se llevaron a cabo actos de guerra, cuando en agosto de 2004 (como ya se dijo) comenzaron a transmitir desde una aeronave militar del tipo EC-130J, perteneciente al Comando Solo de una Unidad de Guerra Sicológica de las Fuerzas Armadas de los Estados Unidos, señal que por demás, también fue interferida.

A un plan obedece nuestro enemigo: el de enconarnos, dispersarnos, dividirnos, ahogarnos. Por eso obedecemos nosotros a otro plan: enseñarnos en la nuestra altura, apretarnos, juntarnos, burlarlo

Un Girón electrónico

Fig. 17. Editorial del 29 de marzo de 1990 en el periódico *Granma*: “Talento contra talento nuestros profesionales enfrentaron con decoro el desafío y por esta vez sus antagonistas de la General Electric, la NASA y el ejército de los Estados Unidos, comprometidos en esta aventura, mordieron el polvo. Son hechos, y ellos revelan que la CUJAE puede emular ventajosamente con Harvard o Massachusetts”.

El derecho internacional y la televisión jamás vista

La agresión televisiva contra nuestro país, iniciada el 27 de marzo de 1990, se enmarca dentro del largo proceso del diferendo histórico mantenido entre los Estados Unidos y Cuba.

En la década del sesenta, la Agencia Central de Inteligencia (CIA), montó un andamiaje propagandístico y desinformativo con fines contrarrevolucionarios, abriendo así un vasto frente de agresión contra Cuba que se mantiene en nuestros días.

Basta decir que en los últimos 60 años han transmitido contra Cuba más de 120 estaciones de radio y televisión, patrocinadas por más de 40 organizaciones contrarrevolucionarias, que han utilizado como promedio más de 20 frecuencias con más de 2000 horas semanales.

En este contexto se ha destacado la mal llamada TV Martí, perteneciente al Gobierno de los Estados Unidos que, transmitiendo en diferentes canales y por diferentes vías, ha violado numerosas normas jurídicas y del derecho internacional e intentado lesionar la soberanía de nuestro país sobre el espectro radioeléctrico, que es un recurso limitado.

¿Cuáles son las regulaciones internacionales sobre la televisión que violó la operación de guerra tecnológica y sicológica, denominada TV Martí?

Lo primero es que, en diferentes zonas, a distintas horas, de modo regular y esporádico, en nuestro país es posible captar varias emisoras radiales de los Estados Unidos, Centroamérica, México, las Antillas, así como las grandes plantas de todo el mundo que se dedican, en ondas cortas, a la radiodifusión internacional. En determinadas condiciones de propagación, la televisión de los Estados Unidos es visible en nuestra costa norte. Cuba nunca ha actuado, ni actuará contra ninguna de esas plantas que operan de forma legal.

Para nosotros la radio extranjera y la agresión radial y televisiva son conceptos en esencia, distintos.

Otra cosa es la televisión anticubana, que es una estación doméstica estadounidense, convertida en una estación internacional. No se trató de un desbordamiento de la señal de televisión generada en un Estado que afecta las televisiones de otros países vecinos o fronterizos, sino de un acto deliberado de transmitir hacia otro país contra la voluntad de este, constituyendo un acto grosero de intervención. (Fig. 18).

En el colmo del cinismo, algunos personeros del Gobierno de los Estados Unidos alegaron que no había regulación específica internacional sobre la emisión de señales de televisión internacional y que podían emitir señales contra Cuba.

Las regulaciones internacionales sobre la televisión se encuentran en el mismo marco regulador de las trasmisiones por radio de ondas medias y FM, siendo el tratado de mayor jerarquía internacional la Constitución y el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT). Dicho reglamento define las telecomunicaciones como: toda trasmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos. La radiocomunicación es toda telecomunicación trasmitida por medio de las ondas radioeléctricas.

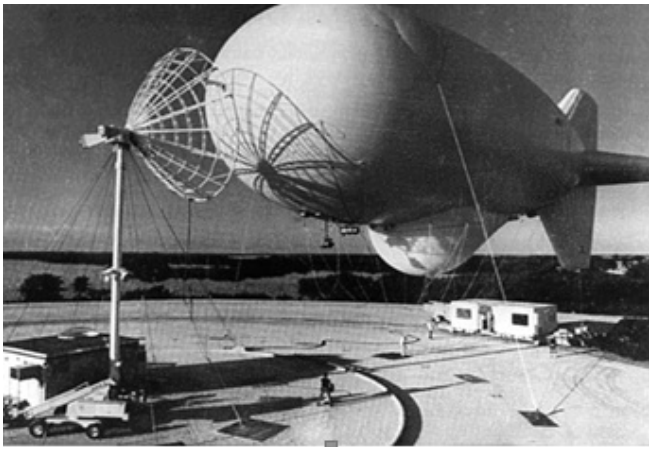


Fig. 18. Variante para ejecutar la agresión televisiva. Foto tomada del libro *Terrorismo en el éter* del autor.

La transmisión de la *TV Martí* contra Cuba desde territorio estadounidense es ilegal, por cuanto el preámbulo de la Constitución de la UIT dice que cada país tiene el derecho soberano a reglamentar sus comunicaciones; y Cuba, sobre la base de ese derecho, dispone de sus canales de televisión. Por tanto, todos los canales de VHF del 2 al 13 de la Televisión Cubana estaban real o potencialmente ocupados por estaciones televisivas cubanas, y por cualquiera de estos canales que saliera la estación, se estarían interfiriendo las trasmisiones y el derecho cubano a reglamentar su espectro.

Pero en las bandas de ondas medias, FM y de televisión, también se violenta el numeral 23.3, del Reglamento de Radiocomunicaciones de la UIT, aplicable a la señal de televisión cuya potencia debe ser regulada para no traspasar la frontera nacional.

¿Qué otras normas del derecho internacional se violaron con la agresión televisiva contra Cuba?

Además de las citadas, la agresión televisiva contra Cuba se contrapone a numerosas normas del derecho internacional. Se violaron en particular, los principios básicos internacionales de la igualdad soberana de los Estados y de la no intromisión en los asuntos internos, como aparecen en la Carta de las Naciones Unidas y en numerosos convenios internacionales; la obligación jurídica internacional para el desarrollo de buenas relaciones amistosas entre vecinos, en el interés del mantenimiento de la paz mundial y la seguridad internacional.

El artículo 1, párrafo 2, de la Carta, establece como objetivo “desarrollar relaciones amistosas entre las naciones, basadas en el respeto del principio de igualdad de derechos y del derecho de autodeterminación de los pueblos”. La instalación de una estación televisiva con un fin subversivo es una transgresión del propósito de desarrollar “relaciones amistosas”.

La televisión contra Cuba debe ser considerada también una violación del principio de “igualdad soberana”, mencionado en el artículo 2, párrafo 1. Los programas de esta estación tienen el claro objetivo de cercenar la soberanía de Cuba. (Fig. 19).

Por otro lado, el tratado del 27 de enero de 1967 sobre el espacio cósmico, al cual pertenecen tanto los Estados Unidos como Cuba, obliga a los Estados a "dirigir el empleo del espacio cósmico al bienestar de todos los pueblos, sin hacer distinción a su desarrollo económico o científico" y "a fomentar la comprensión mutua", así como contribuir a la consolidación de las relaciones amistosas entre los Estados y pueblos.

Denuncia ante la UNESCO

Cuba no permitirá la violación impune de su soberanía nacional

PARIS, 29 de marzo (PL).— La delegación permanente de Cuba ante la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) denunció aquí la agresión televisiva de Estados Unidos contra su país.

La representación diplomática remitió a todas las delegaciones permanentes acreditadas ante esa institución y a su director general, Federico Mayor, una carta de la Comisión Cubana de la UNESCO que denuncian el inicio de las pruebas de la denominada Tele Martí.

En esa comunicación se destacan los propósitos subversivos y la usurpación del canal del espectro radioelectrónico de Cuba, así como la violación por Washington de la Convención de Nairobi de 1982 y de la resolución de la UNESCO de 1978 sobre los medios masivos de comunicación.

Reitera que Cuba no permitirá la violación impune de su soberanía nacional ni que se intente imponerle unilateralmente una programación no autorizada por el Gobierno cubano y con el declarado propósito de propaganda hostil a ese país.

Asimismo, pide al director general que a tenor de lo establecido en las resoluciones mencionadas, exija al Gobierno de Estados Unidos el cese inmediato de esas trasmisiones ilegales.

Angola

Desafío a normas del derecho internacional

LUANDA, 29 de marzo (PL).— La salida al aire de un canal televisivo estadounidense dirigido contra Cuba constituye un desafío a la legislación internacional en materia de telecomunicaciones, afirma el diario *Jornal de Angola*.

El periódico se hace eco de declaraciones del Gobierno cubano sobre el inicio, la madrugada del martes último, de las pruebas de la llamada TV-Martí, en idioma español, emitida hacia la isla caribeña e interferida inmediatamente.

La publicación inserta también declaraciones de diversas personalidades y funcionarios oficiales de otros países, según las cuales la nueva agresión norteamericana agudiza aún más las tensiones entre ambos Estados.

El cotidiano además califica el hecho de "guerra ideológica y acción injerencista sin precedentes.

Denuncia China intervención norteamericana contra Cuba

PEKÍN, 29 de marzo (PL).— China denunció la intervención de Estados Unidos contra Cuba por medio de transmisiones televisivas y radiales y la calificó de acto de perturbación, agresión y salvajismo.

El diario *Renmin Ribao*, órgano oficial del Partido Comunista Chino, condenó enérgicamente esos hechos, que consideró una intervención grosera, violatoria de estipulaciones y tratados de las Naciones Unidas sobre las comunicaciones aeroespaciales y nueva arremetida de Washington para llevar la subversión a los países socialistas.

A solo 90 millas de Estados Unidos, señaló, y después de 31 años de hostilidad, bloqueo y aislamiento, Cuba nunca se someterá. Si las agresiones militares y económicas no pudieron doblegarla tampoco la agresión por telecondas tendrá resultado, afirmó.

El comentario, tras recomendar a Estados Unidos desistir del empeño, recuerda que no es la primera penetración subversiva organizada contra Cuba por Washington, cuyas transmisiones radiales abarcaron desde 1960 a la contrarevolución y en 1985 tomaron un nuevo nivel en la guerra psicológica, mediante rumores y calumnias.

Ahora, con apoyo de su alta tecnología y el poder del dinero, utilizan la televisión para penetrar y subvertir a un país soberano y como con la llamada Radio Martí insultan la sensibilidad nacional.

El comentario enumera las agresiones antecubanas de la Agencia Central de Inteligencia (CIA) de Estados Unidos, desde las comunicaciones radiales hasta su apoyo a la invasión mercenaria de Playa Girón en 1961.

Actualmente, dice, suman 60 horas diarias la emisión de programas de diversas emisoras de radio de Estados Unidos contra Cuba.

Fig. 19. Denuncia ante la UNESCO de la agresión televisiva contra Cuba.

Violaron también, la prohibición de la propaganda de guerra, reflejado en la Resolución 110 de la ONU, del 3 de noviembre de 1947. Esta prohibición, ratificada en la Convención de la ONU de 1966, sobre los derechos humanos, como un principio del derecho internacional, obliga a los Estados a tomar las precauciones necesarias a nivel nacional y excluir la posibilidad de la propaganda de guerra, dictando para ello las leyes correspondientes.

Se debe hacer alusión también en este contexto a la Resolución 37/92, del 10 de diciembre de 1982, sobre la regulación del empleo de satélites artificiales de la tierra para la transmisión televisiva directa internacional por parte de los Estados.

Los artículos 6, 10, 13 y 14 de esta resolución exhortan a los Estados a "colaborar" con el Estado receptor y, en caso de iniciar transmisiones televisivas directas hacia otros Estados, insta a comenzar "reuniones" y a firmar los "convenios" respectivos. Los Estados Unidos no buscaron la colaboración con Cuba y mucho menos realizaron las reuniones correspondientes. No se firmó en ningún momento un convenio.

El Gobierno yanqui también desconoció a la declaración de la UNESCO del 28 de noviembre de 1978, sobre los principios básicos en relación con la contribución de los medios de difusión masiva a la consolidación de la paz y a la comprensión internacional, aprobada de forma unánime por la Vigésima Conferencia General de la UNESCO.

Cuba ha denunciado estos actos ilegales en el marco de diversos escenarios multilaterales y en el orden bilateral, y ha emprendido medidas político-diplomáticas con dicho fin.

Una guerra electrónica entre David y Goliat

Salvando la distancia geográfica y en tiempo, las operaciones de los Estados Unidos contra Venezuela, me recuerda lo acontecido hace 30 años cuando el Gobierno estadounidense lanzó al éter la mal llamada Televisión Martí, con el objetivo de agredir la soberanía y seguridad nacional de Cuba y aplastar la Revolución. ¿Qué opinión le merece esta situación?

El 3 de abril de 1990, en conferencia de prensa ofrecida por el Comandante en Jefe, Fidel Castro Ruz sobre la televisión anticubana, a la que asistieron 246 periodistas procedentes de todas partes del mundo, de ellos 53 representantes de 22 órganos de la prensa estadounidense, varios corresponsales se interesaron por conocer si la teleagresión podría devenir en un asunto militar, y la probabilidad de que los Estados Unidos realizara una operación militar aérea quirúrgica contra las torres que producían la interferencia a *TV Martí*. La respuesta de Fidel fue la siguiente:

> Cuando se inicia una aventura como esta, cuando se llevan a cabo actos violatorios de la ley internacional, cuando se produce una agre-

> sión contra un país soberano, como ha ocurrido en este caso, cualquier cosa puede pasar. Incluso, cuando nosotros vemos lo absurdo de todo esto, hemos pensado, a veces, que tal vez los Estados Unidos estén buscando algunos pretextos para llevar a cabo una confrontación militar contra Cuba […].
>
> […] No estamos en condiciones de asegurar cuáles son las intenciones verdaderas de los Estados Unidos, pero, de todas formas, eso no nos intimida. No será fácil para los Estados Unidos doblegar a Cuba; no será fácil que nos pueda imponer por la fuerza algo que está contra la voluntad de nuestro país, y no será fácil llevar adelante aventuras de tipo militar contra nuestra patria […].
>
> […] Nosotros trataríamos, en ese caso, de que el "cirujano" salga lo peor parado posible, pague su precio por eso; porque hacer cirugía no es tan fácil, agarrar un tigre con la mano no es tan fácil. Sé que tienen tecnología y tienen muchas cosas, pero nosotros tenemos otras, sobre todo, de tipo moral; en especial, que no les tenemos ningún miedo y, sobre todo, porque estamos dispuestos a enfrentar la lucha en cualquier terreno. No te creas que con nosotros se puede estar jugueteando a eso, a estar haciendo operaciones quirúrgicas, porque nosotros podemos hacer también operaciones quirúrgicas en un terreno o en otro.
>
> […] Permíteme decirte que cualquier agresión a Cuba se puede convertir en un problema más serio, mucho más complicado, se puede convertir en una guerra. Así que realizar operaciones de ese tipo contra nuestro país, nadie sabe las consecuencias que pueda tener, nosotros no nos vamos a quedar con los brazos cruzados, porque tenemos imaginación y sabremos responder golpe por golpe, donde hay que golpear y en el momento que hay que golpear. De eso no le quepa duda a nadie. Así que espero que se aconsejen bien antes de que empiecen a querer hacer alardes tecnológicos aquí. A lo mejor vienen con sus aviones invisibles, y nosotros podemos hacer otras cosas invisibles también. Y ahora que ellos interpreten lo que quieran […].

En relación al insulto al honor del país, que representó nombrar a la televisión enemiga, José Martí, el líder de la Revolución Cubana argumentó:

> Es que no hemos mencionado lo que significa el hecho de que le pongan el nombre de Martí a ese grosero instrumento de subversión y desestabilización: primero, porque se ignora quién era Martí […].

[…] El primero que empezó a hablar del imperio desde finales del siglo pasado fue Martí, antes que Lenin. Martí calificó al imperio naciente de los Estados Unidos como un monstruo que conocía bien, porque había vivido en sus entrañas. Y escogen el nombre de quien dijo, en víspera de su muerte en combate, que todo lo que hizo y haría, era para impedir con la independencia de Cuba que los Estados Unidos se extendiera con una fuerza más sobre los pueblos de América, escogen ese nombre para bautizar esa porquería, en el momento en que nosotros somos una trinchera, ¡la primera trinchera que defiende la soberanía de América Latina!

[…] Además, para que los norteamericanos lo entiendan bien, es como si nosotros buscamos un prostíbulo en un lugar del mundo y le ponemos el nombre de George Washington, o un basurero aquí en La Habana y le ponemos el nombre de George Washington o de algún personaje histórico de los Estados Unidos. Eso es lo que han hecho, no se dan cuenta, son brutos, son imbéciles y no se percatan de lo que eso irrita al pueblo […].

Sobre la guerra electrónica impuesta a Cuba por el Gobierno de los Estados Unidos y su repercusión, Fidel explicaría:

[…] Nosotros lo que reclamamos es el derecho a transmitir por radio a todo el territorio de los Estados Unidos. Nos parece un derecho elemental, nos parece un derecho recíproco al que los Estados Unidos se ha tomado con relación a Cuba.

[…] Ahora, nosotros no tenemos la culpa de ser una isla pequeña, ni tenemos la culpa de que los Estados Unidos sean tan grande. No tenemos la culpa tampoco de este problema, no lo hemos creado nosotros, ni tenemos responsabilidad por la estructura del sistema radial norteamericano; pero ya se está agotando el argumento de que no hay posibilidades técnicas de resolver ese problema.

[…] En un tiempo se estuvo discutiendo con el Gobierno de los Estados Unidos la solución, porque nosotros decíamos: “Transmitan, pero nosotros también queremos transmitir”. Los Estados Unidos no han seguido discutiendo, los Estados Unidos no han querido resolver ese problema, y no podemos renunciar a nuestro derecho a transmitir a todo el territorio de los Estados Unidos […].

[…] Hemos tenido paciencia, hemos esperado cinco años y no vemos por parte de los Estados Unidos ninguna voluntad de resolver el problema, sino la de crear nuevos problemas y nuevos conflictos. Esa es la realidad que tenemos con esto, para una televisión, además,

> que no se ve. Pero nosotros, incluso, hemos calculado que puede en un momento llegar a verse; no sé qué medios técnicos se puedan inventar para que se vea a la fuerza. Tenemos calculadas también las distintas respuestas a cada una de las situaciones.
>
> […] Digo que es una tontería. En realidad, los Estados Unidos no tenían ninguna necesidad de enfrascarse en esta ingloriosa acción; no le veo todavía lógica a incurrir en esta violación de la ley internacional. Ciertamente, en este caso no estamos defendiendo solo el derecho de Cuba; son decenas de países, muchos países, la inmensa mayoría del mundo, los que no están de acuerdo con esto, y no están de acuerdo porque ningún país se resigna fácilmente a aceptar la idea de que venga una gran potencia y desde un satélite, desde un globo, desde un zepelín, desde un avión, desde un barco, desde cualquier lugar le imponga las transmisiones de televisión.
>
> […] En este caso, nosotros no solo estamos defendiendo el derecho de Cuba: esta es la guerra de David contra Goliat, una vez más; una guerra electrónica ahora entre David y Goliat, en que realmente David está demostrando tener mucha más inteligencia que Goliat. Me explico por qué Goliat, ese personaje bíblico, fue derrotado: por bruto […].

Han pasado 30 años y mientras que Cuba se enfrenta hoy a la pandemia del coronavirus y expresa con hechos concretos la vocación humanista y solidaria de la Revolución, la diplomacia de guerra de los Estados Unidos ha decidido profundizar su guerra no convencional y asimétrica, el bloqueo y las sanciones contra Cuba, Venezuela y otros gobiernos de izquierda.

Recordar las ideas expuestas por Fidel aquel 3 de abril de 1990, nos fortalece, en el empeño de salvaguardar la seguridad y soberanía del país, en particular, en el orden tecnológico y comunicacional, y nos pone a pensar en cómo usar en la actualidad, no solo los canales de la radiodifusión, sino también la internet y las redes sociales digitales, en esos propósitos.

Bibliografía consultada

Asamblea General de Las Naciones Unidas: Informe sobre la "necesidad de poner fin al bloqueo económico, comercial y financiero impuesto por los Estados Unidos de América contra Cuba", en los años 2010-2019. Disponible en www.minrex.gob.cu

Castro Ruz, Fidel (1988): Discurso en la clausura del III Encuentro Continental de Mujeres, La Habana, 7 de octubre. *Granma*, 12 de octubre de 1988, p. 5.

_____ (1990): Conferencia de prensa ofrecida sobre la televisión anticubana, 3 de abril.

_____ (2007): "Mentiras deliberadas, muertes extrañas y agresión a la economía mundial", 18 de septiembre, *Granma Digital*.

Castro Ruz, Raúl (2015): Discurso en la VII Cumbre de las Américas, Panamá, 11 de abril. Disponible en www.cubaahora.cu.

Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2): "Estudio sobre fuerza de trabajo en ciberseguridad", 6 de noviembre de 2018. Disponible en www.isc2.org

Cumbre Mundial de la Sociedad de la Información: Informe presentado en la primera fase, Cuba: Tecnologías de la Información y las Comunicaciones para todos, Ginebra, diciembre de 2003.

Domínguez, L. Eduardo: "Segurmática Antivirus, en defensa del Ciberespacio Nacional", 3 de septiembre de 2019. Disponible en www.cubadebate.cu

Editorial del Periódico Granma: "Un Girón electrónico", 29 de marzo de 1990.

Empresa de Consultoría y Seguridad Informática, Segurmática: Informe de balance de 2019.

Fernández González, Juan Antonio (2012): "La crisis de octubre y el secreto mejor guardado de internet", 10 de octubre. Disponible en lapupilainsomne.wordpress.com

Fundación George W. Bush (2010): Conferencia sobre ciberdisidencia en el SouthernMedhodist de la Universidad de Dallas, Texas, 19 de abril. Disponible en http://georgewbushinstitute.com/the-conference-on-cyber-dissidents-global-successes-and-challenges/

Gaceta Oficial No. 45 Ordinaria: Decreto-Ley No. 370/2018, sobre La informatización de la sociedad en Cuba, 4 de julio de 2019.

_____: Decreto No. 360/2019, sobre La Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, 4 de julio de 2019.

García Pierrat, Gonzalo (2014): *Administración de incidentes de seguridad informática* [s.n.].

González-Manet, Enrique (1987): *La guerra oculta de la información*, Ed. Ciencias Sociales, p. 27, La Habana, Cuba.

Guadis Salazar, Edgar (2015): "Evolución de los programas malignos desarrollados en Cuba o para Cuba", Rev. *Tino* n.º 46, 27 de octubre.

Marante Rizo, Francisco (2020): Entrevista concedida para el programa de televisión La Pupila Asombrada, 26 de marzo. Disponible en www.tvcubana.icrt.cu

Ministerio de Comunicaciones de Cuba: Resolución No. 98/2019. Reglamento para el empleo de redes de telecomunicaciones inalámbricas de alta velocidad en las bandas de frecuencias de 2.4 GHz y 5 GHz, *Gaceta Oficial de la República de Cuba*, n.º 39 Ordinaria, 29/5/2019. Disponible en www.gacetaoficial.gob.cu

Ministerio de Comunicaciones de Cuba: Resolución No. 99/2019. Reglamento para las redes privadas de datos, *Gaceta Oficial de la República de Cuba*, n.º 39 Ordinaria, 29/5/2019. Disponible en www.gacetaoficial.gob.cu

Ministerio de Comunicaciones de Cuba: Informe sobre el estado del subprograma de ciberseguridad, enero de 2021.

Misión Verdad: "Venezuela bajo ataque: 7 apuntes sobre el shock eléctrico", 11/3/2019. Disponible en misionverdad.com

Oficina de Seguridad de las Redes Informáticas (OSRI): Informe de balance del año 2019.

Pérez Salomón, Omar: *Terrorismo en el éter*, Ed. Política, La Habana, Cuba, 2007.

_____ (2014): "La guerra cibernética made in USA y el ladrón que grita ¡ataja!", 30 de mayo. Disponible en www.lapupilainsomne.com

Sánchez Espinosa, Iroel (2013): "A la luz plan secreto del Gobierno estadounidense contra Cuba que involucró a Alan Gross", 18 de enero. Disponible en www.lapupilainsomne.wordpress.com

_____ (2018): "Breve e incompleta cronología de un fracaso", 23 de mayo. Disponible en www.lapupilainsomne.wordpress.com

Santander Molina, Pedro (2019): "¿Cómo combatir las *fake news* sin contribuir a su propagación?", 25 de junio. Disponible en www.cubadebate.cu

Kaspersky Lab: Informes de los años 2019 y 2020.

Kemp, S. (2017): "Digital in 2017 Global Overview". *We Are Social*, Nueva York.

Índice

PRESENTACIÓN 4

INICIOS DE LOS EVENTOS DE CIBERSEGURIDAD 8

Primeros incidentes 8
Comportamiento en Cuba 10

CAUSAS Y CONDICIONES QUE FACILITAN LOS INCIDENTES DE CIBERSEGURIDAD Y SU GESTIÓN 15

Tratamiento a las vulnerabilidades de los sistemas informáticos 15
Amenazas de ciberseguridad a que están expuestos los sistemas informáticos 19
Modalidades más empleadas en los ataques a los sistemas informáticos 22
Modo de actuación para afrontar de manera adecuada un incidente de ciberseguridad 29

MEDIDAS PARA FORTALECER LA PROTECCIÓN DEL CIBERESPACIO NACIONAL DE CUBA 33

Protección a las infraestructuras críticas 33
Migración a plataformas de código abierto 38
Formación y preparación de especialistas en ciberseguridad 42
Normas jurídicas relacionadas con la ciberseguridad en Cuba 44
Segurmática, una empresa cubana de ciberseguridad 48

GUERRA CIBERNÉTICA EN INTERNET Y LAS REDES SOCIALES DIGITALES 53

CID 201, un ejemplo de soberanía tecnológica en Cuba 53
Algunos antecedentes de guerra cibernética 58

Manipulación en el tema internet en Cuba 62
Ataques en la red social *Twitter* *65*
Noticias falsas o *fake news* *68*
La batalla de la izquierda en las redes sociales 71
El bloqueo del Gobierno de los Estados Unidos afecta la protección del ciberespacio nacional cubano 77
Cuba en tiempos de coronavirus, su repercusión mediática 79

STATUS QUO DE LA GOBERNANZA DE INTERNET 83

Control unilateral de los Estados Unidos sobre internet 83
Estados Unidos evita cualquier cambio al *status quo* de la gobernanza de internet 86
Pronunciamientos de los países subdesarrollados en la Organización de Naciones Unidas, sobre ciberseguridad 88

VIOLACIONES Y USO INADECUADO DEL ESPECTRO RADIOELÉCTRICO NACIONAL 93

Afectaciones a la soberanía y a los servicios de telecomunicaciones 93
Violaciones del espectro radioeléctrico de Cuba 96
Cuando Cuba humilló tecnológicamente a los Estados Unidos 103
El derecho internacional y la televisión jamás vista 109
Una guerra electrónica entre David y Goliat 113

Bibliografía consultada 117

HABLANDO DE CIBERSEGURIDAD

Hablando de ciberseguridad es una interesante propuesta en la que su autor junto con su entrevistado, presentan una visión sobre aspectos relacionados con la ciberseguridad. La obra, escrita con un lenguaje claro y ameno, expone las causas y condiciones que facilitan los incidentes de ciberseguridad y el modo de actuación para afrontarlos, las medidas para fortalecer la protección del ciberespacio nacional de Cuba, la guerra cibernética, entre otros.

Contribuir a promover un mejor uso de las tecnologías de la información y la comunicación es el propósito de este libro.

Omar Pérez Salomón (Matanzas, 1961)
Político, investigador y escritor. Ingeniero en Telecomunicaciones y Máster en Gerencia y Comunicación. Ha publicado, entre otros títulos, *Estrellas en la frente, Terrorismo en el éter, Cuba: 125 años de telefonía, Fidel Castro, soldado de las ideas.*

Es fundador de la Enciclopedia Colaborativa Cubana *EcuRed*. Ha colaborado con la revista *Cuba Socialista* y con los sitios digitales *La pupila insomne* y *Cubadebate*. Actualmente es funcionario del Comité Central del Partido Comunista de Cuba.

citmatel

Avenida 47 No. 1802 entre 18-A y 20,
Playa, La Habana, Cuba. CP: 11300
Teléfono: (537) 204 3600
comercial@citmatel.com
www.editorialcitmatel.com
www.libreriavirtualcuba.com
© Copyright CITMATEL®. Todos los derechos reservados. **ISBN 978-959-315-173-3.**