TERRORISMO CIBERNÉTICO. PERSPECTIVAS DESDE LOS DERECHOS FUNDAMENTALES

CYBER TERRORISM. FUNDAMENTAL RIGHTS PERSPECTIVES

Por *Jorge Isaac Torres Manrique* (*)

ABSTRACT: In this installment, the author develops the aforementioned theme in a rigorous, insular, deep, maximalist way. In this way, it unravels and analyzes the real nature, dimension and scope of the new cyber crime. The added value that it offers is that it also does so from a viewpoint of fundamental rights, demonstrating in a concrete way how it is that in the current Constitutional State of Law, both constitutional law and in this case, fundamental rights are present in all branches of the legal system, specifically, in criminal law. And so too, the influence that this criminal manner has on the respective fundamental rights.

RESUMEN: En la presente entrega el autor desarrolla la referida temática de una manera rigurosa, insular, profunda, maximalista. Desentraña y analiza así la real naturaleza, dimensión y alcances del nuevo delito cibernético. El valor agregado que ofrece, es que lo hace además desde una mirada de los derechos fundamentales, demostrando de manera concreta cómo es que, en el actual Estado Constitucional de Derecho, tanto el derecho constitucional y en este caso, los derechos fundamentales se encuentran presentes en la totalidad de ramas del sistema jurídico, de manera específica, en el derecho penal. Y así también, la influencia que dicha manera delictiva tiene en los respectivos derechos fundamentales.

KEY WORDS: Cyber terrorism; Fundamental rights; Cyber terrorism.

PALABRAS CLAVES: Ciber terrorismo; Derechos fundamentales; Terrorismo cibernético.

(*) Consultor jurídico. Abogado por la UCSM (Arequipa). Doctorados en Derecho y Administración, por la UNFV (Lima). Presidente de la Escuela Interdisciplinar de Derechos Fundamentales Praeeminentia Iustitia (Perú). Director de la Biblioteca: "Recientes y próximos escenarios de los Ordenamientos Jurídicos", publicada por Ediciones Olejnik (Chile). Director Académico de la Revista Dogmática Penal latinoamericana (Perú). Diamont Ambassador of the Organization of World Ambassadors (Argentina). Miembro del Comité Editorial de la EDUCS- Editora da Universidade de Caxias do Sul (Brasil). Miembro del Consejo Académico del Instituto Iberoamericano de Estudios Superiores, adscrito a la Universidad de Santo Tomás de Oriente y Medio Día (Nicaragua). Pesquisador Internacional del Grupo de Responsabilidade Civil e Processo Ambiental de la Escola Superior Dom Helder Câmara (Brasil). Colaborador Extranjero del Grupo de Investigação de Investigação Metamorfose Jurídica y Colaborador do projeto de pesquisa Constitucionalismo e Meio Ambiente: Sustentabilidade, Direitos Fundamentais e o Socioambientalismo na Sociedade Consumocentrista; ambos vinculados ao Programa de Pós- Graduação em Direito da Universidade de Caixas de Sul (Brasil). Miembro de la International Association of Constitutional Law- IACL (Serbia). Autor y coautor de diversos libros y tratados en Derecho Constitucional, Penal, Administrativo. CoDirector de los Códigos Penales Comentados de Ecuador, Colombia. CoDirector de los Tratados: Lavado de Activos, Litigación Oral Estratégica, Derecho Probatorio, entre otros. kimblellmen@outlook.com; http://lattes.cnpq.br/0707774284068716.

DOI http://dx.doi.org/10.22529/rdm.2021(4)07

Sumario: 1. Prolegómeno. 2. El ciberespacio. 3. Importancia del ciberespacio. 4. Ciberterrorismo. 5. Naturaleza del ciberterrorismo. 6. Terrorismo y ciberterrorismo. diferencias y semejanzas. 7. Ventajas frente al terrorismo. 8. Partícipes de la figura ciberterrorista. 9. Vertientes principales del ciberterrorismo. 10. Agentes ciberterroristas. 11. Motivaciones y finalidades. 12. Nuevas tecnologías favorecen el accionar ciberterrorista. 13. Opera desde la deep web. 14. Ciberseguridad a los recursos on line. 15. Recientes vulnerabilidades. 16. Técnicas y procedimientos de infección y ataque. 17. Modalidades de actuación ciberterrorista. 18. Posibles consecuencias del ciberterrorismo y de los ataques informáticos. 19. El sector salud también escenario de ataques. 20. Costos del cibercrimen. 21. Las verdades de la seguridad informática frente al ciberterrorismo. 22. Políticas de estado contra el ciberterrorismo. 23. Instrumentos contra el ciberterrorismo. 24. Echan mano de los cibercafés y bibliotecas virtuales. 25. Capacidades prospectivas españolas. 26. Futura letalidad. 27. Alternativas de regular Internet. 28. Estrategia del reino unido de ciberseguridad nacional 2016-2021. 29. Tendencias. 30. Perspectiva desde los derechos fundamentales. 31. Análisis. – 32. Conclusiones. 33. Sugerencias. 34. Referencias bibliográficas.

1. PROLEGÓMENO.

El ciberespacio se ha convertido no solamente en el lugar común de gran parte de la población de las naciones, puesto que el mismo se constituye en un gran aliado facilitador de labores esenciales. Empero, el mismo es materia de peligros y ataques de diversa índole, uno de ellos constituye el ciberterrorismo. En la presente entrega se analiza la referida modalidad delincuencial, a efectos de desentrañar su naturaleza, arribando a análisis, conclusiones y sugerencias.

2. EL CIBERESPACIO.

El ciberespacio se puede definir como una realidad espacio-virtual, que no tiene una localización física y que abarca los sistemas de información y comunicación contenidos en

la Red. De esta nueva dimensión del espacio dependen, también, nuestros servicios básicos, infraestructuras críticas, economía y progreso como sociedad. Por tanto, la tecnología es el elemento físico básico, configurador del ciberespacio o, dicho de otra forma, las TIC se configuran como el elemento físico que hace posible el ciberespacio y, desde finales de los años ochenta, este nuevo espacio ha demostrado ser un medio de comunicación dinámico y con capacidad para llegar a todos los rincones del planeta. El ciberespacio capacita a muchos sujetos —y no solo a los Estados— para acceder a un arma cibernética con capacidad de realizar acciones susceptibles de ser calificadas como ataques, agresiones o usos de la fuerza armada en el contexto internacional. Mas, en particular, como señala Ángel Gómez de Ágreda, el ciberespacio vive en un estado permanente de agresión en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección.[1]

3. IMPORTANCIA DEL CIBERESPACIO.

Es evidente, por tanto, que las tecnologías informáticas y de telecomunicaciones son usadas a diario de manera masiva y para asuntos de gran importancia. Como caso especialmente interesante de la relevancia de la dependencia de las TIC se encuentran las llamadas "infraestructuras críticas": son aquellas que no solo son importantes, sino que resultan imprescindibles para la vida diaria de los países. Estas infraestructuras pueden tener sus sistemas de gestión comunicados por algún tipo de red telemática, y emplearán sistemas informáticos de control, lo cual las convierte en parte del ciberespacio. Su importancia la diferencia de otros servicios que simplemente hacen la vida más cómoda y agradable (no es igual no poder sacar una entrada para el teatro por Internet que la imposibilidad de realizar una transacción económica importante vía web).[2]

[1] MORÁN BLANCO, Sagrario. *La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo*. En línea: Recuperado en fecha 30/09/21 de http://www.revista-redi.es/wp-content/uploads/2017/08/8_estudios_moran_blanco_ciberseguridad.pdf. Madrid, 2017, p. 197.
[2] ROCA BLÁZQUEZ, José Luis. *Cibercrimen y ciberterrorismo: ¿Exageración mediática o realidad?*. En línea: Recuperado en fecha 30/09/21 de http://oa.upm.es/32868/1/TFG_jose_luis_roca_blazquez.pdf. Madrid, 2014, pp. 15- 16.

En ese sentido, la obligación del Estado no solamente transcurre por garantizar un ciberespacio libre de riesgos de ciberamenazas, sino, además, que la población se encuentre en condiciones de poder hacer uso del mismo de manera libre, gratuita.

4. CIBERTERRORISMO.

El Consejo de Europa define el ciberterrorismo como la forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos. [3]

Por su parte, la Unión Europea (UE) considera que es una tipología delictiva cometida a través de las tecnologías de información y comunicación (TIC) por organizaciones terroristas, utilizando la red como herramienta de comisión de los delitos y consecución de sus objetivos.[4]

5. NATURALEZA DEL CIBERTERRORISMO.

El ciberterrorismo representa una amenaza de orden dual (ataque a infraestructura crítica y propaganda, incitación y reclutamiento) que puede afectar seriamente la seguridad nacional, es por ello que una política pública en materia de ciberseguridad que contemple los elementos de las estrategias internacionales debe ser una prioridad estatal.[5]

6. TERRORRISMO Y CIBERTERRORISMO. DIFERENCIAS Y SEMEJANZAS.

[3] SUBIJANA ZUNZUNEGUI, Ignacio José. *El ciberterrorismo:una perspectiva legal y judicial*. En línea: Recuperado en fecha 30/09/21 de https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf. San Sebastián, 2008, p. 172.

[4] CESPEDOSA RODRÍGUEZ, Carolina. *Yihadismo, internet y ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30875/BorradorTFG_Ciberterrorismo_CarolinaCespedosa%20%281%29.pdf?sequence=1&isAllowed=yhttp://www.revistasculturales.com/xrevistas/PDF/72/1874.pdf. Madrid, 2019, p. 4.

[5] BOLAÑOS RODRÍGUEZ, Ricardo. *Ciberterrorismo: una amenaza a la seguridad nacional*. En línea: Recuperado en fecha 30/09/21 de http://biblio.upmx.mx/tesis/195364.pdf. Ciudad de México, 2018, p. 183.

En principio, si bien es cierto que el término: "ciberterrorismo" resulta de la unión de: "cibernética" y "terrorismo", amerita dejar constancia que el significado que adopta en conjunto dista de la naturaleza del término "terrorismo" convencional o tradicional.

Así, tenemos que mientras que el terrorismo busca causar zozobra en la población mediante ataques sistemáticos, con la finalidad de hacer caer el régimen que ellos pretender asumir; en el caso del ciberterrorismo, es de verse que su quintaesencia se encuentra orientada a apropiarse de manera ilegal e ilegítima de recursos económicos ajenos, a la vez de hacer apología a sus convicciones políticas, religiosas y reclutar adeptos, principalmente.

Por otro lado, cebe apostrofar que tanto el terrorismo y el ciberterrorismo coinciden en su accionar anónimo, clandestino, ilegal, delictivo.

7. VENTAJAS FRENTE AL TERRORRISMO.

Las ventajas del ciberterrorismo frente al terrorismo las han desarrollado durante las últimas décadas autores especialistas en esta materia y, en líneas generales, coinciden en que; en primer lugar, el ciberterrorismo no comporta riesgo físico al terrorista, incluyendo la gran garantía de anonimato que facilita. En segundo lugar, su ámbito geográfico de actuación es ilimitado al poder conectarse a la red desde casi cualquier lugar del mundo. En tercer lugar, sus actos generan una gran repercusión a nivel mundial al hacerse eco los medios de comunicación consiguiendo un gran efecto propagandístico. Por último, el beneficio económico que el ciberespacio ofrece, ya que no se emplea mucho coste en su utilización.[6]

8. PARTÍCIPES DE LA FIGURA CIBERTERRORISTA.

Entre los mismos podemos apreciar: i) Sujeto activo: El criminal, ii) Sujeto pasivo: La sociedad, iii) Bien Jurídico Protegido: La seguridad de la sociedad.[7]

[6] CESPEDOSA RODRÍGUEZ, Carolina. *Ob. Cit.*
[7] SANTIVAÑEZ ANTUNEZ, David Alonso. *La figura del ciberterrorismo como propuesta delictiva para la creación de una norma especial en nuestra legislación peruana vigente*. En línea: Recuperado en fecha 30/09/21 de http://repositorio.unfv.edu.pe/handle/UNFV/2132. Lima, 2018, pp. 67- 69.

9. VERTIENTES PRINCIPALES DEL CIBERTERRORISMO.

Al respecto podemos citar: i) Como apología del terrorismo, ii) Como medio de implantación del terror, iii) Como arma de ataque contra la sociedad, iv) Como medio de captación, v) Gamificación delictiva: Videojuegos en el plan de expansión del ciberterrorismo.[8]

10. AGENTES CIBERTERRORISTAS.

Los posibles agentes que podrían realizar alguna acción dañina en el ciberespacio son: i) Los Estados, ii) Los grupos extremistas, tanto ideológicos como políticos, iii) El crimen organizado y, iv) Las actuaciones delictivas individuales.[9]

11. MOTIVACIONES Y FINALIDADES.

Es de precisar que el ciberterrorismo busca basilarmente, agenciarse ilícitamente de financiamiento económico, a efectos de solventar su extremismo y motivos políticos.[10]

12. NUEVAS TECNOLOGÍAS FAVORECEN EL ACCIONAR CIBERTERRORISTA.

En efecto, al respecto es de señalar como tal:[11] i) Favorecer la ejecución transnacional del hecho, ii) Dificultar la obtención de fuentes de prueba de la comisión y su autoría, iii) Facilitar su acceso y manejo sin exigir una fuerte inversión económica, iv) Permitir la potencialidad de producir efectos deletéreos sobre núcleos importantes de personas o significativos daños o detrimentos sobre infraestructuras públicas o servicios comunitarios básicos, v) Coadyuvar a sus comunicaciones para la transmisión de información de manera rápida y difícilmente detectable, máxime cuando se acude a técnicas como la encriptación o la asociación a fotografías u otros elementos neutrales, vi) Transmitir su propaganda a

[8] SANTIVAÑEZ ANTUNEZ, David Alonso. *Ob. Cit.* Pp. 70- 82.
[9] CANDAU ROMERO, Javier. *Estrategias nacionales de ciberseguridad. Ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. Madrid, 2010, p. 263.
[10] CANDAU ROMERO, Javier. *Ob. Cit.*
[11] SUBIJANA ZUNZUNEGUI, Ignacio José. *Ob. Cit.* Pp. 172 -173.

través de sitios Web de escaso coste y fácil confección, vii) Permitir la guerra psicológica, las incitaciones al odio y el crimen, viii) Posibilitar el reclutamiento de sus miembros, ix) Facilitar la instrucción de sus componentes y la planificación de sus acciones, x) Instar la búsqueda de nuevas fórmulas de financiación (por ejemplo, la extorsión, xi) Infomática bajo la amenaza de ser ciber-atacados), la ejecución de complejas, transacciones internacionales o la realización de pagos por la adquisición de materiales y equipos utilizados en la actividad criminal y blanqueo de cantidades de dinero que, procediendo de actividades ilegales, pretenden su aplicación a las actividades terroristas.

El ciberterrorismo es un fenómeno criminal que se nutre del desarrollo tecnológico de la sociedad digital. Por lo tanto, es una criminalidad del siglo XXI, caracterizada por un trazo ejecutivo transnacional que se pergeña en organizaciones complejas, carentes de una ubicación espacial definida y dotadas de estructuras de financiación y medios técnicos suficientes para ejecutar delitos muy graves y hacer desaparecer, en escaso tiempo, las fuentes de prueba de su comisión y autoría.[12]

No obstante, consideramos que la harta demostrada supremacía y dominio de los ciberterroristas respecto de temas de vulneración del ciberespacio en general, cuentan como un factor de primer orden para la consecución y logro de sus objetivos delictivos. Soberanía en dichos predios, que cierta como lamentablemente el sector estatal y empresarial no han sabido comandar, superar, siquiera igualar.

13. OPERA DESDE LA *DEEP WEB*.

Inicialmente desarrollamos alcances acerca de la Depp Web. Así, tenemos que aparentemente, los buscadores o motores de búsqueda convencionales indicados en el acápite anterior, representan casi la totalidad de la información accesible vía la Red.

Sin embargo, únicamente representa el 4% de la toda la información disponible (superficial web o web abierta). El 96% restante está en la deep web, o Internet profunda, la misma que ofrece diversos niveles de información. Entonces, queda claro que accedemos a un porcentaje muy reducido de la información que figura en la Red.

[12] SUBIJANA ZUNZUNEGUI, Ignacio José. *Cit.* P. 186.

Esta es conocida también como *invisible web*, *dark web* o *hidden web* y es todo aquel contenido que no forma parte del *surface web*. El contenido existente es privado, confidencial y muchas veces ilegal. Para entrar en la Internet profunda se usa la red Tor por medio de las url.onion. Entre lo que se puede encontrar en la Internet profunda tenemos: i) Mercado negro (armas, drogas…), ii) Servicios Hacking, iii) Piratería, iv) Contratación de sicarios, asesinos, espías..., v) Tráfico de órganos, animales, personas, y vi) Porno ilegal, principalmente.[13]

La deep web, o Internet profunda "*engloba toda clase de webs, material e información no indexada en ningún buscador. Existen una serie de métodos muy eficaces para convertir todo tipo de documentos y páginas en no indexables: realizarlas íntegramente en flash o sin contenido html o protegerlas con contraseña. Un dato bastante importante y significativo es que este 'internet sumergido' supera ampliamente en contenido a la denominada Web Superficial (es hasta 500 veces mayor), a la que todos tenemos acceso mediante los buscadores tradicionales. Se estima que en la actualidad tiene un tamaño de 91.000 Terabytes*" [14].

A continuación, es de señalar que el ciberterrorismo lleva a cabo su accionar desde la *Deep Web*, amparado en el carácter inaccesible, clandestino como de extremo peligro, que presenta la Internet oscura.

14. CIBERSEGURIDAD A LOS RECURSOS *ON LINE*.

Habitualmente en ciberseguridad se habla de proteger: i) La disponibilidad; como ejemplo, ¿qué ocurriría si durante un tiempo no estuviera disponible la capacidad de consulta de saldos en cuentas bancarias? Se paralizarían multitud de transacciones y eso ocasionaría pérdidas económicas, ii) Integridad: es necesario que la información que se transmita o almacene llegue a su destino sin modificaciones ni alteraciones indeseadas, iii) Confidencialidad es otro aspecto clave cuando se trata de seguridad, pues gran cantidad de información transmitida o almacenada debe ser accesible solo a aquellos actores que

[13] MORALES, Javier. *Tor y la deep web "La internet que no conocemos"*. En línea: Recuperado en fecha 30/09/21 de https://prezi.com/lvlu3i7yx1uj/tor-y-la-deep-web-la-internet-que-no-conocemos/. 2014.
[14] S/a. *Conociendo la deep web: conceptos clave.* En línea: Recuperado en fecha 30/09/21 de https://ladycybermarketing.wordpress.com/2015/04/26/conociendo-la-deep-web-conceptos-clave/.

puedan y deban conocerla, iv) Autenticación, es decir, la seguridad de que los intervinientes en una comunicación son quieres aseguran ser.[15]

Todos estos factores son algunos de los que hay que cuidar y proteger, de tal manera que, ante las distintas amenazas que se presentan, sea conveniente asegurar la disponibilidad de los servicios ofrecidos y del ciberespacio y la integridad y confidencialidad de los datos que por él transitan o se almacenan. Hasta hace algunos años esta preocupación correspondía al usuario final (particular o empresa) que quería proteger sus activos y que podía verse amenazado de manera puntual y aislada. Sin embargo, el gran auge que ha experimentado el cibercrimen en los últimos años y las graves consecuencias que supone han hecho que haya pasado a ser preocupación de la esfera de los distintos gobiernos y organismos internacionales. Para hacer frente al cibercrimen y a los ciberataques ha sido necesaria la inclusión de las nuevas ciberamenazas en las respectivas políticas y estrategias de seguridad y defensa de países y organismos supranacionales.[16]

15. RECIENTES VULNERABILIDADES.

Las siguientes son las vulnerabilidades más significativas de 2018:[17]

15.1. Vulnerabilidades en el software y en el hardware. El número de vulnerabilidades conocidas en los productos de software ha sido alto y no hay indicios de que esta situación varíe en los próximos años. Son claras ciertas tendencias en el software que afectan a la seguridad del producto final.

15.2. Nuevas formas de explotación. En enero de 2018, equipos de investigación revelaron dos nuevas familias de vulnerabilidades hardware, denominadas Spectre y Meltdown, que permitirían a los atacantes obtener información confidencial ejecutando el código del programa en el ordenador de la víctima. Como nueva forma de explotación, cabe mencionar la vulnerabilidad GLitch, publicada por investigadores de la Universidad Libre

[15] ROCA BLÁZQUEZ, José Luis. *Ob. Cit.* P. 16.
[16] ROCA BLÁZQUEZ, José Luis. *Cit.*
[17] CENTRO CRIPTOLÓGICO NACIONAL. *Ciberamenazas y tendencias 2019*. En línea: Recuperado en fecha 30/09/21 de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html. Madrid, 2019, pp. 16- 19.

de Ámsterdam, capaz de perpetrar lo que se conoce como ataques de Rowhammer a través del procesador gráfico de un ordenador. Asimismo, mediante la explotación de una vulnerabilidad de Apache Struts, la empresa Equifax informó de que los atacantes habían sustraído los datos de 4,9 millones de norteamericanos, el ataque ocasionó a Equifax una pérdida de 87,5 millones de dólares.

15.3. Ataque DDoS a través de sistemas públicamente accesibles. A partir de febrero de 2018, se evidenció en las acciones DDoS el uso de los llamados ataques "Memcached", a través de sistemas accesibles al público. Los sistemas Memcached están diseñados para almacenar temporalmente pequeñas cantidades de datos de otras fuentes tales como bases de datos y APIs, para hacer que los sitios web sean más rápidos. Los sistemas no requieren autenticación para las comunicaciones y no han sido desarrollados para ser de acceso público, posibilitando por tanto ataques por amplificación. Según la compañía Panda, el 28 de febrero de 2018 tuvo lugar el ataque DDoS más potente de la historia: 1,35 terabits por segundo de tráfico dirigido a GitHub, la plataforma web de proyectos de desarrollo colaborativos. Unos días más tarde, se superó el record con un ataque con picos de tráfico de 1,7 Tbps. En estas acciones, el atacante envía lo que simula ser una solicitud en nombre del objetivo, falsificando su dirección IP. Puesto que las respuestas son más largas que la solicitud, el actor puede usar un ancho de banda relativamente pequeño para configurar un ataque mayor.

15.4. La seguridad de los dispositivos médicos y sanitarios. Varias pruebas en laboratorio, realizadas en Estados Unidos, han demostrado que dispositivos médicos como marcapasos, desfibriladores o respiradores son vulnerables a ciberataques. En consecuencia, la ciberseguridad debe ser integrada e implementada desde el principio del desarrollo y fabricación de estos dispositivos, con el fin de garantizar su uso. A menudo, los mecanismos de autenticación en dispositivos médicos digitales no están suficientemente protegidos y las técnicas de cifrado de datos para la comunicación y el almacenamiento son débiles o, incluso, inexistentes. En estas circunstancias, sería posible obtener acceso no autorizado y manipular el dispositivo sin el conocimiento del paciente.

16. TÉCNICAS Y PROCEDIMIENTOS DE INFECCIÓN Y ATAQUE.

Entre los mismos podemos señalar: i) Phishing, Spam, ii) Skimming, Carding y técnicas asociadas, iii) Propagación de código dañino, iv) Ataques basados en web, v) Ataques dirigidos, vi) Redes zombi y Kits de herramientas, vii) APT.[18] Al respecto, cabe precisar las respectivas definiciones:

16.1. Phishing. Es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia. Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.[19]

16.2. Spam. Es un término genérico para cualquier mensaje no solicitado entregado a través del sistema electrónico de mensajería. Aunque se puede aplicar a cualquier elemento, desde mensajería instantánea y mensajes de texto, hasta foros de internet y redes sociales, el término spam se asocia normalmente con los mensajes de correo electrónico. También conocido como correo basura, los emails de spam son mensajes enviados a múltiples direcciones a la vez, normalmente para fines publicitarios. No todo el spam es comercial.

[18] ROCA BLÁZQUEZ, José Luis. *Cit.* 73- 94.
[19] MALWAREBYTES. *¿Qué es phishing?*. En línea: Recuperado en fecha 30/09/21 de https://es.malwarebytes.com/phishing/. One Albert Quay.

Los cibercriminales también pueden usar spamming para distribuir software dañino y robar datos personales de objetivos inocentes. Esto se hace con la inclusión de enlaces que parecen legítimos, que llevan a los receptores a páginas de registro falsas que recogen sus datos, así como páginas que parecen auténticas que alojan malware. En los años recientes, los hackers han empezado a usar emails de spam y malware para silenciosamente tomar el control de redes de ordenadores enteras y formar botnets que pueden usar para atacar a otras redes y páginas web.[20]

16.3. Skimming. Conocido también como web skimming es una técnica utilizada por ciberdelincuentes para obtener información bancaria y personal de tiendas online legítimas que posteriormente será vendida en el mercado negro, o utilizada directamente por los ciberdelincuentes en su propio beneficio. El primer paso que deben llevar a cabo los ciberdelincuentes consiste en obtener acceso a la tienda online, para ello se suelen valer de vulnerabilidades no parcheadas en el gestor de contenidos o mediante campañas de phishing. Una vez han conseguido acceso a la tienda, modifican parte de su código fuente para que, cuando el cliente introduce información personal o bancaria, sea enviada al banco y también robada. De esta forma, tanto el cliente como el comercio no son conscientes del robo, ya que el pago es correcto, sin embargo, toda esa información ya está en manos de los ciberdelincuentes. Este tipo de técnica afecta, principalmente, a aquellos comercios online cuya pasarela de pago está integrada dentro de la propia tienda, ya que toda la información bancaria es gestionada internamente. Las tiendas online que utilizan una pasarela de pago de un tercero tampoco están libres de riesgo, ya que, aunque los datos de la tarjeta no son gestionados por el comercio, la información personal de los clientes puede ser sustraída igualmente.[21]

16.4. Carding. Es una modalidad de fraude electrónico. En la cual las personas detectan cargos no reconocidos en sus tarjetas de crédito o de débito. Los delincuentes

[20] SOFTWARELAB. *¿Qué es spam?*. En línea: Recuperado en fecha 30/09/21 de https://softwarelab.org/es/que-es-spam/.
[21] INSTITUTO NACIONAL DE CIBERSEGURIDAD. *E-skimming, qué es y cómo proteger tu tienda contra esta técnica maliciosa*. En línea: Recuperado en fecha 30/09/21 de https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa. Madrid, 2019.

acceden de forma ilegal, a través de un software de manera aleatoria, a la información de tarjetas de crédito o débito. Una vez que obtienen la información realizan pagos con ellas, que en primera instancia pueden pasar desapercibidos, ya que no son montos muy poco significativos, esto ocurre hasta el momento en el que los tarjetahabientes perciben cargos que desconocen. Otra manera de obtener los datos, es a través del phishing. En este tipo de fraude, los estafadores suplantan la identidad o imagen de una empresa (bancos, escuelas, instituciones de gobierno, entre otras), para lograr de esta manera obtener datos, claves, números de cuentas bancarias y tarjetas de crédito, identidad o cualquier otra información para hacer fraude.[22]

16.5. Propagación de código dañino. El código malicioso es lo que vulgarmente conocemos como virus o malware. Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia. En función de la intención del Cracker, el programa podría: a. Robar credenciales, datos bancarios, información, b. Creación de redes con ordenadores botnet, c. Cifrado del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos. Las empresas destinan un gran esfuerzo en luchar contra estas amenazas, por eso es importante saber cuáles son las más comunes y en que nos afecta como usuarios. Se debe tener especial atención por parte de las empresas en asegurar que sus herramientas y dispositivos aseguren una integridad, confidencialidad y disponibilidad de los datos. No olvidemos que los datos de una empresa son lo que garantizan la continuidad de la misma. Una pérdida o robo de los mismos, perjudicaría gravemente a la empresa afectando tanto a su reputación como a la actividad normal de su empresa, pudiendo significar incluso el cierre del negocio.[23]

16.6. Ataques basados en web. Este tipo de ataques se centran en los sistemas y servicios web para comprometer a la víctima, lo que comprende la explotación de los navegadores, los sitios web, la explotación del sistema de gestión de contenido (CMS) y los propios servicios web. Los ataques drive-by, waterhole, redirection y man-in-thebrowser

[22] SILVA, Karla. *¿Qué es el carding y los bineros?*. En línea: Recuperado en fecha 30/09/21 de https://kueski.com/blog/finanzas-personales/dinero-economia/que-es-carding/. 2020.
[23] RUIZ MARTINEZ, Juan Carlos. *Código malicioso ¿Qué es y qué tipos hay?*. En línea: Recuperado en fecha 30/09/21 de https://www.ymant.com/blog/codigo-malicioso-que-es-y-que-tipos-hay/. Valencia.

son algunas de las categorías más conocidas de tales acciones. Durante 2018, los ataques basados en la web siguieron siendo una de las amenazas más importantes, por su amplia difusión. Estas son algunas de las evidencias más significativas de 2018: a. APT, campañas de código dañino y ataques basados en watering hole, b. Extensiones para navegadores, c. Incremento de los compromisos relacionados con los sistemas de gestión de contenido (CMS): A principios de 2018, se observaron varios ataques contra Drupal que entregaban mineros de criptomonedas y herramientas de ingeniería social21. Más tarde, en septiembre de 2018, se evidenció una ola de ataques dirigidos a sitios de Wordpress vulnerables22, d. Continúa la tendencia de los exploits kits basados en el navegador web (drive-by).[24]

16.7. Redes zombi. Conocidas también como. Son un conjunto de ordenadores infectados controlados por el ciberdelicuente para llevar a cabo acciones maliciosas. Es una red informática distribuida, es decir, creada por una elevado número de ordenadores o dispositivos con conexión a Internet que han sido infectados por un malware que permite al hacker controlar dichos equipos y dispositivos de forma remota, con fines, normalmente, ilegales. Por ese motivo, a cualquier equipo infectado que forma parte de una botnet se le llama zombie. Una botnet se puede utilizar con diferentes fines, generalmente con intenciones maliciosas o ilegales, como el envío masivo de spam o virus, el robo de información, llevar a cabo ataques DDoS o incluso la minería de bitcoins. Lo peor de este tipo de control es que el usuario normalmente no lo detecta, pudiendo atribuir la ralentización de su equipo a otros motivos. Por ello es importante estar protegidos y prevenidos ante el tipo de malware empleado para crear la botnet.[25]

16.8. Kits de herramientas. Son utilizados para realizar ataques cibernéticos son muy populares en internet. Existen dos tipos: El más popular es aquel que permite a los cibercriminales establecer en una página web cualquier exploit que les permita entrar en la máquina del usuario si visitan el site. En este caso el objetivo podría ser instalar falsos antivirus en las computadoras de las víctimas que tendrán que pagar para verse libres de él

[24] CENTRO CRIPTOLÓGICO NACIONAL. *Ob. Cit*. P. 31.
[25] RAMÍREZ, Helena. *Botnet o red zombie ¿Qué es y como detectarla antes de que infecte a tu PC?*. En línea: Recuperado en fecha 30/09/21 de https://protecciondatos-lopd.com/empresas/botnet-red-zombie/. Madrid, 2020.

y que además permite a los ciberdelincuentes conseguir cuotas constantes. El segundo tipo de kit permite a los criminales crear su propio malware. En ambos casos el peligro existe y demuestra que es fácil realizar ataques y hacer dinero con el cibercrimen. Otro signo de la creciente sofisticación y peligro para la seguridad en internet es que la mayoría de los kits pueden actualizarse fácilmente, lo que significa que pueden explotar las últimas vulnerabilidades llamadas Día Cero, que normalmente son desconocidas tanto por el usuario como por el fabricante del software o sistema afectado.[26]

16.9. APT. Amenaza Persistente Avanzada (APT). Compuesto por una cuidadosa combinación de diferentes herramientas y métodos, a veces rudimentarios, el temido APT es una amenaza mucho más grande que cualquiera de sus partes compuestas. APT se define como un ataque prolongado enfocado en un objetivo específico con el objetivo de comprometer el sistema y robar información sobre dicho objetivo. Los actores de amenazas que ejecutan ataques APT utilizan una variedad de herramientas y métodos para obtener acceso a su objetivo y ampliar su brecha. Estas herramientas suelen ser malware personalizado para las diversas técnicas que requiere el ataque y, a veces, los grupos de ataque crean familias de malware que consisten en herramientas personalizadas que solo se utilizan en sus ataques APT. Estas herramientas son como tarjetas de visita para el grupo de ataque. Puede tener actores estatales y no estatales. Presenta como características de ataque: a. Aumento de los inicios de sesión a altas horas de la noche, b. Troyanos de puerta trasera generalizados, c. Flujos de información inesperados, d. Paquetes de datos inesperados, e. Campañas enfocadas de spear phishing.[27]

17. MODALIDADES DE ACTUACIÓN CIBERTERRORISTA.

Dentro de la variedad de conductas que pueden ser desarrolladas por los grupos ciberterroristas, podemos señalar las siguientes actividades según la clasificación conocida

[26] MUNDO CONTACT. *Los kits de creación de malware, los mayores generadores de amenazas*. En línea: Recuperado en fecha 30/12/20 de https://mundocontact.com/los-kits-de-creacion-de-malware-los-mayores-generadores-de-amenazas/. 2011.
[27] BELDING, Greg. *Spotlight de malware: ¿Qué es APT?*. En línea: Recuperado en fecha 30/09/21 de https://resources.infosecinstitute.com/topic/malware-spotlight-what-is-apt/. 2019.

como STRIDE (por el acrónimo derivado de las iniciales de cada una de ellas en inglés) establecida por Microsoft:[28]

17.1. ***Spoofing identity*** (suplantación de la identidad de un usuario). Por ejemplo, robar el nombre de usuario y contraseña de una persona.

17.2. ***Tampering with data*** (manipulación de datos). Que consiste en realizar cambios sin autorización a una base de datos.

17.3. ***Repudiation*** (repudio). Que comúnmente opera cuando al realizarse una operación ilegal, el propio sistema carece de la capacidad de rastrear las actividades prohibidas.

17.4. ***Information disclosure*** (revelación de información). La cual ha tenido una fuerte repercusión en los últimos años (sin que por ellos los consideremos como terroristas necesariamente) con los famosos casos de Edward Snowden, Wikileaks y Bradley Manning, por citar tan sólo unos ejemplos, ya que datos que en principio no estaban destinados al público en general ahora se convierten, tras el ataque, del conocimiento de un gran número de usuarios.

17.5. ***Denial of Service*** (negación del servicio). Que también ha sido sumamente difundido en medios de comunicación ya que son blanco de dichos ataques generalmente páginas gubernamentales que no pueden ser vistas por un gran número de horas.

17.6. ***Elevation of privilege*** (acceso privilegiado). Que consiste en una de las amenazas más sofisticadas y peligrosas ya que implica la penetración a los sistemas al ser considerado como un "usuario confiable".

De lo descrito es de reiterar, que el ciberterrorismo domina de manera muy superior la temática en informática, a efectos de lograr su delictuoso accionar sin contar con una oposición de considerar para ello, lo que deviene en sumamente penoso como preocupante.

18. POSIBLES CONSECUENCIAS DEL CIBERTERRORISMO Y DE LOS ATAQUES INFORMÁTICOS.

[28] CORONADO CONTRERAS, Laura Verónica. *La libertad de expresión en el ciberespacio*. En línea: Recuperado en fecha 30/09/21 de https://eprints.ucm.es/33067/1/T36374.pdf. Madrid, 2015, p. 224.

Entre los mismos podemos mencionar:[29] i) Corte del suministro eléctrico y posible descontrol de centrales nucleares, centrales hidroeléctricas y térmicas, ii) Colapso total de las redes telefónicas y los sistemas de comunicaciones, iii) Desarrollo de ataques específicos contra los sistemas de comunicaciones militares, iv) Caos financiero: ataques a las entidades financieras y a las bolsas, paralizando cualquier gestión y borrando o alterando los datos de todas las cuentas corrientes y otros registros de información, v) Intervención del control del tráfico aéreo y ferroviario, provocando colisiones de aviones y trenes, y dejando inoperantes estas redes de transporte, vi) Ataques informáticos de todo tipo protagonizados por virus, programados y controlados de forma remota para activarse en el momento adecuado, vii) Destrucción de grandes bases de datos estatales, vitales para el funcionamiento del país, como las de los cuerpos de policía, el Tesoro Público, la Sanidad, la Seguridad Social y el resto de Administraciones Públicas en general, viii) Sabotajes locales en la capital y otras ciudades importantes por su población o su actividad económica, alterando el funcionamiento de los semáforos para causar choques en cadena que colapsen durante horas las principales carreteras, ix) Otros sabotajes, como por ejemplo los dirigidos a las empresas más importantes y a organismos oficiales locales, x) Lanzamiento de bombas electromagnéticas para neutralizar todos los equipos electrónicos militares no protegidos y silenciar a las principales emisoras de radio y televisión.

19. EL SECTOR SALUD TAMBIÉN ESCENARIO DE ATAQUES.

El entorno sanitario español, y en especial los hospitales, no escapa a los ciberataques. En los últimos dos meses se ha detectado un incremento de actividad cibernética maliciosa, utilizando Covid-19 como vector de ataque. ¿Por qué atacar al sector sanitario?. GMV distingue cuatro factores determinantes que explican esta efervescencia

[29] GÓMEZ VIEITES, A. *La lucha contra el ciberterrorismo y los ataques informáticos*. En línea: Recuperado en fecha 30/09/21 de https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf. Madrid, pp. 1-2.

del malware en la sanidad. En primer lugar, el coste medio de una brecha de datos en el sector sanitario se cotiza a 408 dólares por historial médico, frente a los 225 euros que se paga en el resto de las industrias. En la Deep Web se puede adquirir el historial clínico de los pacientes por 80 euros. En segundo lugar, la tecnología de los hospitales, heterogénea y con sistemas antiguos de más de 20 años, con redes mal segmentadas conforma un blanco apetecible por las bajas dificultades que plantean a los cibercriminales. El robo de propiedad intelectual es otro motivo de peso, como explica el estudio de GMV: La investigación médica es costosa y algunos grupos de amenazas persistentes avanzadas (APT), especializados en el robo de propiedad intelectual, atacan a institutos de investigación médica y empresas farmacéuticas que habitualmente llevan a cabo investigaciones innovadoras para hacerse con sus desarrollos. De hecho, la caza de la vacuna es una obsesión del 'lado oscuro', y así lo ha advertido el FBI.[30]

20. COSTOS DEL CIBERCRIMEN.

En lo relacionado a las consecuencias de los fallos y ataques en las empresas, tenemos:[31] i) Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes, ii) Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: coste de oportunidad por no poder utilizar estos recursos, iii) Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos, iv) Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores, contactos comerciales o candidatos de empleo, con las consecuencias que se derivan del incumplimiento de la legislación en materia de protección de datos personales vigentes en toda la Unión Europea y en muchos otros países, v) Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores,

[30] CONTRERAS, R. *El ciberterrorismo se viste de phishing. Arrecian los ataques que utilizan Covid-19 como señuelo*. En línea: Recuperado en fecha 30/09/21 de https://recursos.bps.com.es/files/960/78.pdf. Barcelona, 2020, p. 49.
[31] GÓMEZ VIEITES, A. *Ob. Cit.* Pp. 2- 3.

etcétera, vi) Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, pérdida de oportunidades de negocio, vii) Posibles daños a la salud de las personas, con pérdidas de vidas humanas en los casos más graves, viii) Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales y la imposición de sanciones administrativas. Las organizaciones que no adoptan medidas de seguridad adecuadas para proteger sus redes y sistemas informáticos podrían enfrentarse a penas civiles y criminales bajo una serie de leyes existentes y decisiones de tribunales: protección de la privacidad y los datos personales de clientes y empleados; utilización de aplicaciones P2P para intercambio de contenidos digitales protegidos por derechos de autor; etcétera.

Por otro lado, resulta interesante observar que el coste medio de pérdidas por el cibercrimen ha ido aumentando a lo largo de los cuatro años en los que se ha realizado el mismo estudio en E.E.U.U. En el año 2010 la media de pérdidas fue de 6'5 millones de dólares; en 2011 era de8'4 millones, en 2012 aumentó un 6% hasta llegar a los 8'9 millones y en 2013 subió un 26%, llegando a los 11'6 millones de dólares antes mencionados. En Japón, Alemania, Australia y Reino Unido los costes incurridos por los ataques fueron distintos, así como los tipos de ataques sufridos. Las empresas japonesas eran las que menos incidentes sufrieron por personal interno; esto puede indicar una gran influencia de los valores culturales en aquel país. Por otra parte, la importancia de los distintos costes varía entre países: para E.E.U.U. y Alemania la pérdida de información constituye el mayor porcentaje de pérdidas, mientras que para Australia y Reino Unido esa circunstancia le corresponde a la interrupción del negocio. Para las empresas japonesas tienen igual importancia, en cuanto a pérdidas económicas, la pérdida de información y la interrupción de las operaciones.[32]

El ciberterrorismo puede afectar de manera contundente a la economía no sólo de una persona o industria, sino el correcto funcionamiento de la economía de un país, motivo por

[32] ROCA BLÁZQUEZ, José Luis. *Cit.* Pp. 120- 121.

el cual debe ser observado como un riesgo que debe atenderse con programas de corto y mediano plazo.[33]

21. LAS VERDADES DE LA SEGURIDAD INFORMÁTICA FRENTE AL CIBERTERRORISMO.

Todos los sistemas informáticos dependen del factor humano y por ende, este podrá ser el eslabón débil en la cadena de seguridad. Una de las leyes de la Seguridad Informática establece que la tecnología no es una panacea y otra que ningún sistema informático es 100% seguro. La seguridad informática depende en gran parte de lo complejo de las claves de acceso elegidas y de la fiabilidad de los administradores. En el mundo de la seguridad informática, el 80% de los incidentes de provienen de personas que son del mismo entorno del sistema objeto de ataque. Los empleados descontentos o exempleados que guardan resentimientos pueden producir problemas. Los sistemas de seguridad pueden ser atacados con más facilidad por personas que conocen el entorno pudiendo instalar bombas lógicas y abrir puertas de conexión a terceros comprometiendo gravemente la seguridad del sistema. Es conocido en el mundo del espionaje que los servicios de inteligencia buscan candidatos que se encuentren trabajando en ciertos puntos de interés para obtener acceso a información clasificada o bien para conocer en el caso de informática fallos de seguridad.[34]

22. POLÍTICAS DE ESTADO CONTRA EL CIBERTERRORISMO.

Los Estados están obligados a articular un sistema nacional de ciberseguridad que gestione, con eficacia, los riesgos que amenazan el ciberespacio. El fortalecimiento de la ciberseguridad proporciona a las Administraciones públicas, al tejido industrial y

[33] NAVA GARCÉS, Alberto Enrique. *Ciberterrorismo: la nueva cara de la delincuencia en el siglo XXI. La participación y fomento al delito por órganos de gobierno y empresas*. En línea: Recuperado en fecha 30/09/21 de http://rabida.uhu.es/dspace/bitstream/handle/10272/17083/ciberterrorismo.pdf?sequence=2. Huelva, 2017, p. 163.

[34] ORTA MARTÍNEZ, Raymond. *Ciberterrorismo.* En línea: Recuperado en fecha 30/09/21 de http://servicio.bc.uc.edu.ve/derecho/revista/relcrim21/art06.pdf. Carabobo, p. 124.

empresarial, a la comunidad científica y a los ciudadanos en general, una mayor confianza en el uso de las TIC. Por ello, los organismos públicos responsables reconocen la importancia que tiene trabajar en coordinación con el sector privado y con los propios ciudadanos, para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información. Ahora bien, el logro de un ciberespacio más seguro y fiable solamente es posible mediante el refuerzo de la colaboración y la cooperación internacionales, creando relaciones de confianza, sobre todo entre los Estados, para el intercambio de información y de los datos esenciales en materia de ciberseguridad. Los Estados aplican políticas antiterroristas de infiltración y monitorización, dirigidas por los centros de inteligencia y agencias policiales, con el fin de prevenir posibles atentados terroristas y obtener pruebas que ayuden en la instrucción judicial; y, también, llevan a cabo las políticas contraterroristas dirigidas a la creación de cuerpos e instituciones especializadas.[35]

23. INSTRUMENTOS CONTRA EL CIBERTERRORISMO.

Al respecto hacemos mención: i) La UE puso en marcha el Centro Europeo sobre la Cibercriminalidad (2013), ii) Agenda Europea de Seguridad (2015-2020), iii) Programa Europeo de protección de Infraestructuras Críticas y el Programa de protección de Infraestructuras TIC, iv) Estrategia de Ciberseguridad Nacional de España (2013), v) Estrategia de Ciberseguridad de la UE (2008), vi) La OTAN lleva organizando congresos de ciberseguridad desde comienzos del siglo XXI. *Verbi gratia*: Cumbre de Praga (2002), Cumbre de Bucarest (2008), Consejo del Atlántico Norte firma la Política de Ciberdefensa (2008), Cumbre de Varsovia (2016),[36] vii) Ley de Seguridad Informática de Alemania (2015, viii) Directiva sobre Seguridad de Redes y Sistemas de Información, aprobada por el Parlamento Europeo (2016), ix) Austria publicó la National Security ICT Strategy (2012) y Cyber Security Strategy (2013), x) Francia publicó su National Cyber Security Strategy (2015), xi) EE.UU. publicó su National Strategy Security (2017, xi) Chile presentó su

[35] MORÁN BLANCO, Sagrario. *Ob. Cit*. Pp. 207- 208.
[36] MORÁN BLANCO, Sagrario. *Cit*. Pp. 208- 210.

Política **N**acional de Ciberseguridad (2017).[37] Estrategia del Reino Unido de Ciberseguridad Nacional 2016-2021, principalmente.

24. ECHAN MANO DE LOS CIBERCAFÉS Y BIBLIOTECAS VIRTUALES .

Los terroristas se han servido de cibercafés, en algunos casos, para llevar a cabo actos relacionados con el terrorismo. No hay datos precisos sobre la proporción de este tipo de actividad en relación con las actividades realizadas legítimamente y las que no lo son a través de estos servicios de Internet. Precisamente por ello, la investigación de los casos de terrorismo con uso de Internet u otros servicios conexos por presuntos terroristas suele exigir la realización de actividades intrusivas o coercitivas de registro, vigilancia o monitorización por los servicios de inteligencia o los organismos encargados de hacer cumplir la ley. No obstante, para que las autoridades emprendan ese tipo de actividades necesitan de la cooperación de los proveedores de servicios públicos de telecomunicaciones o servicios conexos. Por ello, los Estados deben ofrecer una base jurídica que incida de forma evidente sobre las obligaciones de las partes del sector privado, en la que se indique cuál es el plazo aplicable, si lo hubiere, durante el cual los proveedores deben retener los datos en su poder.[38]

En algunos Estados, como Egipto, India, Jordania y Pakistán, los Gobiernos aplican medidas legislativas o reglamentarias concretas que obligan a los operadores de cibercafés a obtener, retener y, previa solicitud, entregar una identificación de los clientes a los organismos encargados de hacer cumplir la ley. Por tanto, algunos Gobiernos han impuesto obligaciones específicas a los operadores de los cibercafés, obligando a los proveedores de servicios de Internet a retener, por ley, ciertos tipos de datos relacionados con comunicaciones durante un plazo determinado; con el fin de poder obtener, conservar y, previa solicitud, presentar a la Policía identificación fotográfica, domicilio y datos de uso, y conexión de los clientes. La utilidad de esas medidas es cuestionable y no suele ser tan

[37] PONS GAMÓN, Vicente. *Ciberterrorismo. Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*. En línea: Recuperado en fecha 30/09/21 de http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf. Madrid, 2018, pp. 110- 115.
[38] MORÁN BLANCO, Sagrario. *Cit*. P. 213.

eficaz por diversas razones. Entre ellas, por el largo tiempo que precisan los procedimientos tradicionales de asistencia judicial recíproca en casos transnacionales y, sobre todo, porque hay otros servicios de Internet a disposición del público, por ejemplo, los ordenadores de las bibliotecas públicas o locales públicos con conexión inalámbrica a Internet (WiFi), que ofrecen oportunidades similares para el uso anónimo de Internet por terroristas.[39]

25. CAPACIDADES PROSPECTIVAS ESPAÑOLAS.

Hablar de prospectiva refiere la capacidad de predecir el futuro desde una perspectiva holística, proactiva y anticipatoria. Entonces, evaluaremos hasta qué punto se encuentra España en dicha capacidad para afrontar los ataques ciberterroristas:[40]

Al respecto, es de verse: i) Capacidades gubernamentales y de coordinación. Las atribuciones legales del Centro Criptológico Nacional (CCN) en materia de asesoramiento gubernamental, lo habilitan para proveer a los órganos de decisión superiores de información y análisis técnico en materia anticiberterrorista, llegado el caso, ii) Capacidades policiales, iii) Capacidades civiles y empresariales. La naturaleza del Instituto Nacional de Ciberseguridad de España (INCIBE) hace que tenga una inclinación de ciberseguridad más ciudadana y empresarial, orientada a los riesgos del día a día, no tanto al ciberterrorismo. No obstante, con los distintos canales que tiene abiertos con sus interlocutores puede recibir información relacionada directa o indirectamente con actividad ciberterrorista que pondrá en conocimiento de las fuerzas nacionales directamente encargados de su lucha y prevención, iv) Capacidades militares.

26. FUTURA LETALIDAD.

El empleo más probable en el futuro será el relacionado con la capacidad de influir en audiencias concretas: población de un país, grupos sociales determinados. Se ha visto claramente la potencialidad de su empleo combinado con los métodos tradicionales de

[39] MORÁN BLANCO, Sagrario. *Cit.* P. 214.
[40] GONZÁLEZ-GARCÍA, Abel y GIRAO GONZÁLEZ, Francisco José. *Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español*. En línea: Recuperado en fecha 30/09/21 de https://revistas.unlp.edu.ar/RRII-IRI/article/view/9489/9063. Buenos Aires, 2020, pp. 246- 255.

combate, como ha realizado Rusia en Ucrania (conflicto híbrido) o en procesos electorales como el americano. La reciente controversia de Facebook y el posible impacto en las elecciones de los Estados Unidos sobre las filtraciones de millones de datos de los usuarios son un buen ejemplo de ello. Como conclusión y a pesar de la narrativa de algunos países, los actores más probables y peligrosos que realizarán ciberataques serán los estados y no tanto los grupos terroristas.[41] El ciberterrorismo es la antesala de la ciberguerra.[42]

27. ALTERNATIVAS DE REGULAR INTERNET.

A principios de este siglo, el Estado manifestó un interés en re-regular aquellos sectores debido a las crisis potenciales que suponía un sistema sin ningún tipo de control estatal y los peligros que generaba la ausencia de regulación para la seguridad nacional. En el caso de Internet, esta crisis se reflejó en el colapso de la "burbuja punto-com" (dot-com bubble) entre los años 2000-2002. A partir del año 2005 se ha mostrado una (nueva) tendencia a la co-regulación, principalmente en Europa. [43]

Como alternativas tenemos: i) Auto-regulación. Bajo este sistema un grupo de agentes o individuos detentan el control sobre su propio comportamiento. Pertenecer al grupo regulado es voluntario y los participantes diseñan sus propias reglas utilizando herramientas como códigos de conducta o soluciones y estándares técnicos frente a los problemas recurrentes, ii) Regulación estatal directa. Este mecanismo consiste en la aplicación de leyes especiales por parte del Estado para desarrollar una regulación particular en un sector determinado. El cumplimiento es monitoreado y mantenido por agencias o entes estatales que tienen el poder de hacer cumplir la norma, iii) Co-regulación. Es la combinación de una amplia gama de fenómenos de regulación donde el régimen regulatorio se crea a partir de la

[41] NIETO FERNÁNDEZ, Ignacio. *La letalidad del ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de https://armada.defensa.gob.es/archivo/rgm/2018/07/rgm072018cap11.pdf. Madrid, 2018, p. 141.
[42] NAVA GARCÉS, Alberto Enrique. *Ob. Cit.* P. 163.
[43] REYES BENZ, Arlette Belén. *Alcances del "ciber-terrorismo" en la sociedad contemporánea*. En línea: Recuperado en fecha 30/09/21 de http://repositorio.uchile.cl/bitstream/handle/2250/116821/de-reyes_a.pdf?sequence=1&isAllowed=y. Santiago, 2014, p. 130.

interacción compleja entre la legislación general y la auto-regulación. La co-regulación permite la inclusión de diversos actores, lo que le otorga gran legitimidad.[44]

28. ESTRATEGIA DEL REINO UNIDO DE CIBERSEGURIDAD NACIONAL 2016-2021.

El Reino Unido es uno de los países digitales más destacados del mundo. Gran parte de su prosperidad depende de su capacidad de proteger su tecnología, datos y redes de las múltiples amenazas a las que nos enfrentamos. Sin embargo, los ciberataques son cada vez más frecuentes, sofisticados y perjudiciales, cuando logran su cometido. Por lo tanto, han tomado medidas contundentes para proteger tanto su economía como la privacidad de los ciudadanos del Reino Unido. Su Estrategia de ciberseguridad nacional presenta el presente plan para que el Reino Unido tenga confianza, capacidad y resiliencia en un mundo digital que evoluciona rápidamente. La amenaza cibernética no puede eliminarse totalmente. Las tecnologías digitales funcionan porque son abiertas, y esa misma apertura conlleva el riesgo. Lo que resta es reducir la amenaza para asegurar su mantención a la vanguardia en la revolución digital. Esta estrategia explica cómo lograrlo. A continuación, una síntesis de la referida estratagema:[45]

28.1. Defender. Tienen los medios para defender al Reino Unido contra las ciberamenazas que evolucionan, para responder eficazmente a los incidentes, para asegurar que las redes, los datos y los sistemas del Reino Unido estén protegidos y sean resilientes. Los ciudadanos, empresas y el sector público tienen los conocimientos y las habilidades para defenderse.

28.2. Disuadir. El Reino Unido será un blanco difícil para toda forma de agresión en el ciberespacio. Detectan, entienden, investigan e interrumpen las acciones hostiles

[44] REYES BENZ, Arlette Belén. *Ob. Cit.* pp. 131- 133.
[45] MINISTERIO DE HACIENDA DEL REINO UNIDO. *Estrategia de ciberseguridad nacional 2016-2021*. En línea: Recuperado en fecha 30/09/21 de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf. Pp. 4- 7.

emprendidas en su contra, persiguen y enjuician a los infractores. Tienen los medios para tomar medidas ofensivas en el ciberespacio, si deciden tomarlas.

28.3. Desarrollar. Cuentan un sector de ciberseguridad innovador, cada vez más grande, respaldado por investigación y desarrollos científicos líder en el mundo. Tienen una cartera de talentos en curso autosostenible que brinda las habilidades para responder a sus necesidades nacionales en los sectores público y privado. Su análisis y experiencia de vanguardia permitirán al Reino Unido cumplir y superar las amenazas y desafíos futuros.

Respaldando estos objetivos, buscarán que haya ACCIÓN INTERNACIONAL y emplearán su influencia para invertir en alianzas que den forma a la evolución global del ciberespacio de tal modo que apalanque sus intereses económicos más amplios y de seguridad. Fortalecerán los vínculos con sus socios internacionales más cercanos, reconociendo que esto mejora su seguridad colectiva. También desarrollarán las relaciones con nuevos socios para fortalecer sus niveles de ciberseguridad y proteger los intereses del Reino Unido en el extranjero. Lo harán tanto de forma bilateral como multilateral, incluidos la UE, la OTAN y las Naciones Unidas. Enviarán mensajes claros sobre las consecuencias para los adversarios que amenazan con dañar sus intereses, o los de nuestros aliados, en el ciberespacio.

Para lograr estos resultados en los próximos cinco años, el gobierno del Reino Unido busca intervenir de manera más activa y realizar una mayor inversión, al seguir apoyando a las fuerzas del mercado para elevar los estándares de ciberseguridad en el Reino Unido. El gobierno del Reino Unido, en alianza con las administraciones descentralizadas de Escocia, Gales e Irlanda del Norte, trabajará con los sectores privado y público para asegurar que las personas, las empresas y las organizaciones adopten los comportamientos necesarios para estar a salvo en Internet. Establecerán medidas para intervenir (cuando sea necesario y dentro del ámbito de nuestras competencias) e impulsar mejoras en el interés nacional, sobre todo en relación con la ciberseguridad de sus infraestructuras nacionales críticas.

El gobierno del Reino Unido aprovechará sus capacidades y las del sector para desarrollar y aplicar medidas de ciberdefensa activa para mejorar significativamente los

niveles de ciberseguridad en las redes de todo el Reino Unido. Estas medidas incluyen minimizar las formas más comunes de ataques por phishing, filtrando las direcciones IP nocivas, y bloqueando activamente las actividades maliciosas online. Mejorar la ciberseguridad básica hará que aumente la resiliencia del Reino Unido ante las ciberamenazas que se efectúan más comúnmente.

Crearon el Centro de ciberseguridad Nacional (NCSC por sus siglas en inglés) para que se convierta en la autoridad sobre el entorno de ciberseguridad del Reino Unido, para compartir conocimientos, responder a las vulnerabilidades sistémicas y brindar liderazgo sobre cuestiones clave de ciberseguridad nacional. Se asegurarán que todas nuestras fuerzas armadas sean resilientes y tengan las ciberdefensas necesarias para proteger y defender sus redes y plataformas, para seguir operando y conservando su libertad de acción global a pesar de las ciberamenazas. Su Centro militar de operaciones de ciberseguridad trabajará de cerca con el NCSC y se asegurará de que las fuerzas armadas puedan prestar asistencia en caso de recibir un ciberataque nacional importante.

Contarán con los medios para responder a los ciberataques tal y como responden a cualquier otro ataque, utilizando la capacidad más apropiada, incluida una cibercapacidad ofensiva. Utilizaremos la autoridad y la influencia del gobierno británico para invertir en programas que respondan a la escasez de habilidades en ciberseguridad del Reino Unido, desde las escuelas y universidades hasta toda la fuerza laboral. Lanzarán dos centros de ciberinnovación para impulsar el desarrollo de ciberproductos de vanguardia y nuevas empresas de ciberseguridad dinámicas. También asignarán una proporción del Fondo de defensa y ciberinnovación de 165 millones de libras esterlinas para apoyar adquisiciones y contratación en defensa y seguridad innovadoras.

29. TENDENCIAS.

Las entidades de los sectores del gobierno, la defensa, los think tanks y las ONG continuarán siendo los objetivos prioritarios de sus operaciones. Estas intrusiones, probablemente, serán respaldadas por proveedores de los sectores de telecomunicaciones y

tecnología, y pueden incluir compromisos en la cadena de suministro, como se ha observado en los años precedentes. Es de esperar que los futuros ciberataques incrementen su volumen y su sofisticación. Los siguientes párrafos esbozan lo que cabe esperar del inmediato futuro:[46] i) Aumentarán los ciberataques patrocinados por Estados, ii) Ataques a la cadena de suministro, iii) La nube como objetivo, iv) Sofisticación del código dañino, v) Los ciberataques dirigidos a personas, vi) Utilización de dispositivos inteligentes en ciberataques, vii) Permanencia de los ataques DDoS y su relación con la IoT, viii) Incremento del Criptojacking, ix) El código dañino será más engañoso, x) Aprendizaje automático para bloquear nuevas amenazas, xi) IA como herramienta en los ciberataques, xii) La adopción de 5G ampliará la superficie de ataque, xiii) Incremento de la actividad legislativa y regulatoria.[47]

30. PERSPECTIVA DESDE LOS DERECHOS FUNDAMENTALES.

Es de señalar que las consecuencias del accionar del ciberterrorismo, así como, de la indebida e insuficiente salvaguarda y protección estatal, vulnera sistemática como preocupantemente los derechos fundamentales de la población, empresas y sector público, de los derechos fundamentales vulnerados: a la vida, salud, intimidad, seguridad privada y nacional, paz y tranquilidad, libre desarrollo de la personalidad, libertad, propiedad, entre otros.

31. ANÁLISIS.

En un futuro próximo es muy probable que a través del ciberterrorismo corromper los sistemas bancarios, inhabilitar las transacciones financieras y las operaciones bursátiles, provocando que los países afectados pierdan la confianza en los sistemas económicos. Este

[46] CENTRO CRIPTOLÓGICO NACIONAL. *Ob. Cit.* P. 44.
[47] CENTRO CRIPTOLÓGICO NACIONAL. *Cit.* Pp. 44- 47.

tipo de medidas es uno de los principales objetivos del terrorismo, que consiste en tomar una país a la anarquía, el miedo y la desestabilización a través de las nuevas tecnologías.[48]

El ciberespacio es, lamentablemente para algunos, un excelente medio para que grupos -como aquellos conformados por los terroristas- puedan actuar de manera verdaderamente transnacional y, por ello, la comunidad internacional deberá de buscar mecanismos que efectivamente le otorguen una respuesta trasnacional.[49]

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además, no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas.[50]

Uno de los objetivos de la estrategia de seguridad, es poder legislar sobre todos los delitos que se cometen en este nuevo espacio delictivo del ciberespacio donde no hay fronteras, ni limitaciones en cuanto al poder de la acción basado en el anonimato, al alcance de todos y con gran repercusión social y mediática, pero ejercido siempre desde la búsqueda de la justicia, eficacia y respeto de los derechos humanos. Luego los países deberían estandarizar los nuevas figuras delictivas y legislaciones antiterroristas. Entonces, el control, actualización y estandarización se constituyen de basilar importancia para la lucha contra el ciberterrorismo.[51]

Ergo, un Estado democrático de Derecho no puede elaborar normas específicas que introduzcan excepciones a la prohibición de la tortura, tengan que aplicarse *ex ante* o *ex post*, tanto por razones normativas como iusfilosóficas: la tortura atenta contra la dignidad humana. Por tanto, no está legitimada la regulación de autorizaciones judiciales o

[48] BENTO, André. *Ciber-guerra: Ciber-ameaças*. En línea: Recuperado en fecha 30/09/21 de https://core.ac.uk/download/pdf/62695872.pdf. Lisboa, 2008, p. 11.
[49] CORONADO CONTRERAS, Laura Verónica. *Ob. Cit.* P. 455.
[50] CANDAU ROMERO, Javier. *Cit.* P. 317.
[51] PONS GAMÓN, Vicente. *Ob. Cit.* P. 424.

gubernamentales que posibiliten su práctica. Ahora bien, tampoco pueden establecerse exenciones y procedimientos concretos para supuestos de torturas, aplicables *a posteriori*.[52]

En un mundo digital hiperconectado, las amenazas pueden venir desde cualquier lugar, y el riesgo se dispara. Afortunadamente las redes de mando y control que se encargan de la seguridad de sistemas militares, por ejemplo, están aisladas de Internet lo que imposibilita el ataque externo. Pero otros sistemas críticos, como las centrales nucleares por ejemplo, utilizan

ordenadores personales que si están conectados a Internet.[53]

Tenemos mucho que aprender y muchos que trabajar en el transcurso de los años. Desde la publicación del Global Trends 2030 se recomendaba a los países prepararse en los próximos cinco años para hacer frente al ciberterrorismo, algo que no sucedió en Perú, pero que ya muchos países del mundo vienen discutiendo. Debemos aceptar la dura realidad y afirmar que, por alguna extraña razón, no estamos listos para el cambio y no parce ser prioritario para nuestros legisladores. Cada día la criminalidad va avanzando y el país pretende enfrenta a esta corriente con leyes no funcionales y con códigos ahora modificados, pero bajo sombras de mundos de fantasía. Si antes pretendíamos luchar con códigos originarios de los años 80, ahora luchamos sin guía y sin conciencia de lo que sucede en el mundo. Todavía nos queda un par de puertas que abrir y cerrar, pero es un trabajo duro y de mucha colaboración entre muchos sectores, entre nuestros propios *multistakeholders*.[54]

El informe anual que realiza la empresa de seguridad McAfee se llegó a sostener que vamos camino de una "guerra fría cibernética". De ahí, que se pueda llegar a decir que la

[52] LLOBET ANGLÍ, Mariona. *Terrorismo y "guerra" contra el terror: límites de su punición en un Estado democrático*. En línea: Recuperado en fecha 30/09/21 de https://www.tdx.cat/bitstream/handle/10803/7307/tmll.pdf;sequence=1. Barcelona, 2008, p. 430.
[53] JIMÉNEZ, Carlos. *Ciberterrorismo. Algunas reflexiones personales*. En línea: Recuperado en fecha 30/09/21 de https://www.coit.es/sites/default/files/archivobit/pdf/carlosjimenez.pdf. Madrid, 2006, pp. 56- 57.

[54] SANTIVAÑEZ ANTUNEZ, David Alonso. *Cit.* Pp. 165- 166.

ciberguerra, la ciberdelincuencia y el ciberterrorismo sean unas de las mayores amenazas a las que tendremos que hacer frente en el siglo XXI.[55]

Cabe señalar, que combatir los ciberataques y el ciberterrorismo desde el exclusivo como excluyente balcón de la ciberseguridad y nuevas tecnologías, deviene en quimero, desacertado. Ello, en el entendido que lo que más bien corresponde es tener en cuenta que en principio lograr un 100% de ciberseguridad resulta imposible. Luego, es de considerar que dicha problemática presenta una naturaleza interdisciplinar y es precisamente bajo dicha perspectiva que tiene que asumirse su combate.

Por otro lado, amerita dejar constancia que si lo que busca es la efectiva, contundente como asertiva manera de anular o erradicar el ciberterrorismo, lo que corresponde es ir hacia la determinación de los orígenes que ocasionaron su aparición (y es que señalar que aparecen como producto negativo o desventajoso del auge y desarrollo de las nuevas tecnologías, no deviene en razón suficiente). Una vez determinados los mismos, será bastante más sencillo abrazar su control. A propósito, a manera de ejemplo podemos citar el origen o explicación del origen del terrorismo y se tiene que el mismo se gestó debido a razones como: la postergación, discrimación, falta de oportunidades, de sectores alejados de las metrópolis, esto es, de sectores donde la presencia del Estado deviene en mínima o nula. Entonces, lograr determinar las razones que fermentaron la aparición del ciberterrorismo se constituiría en un gran derrotero.

Así también, es de referir que la modalidad del accionar del ciberterrorismo en el Internet de las cosas preocupa muy de sobremanera. Debido a que dicha modalidad delictiva involucra una toma casi completa del manejo de la administración de los aparatos eléctricos con los que cuenta un hogar. Entonces, ello se constituye en inmanejable y amerita tomar las urgentes cartas en el asunto, a efectos de apuntar a su urgente como efectiva salvaguar del Internet de las cosas.

[55] SÁNCHEZ MEDERO, Gema. *Cibercrimen, ciberterrorismo y ciberguerra: Los nuevos desafíos del S. XXI.* En línea: Recuperado en fecha 30/09/21 de http://www.saber.ula.ve/bitstream/handle/123456789/36770/articulo9.pdf?sequence=1&isAllowed=y. Mérida, 2012, p. 264.

El ciberterrorismo ha venido demostrando que se encuentran en condiciones muy superiores que la totalidad de países del orbe. Ello, en lo relacionado a sus altos conocimientos de cibernética y nuevas tecnologías. Lo que es factible colegir en la permanente como enorme dificultad que los mismos puedan hacer uso de los mismos para desarticularlos e impedir su muy peligroso accionar.

Continuando con lo relacionado al gran nivel de conocimientos que el ciberterrorismo ostenta, habría que considerar que no necesariamente la Internet constituiría una decisiva aliada en razón a la ínfima inversión para su maléfico accionar. Ello, en razón a que queda claro que la inversión empleada para su permanente capacitación, especialización y actualización (de manera harto anticipada a los Estados del mundo), no debe ser decimal.

Huelga apuntar, que el tema de preocupación mayúscula resulta ser que tal como se ha desarrollado en el presente trabajo, esto es, que el Estado se constituiría en la mayor amenaza de ciberterrorismo (incluso a le fecha su actuación no es menor), debido que la obligación del Estado es precisa como contrariamente garantizar un ciberespacio libre de riesgos y amenazas a la población (como ya se expuso, abrazar una ciberseguridad al 100% deviene en quimera). Ello *a fortiori*, debido que el Estado no solo es el obligado a garantizarlo, sino que además, a diferencia de la población y empresariado, cuenta en gran medida con el presupuesto y su caso, con la voluntad política, para tales efectos.

Huelga acotar respecto de la celebración de una fecha emblemática, esto es, los 75 años de creación de la Organización de las Naciones Unidas, es de verse que en lo corresponde a los dos temas más álgidos coyunturales que azotan a la humanidad, como son, los efectos del COVID- 19 y el crecimiento acelerado del ciberterrorismo, dicha organización no ha justificado su quintaesencia, la misma que se resume en mantener la paz y seguridad, así como, prevenir y eliminar las amenazas de los países del orbe. Nada que celebrar, por cierto, a la vez de constituir en una muy penosa como preocupante realidad.

32. CONCLUSIONES.

El ciberterrorismo se constituye en una de las desventajas del arribo y desarrollo incontenible de las nuevas tecnologías. No obstante, su combate y erradicación pasa por apuntar a la determinación del origen o motivaciones de su aparición.

Las personas que laboran en empresas e instituciones a cargo de información confidencial, se constituyen en potenciales blancos de captación por parte del ciberterrorismo.

El combate contra el ciberterrorismo no debe ser entendido exclusiva como excluyentemente desde los predios del Derecho, sino, desde una mirada interdisciplinar acorde a sus orígenes y causas.

Resulta imperativo garantizar la navegación en el ciberespacio libre de riesgos de ciberterrorismo.

Resulta imprescindible la voluntad política estatal, a efectos de liderar una lucha urgente e insoslayable en contra del ciberterrorismo.

El ciberterrorismo viene demostrando desde su aparición, que comanda conocimientos muy superiores respecto de informática y nuevas tecnologías. Ello, relación a los que manejan los especialistas del orbe, al punto que se haya tenido que considerar la unión global estatal para fortalecer los conocimientos de ciberseguridad, a efectos de lograr una reforzada política de lucha contra el ciberterrorismo.

El accionar del ciberterrorismo, así como, la nula respuesta de parte del Estado y del sector empresarial, esto es, el no establecimiento de las garantías ante los efectos de las ciberamenazas; vulneran los irrestrictos derechos fundamentales no solamente de los cibernautas, *verbi gratia*: a la vida, salud, intimidad, seguridad privada y nacional, paz y tranquilidad, libre desarrollo de la personalidad, libertad, propiedad, entre otros.

Resulta muy preocupante que los Estados se constituyan en sujetos activos del ciberterrorismo, a través de los *fake news.*

33. SUGERENCIAS.

Determinar el origen o factores que dieron origen a la aparición del ciberterrorismo.

Las políticas de Estado de lucha contra el ciberterrorismo, deben ser asumidas desde la interdisciplinariedad.

La capacitación y especialización en informática de tecnología de punta en ciberseguridad.

Capacitación y concientización en temas de fidelidad a quienes laboren en sectores que trabajan con información confidencial.

Capacitación y concientización en derechos fundamentales en los diversos niveles del sector educativo. Así como, en el sector estatal y empresarial público y privado.

Establecimiento de un plan nacional de lucha contra el ciberterrorismo.

Amerita la dación de una norma legal global, que regule el fenómeno del ciberterrorismo.

34. REFERENCIAS BIBLIOGRÁFICAS.

BELDING, Greg. *Spotlight de malware: ¿Qué es APT?*. En línea: Recuperado en fecha 30/09/21 de https://resources.infosecinstitute.com/topic/malware-spotlight-what-is-apt/. 2019.

BENTO, André. *Ciber-guerra: Ciber-ameaças*. En línea: Recuperado en fecha 30/09/21 de https://core.ac.uk/download/pdf/62695872.pdf. Lisboa, 2008.

BOLAÑOS RODRÍGUEZ, Ricardo. *Ciberterrorismo: una amenaza a la seguridad nacional*. En línea: Recuperado en fecha 30/09/21 de http://biblio.upmx.mx/tesis/195364.pdf. Ciudad de México, 2018.

CANDAU ROMERO, Javier. *Estrategias nacionales de ciberseguridad. Ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. Madrid, 2010.

CENTRO CRIPTOLÓGICO NACIONAL. *Ciberamenazas y tendencias 2019*. En línea: Recuperado en fecha 30/09/21 de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html. Madrid, 2019.

CESPEDOSA RODRÍGUEZ, Carolina. *Yihadismo, internet y ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30875/BorradorTFG_Ciberterrorismo_CarolinaCespedosa%20%281%29.pdf?sequence=1&isAllowed=yhttp://www.revistasculturales.com/xrevistas/PDF/72/1874.pdf. Madrid, 2019.

CONTRERAS, R. *El ciberterrorismo se viste de phishing. Arrecian los ataques que utilizan Covid-19 como señuelo*. En línea: Recuperado en fecha 30/09/21 de https://recursos.bps.com.es/files/960/78.pdf. Barcelona, 2020.

CORONADO CONTRERAS, Laura Verónica. *La libertad de expresión en el ciberespacio*. En línea: Recuperado en fecha 30/09/21 de https://eprints.ucm.es/33067/1/T36374.pdf. Madrid, 2015.

GÓMEZ VIEITES, A. *La lucha contra el ciberterrorismo y los ataques informáticos*. En línea: Recuperado en fecha 30/09/21 de https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf. Madrid.

GONZÁLEZ-GARCÍA, Abel y GIRAO GONZÁLEZ, Francisco José. *Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español*. En línea: Recuperado en fecha 30/09/21 de https://revistas.unlp.edu.ar/RRII-IRI/article/view/9489/9063. Buenos Aires, 2020.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. *E-skimming, qué es y cómo proteger tu tienda contra esta técnica maliciosa*. En línea: Recuperado en fecha 30/09/21 de https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa. Madrid, 2019.

JIMÉNEZ, Carlos. *Ciberterrorismo. Algunas reflexiones personales*. En línea: Recuperado en fecha 30/09/21 de https://www.coit.es/sites/default/files/archivobit/pdf/carlosjimenez.pdf. Madrid, 2006.

LLOBET ANGLÍ, Mariona. *Terrorismo y "guerra" contra el terror: límites de su punición en un Estado democrático*. En línea: Recuperado en fecha 30/09/21 de https://www.tdx.cat/bitstream/handle/10803/7307/tmll.pdf;sequence=1. Barcelona, 2008.

MALWAREBYTES. *¿Qué es phishing?*. En línea: Recuperado en fecha 30/09/21 de https://es.malwarebytes.com/phishing/. One Albert Quay.

MINISTERIO DE HACIENDA DEL REINO UNIDO. *Estrategia de ciberseguridad nacional 2016-2021*. En línea: Recuperado en fecha 30/09/21 de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf.

MORALES, Javier. *Tor y la deep web "La internet que no conocemos"*. En línea: Recuperado en fecha 30/09/21 de https://prezi.com/lvlu3i7yx1uj/tor-y-la-deep-web-la-internet-que-no-conocemos/. 2014.

MORÁN BLANCO, Sagrario. *La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo*. En línea: Recuperado en fecha 30/09/21 de http://www.revista-redi.es/wp-content/uploads/2017/08/8_estudios_moran_blanco_ciberseguridad.pdf. Madrid, 2017.

MUNDO CONTACT. *Los kits de creación de malware, los mayores generadores de amenazas*. En línea: Recuperado en fecha 30/09/21 de https://mundocontact.com/los-kits-de-creacion-de-malware-los-mayores-generadores-de-amenazas/. 2011.

NAVA GARCÉS, Alberto Enrique. *Ciberterrorismo: la nueva cara de la delincuencia en el siglo XXI. La participación y fomento al delito por órganos de gobierno y empresas*. En línea: Recuperado en fecha 30/09/21 de http://rabida.uhu.es/dspace/bitstream/handle/10272/17083/ciberterrorismo.pdf?sequence=2. Huelva, 2017.

NIETO FERNÁNDEZ, Ignacio. *La letalidad del ciberterrorismo*. En línea: Recuperado en fecha 30/09/21 de https://armada.defensa.gob.es/archivo/rgm/2018/07/rgm072018cap11.pdf. Madrid, 2018.

ORTA MARTÍNEZ, Raymond. *Ciberterrorismo.* En línea: Recuperado en fecha 30/09/21 de http://servicio.bc.uc.edu.ve/derecho/revista/relcrim21/art06.pdf. Carabobo.

PONS GAMÓN, Vicente. *Ciberterrorismo. Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*. En línea: Recuperado en fecha 30/09/21 de http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf. Madrid, 2018.

RAMÍREZ, Helena. *Botnet o red zombie ¿Qué es y como detectarla antes de que infecte a tu PC?*. En línea: Recuperado en fecha 30/09/21 de https://protecciondatos-lopd.com/empresas/botnet-red-zombie/. Madrid, 2020.

REYES BENZ, Arlette Belén. *Alcances del "ciber-terrorismo" en la sociedad contemporánea*. En línea: Recuperado en fecha 30/09/21 de http://repositorio.uchile.cl/bitstream/handle/2250/116821/de-reyes_a.pdf?sequence=1&isAllowed=y. Santiago, 2014.

ROCA BLÁZQUEZ, José Luis. *Cibercrimen y cíberterrorismo: ¿Exageración mediática o realidad?*. En línea: Recuperado en fecha 30/09/21 de http://oa.upm.es/32868/1/TFG_jose_luis_roca_blazquez.pdf. Madrid, 2014.

RUIZ MARTINEZ, Juan Carlos. *Código malicioso ¿Qué es y qué tipos hay?*. En línea: Recuperado en fecha 30/09/21 de https://www.ymant.com/blog/codigo-malicioso-que-es-y-que-tipos-hay/. Valencia.

S/a. *Conociendo la deep web: conceptos clave*. En línea: Recuperado en fecha 30/09/21 de https://ladycybermarketing.wordpress.com/2015/04/26/conociendo-la-deep-web-conceptos-clave/.

SÁNCHEZ MEDERO, Gema. *Cibercrimen, ciberterrorismo y ciberguerra: Los nuevos desafíos del S. XXI.* En línea: Recuperado en fecha 30/09/21 de http://www.saber.ula.ve/bitstream/handle/123456789/36770/articulo9.pdf?sequence=1&isAllowed=y. Mérida, 2012.

SANTIVAÑEZ ANTUNEZ, David Alonso. *La figura del ciberterrorismo como propuesta delictiva para la creación de una norma especial en nuestra legislación peruana*

vigente. En línea: Recuperado en fecha 30/09/21 de http://repositorio.unfv.edu.pe/handle/UNFV/2132. Lima, 2018.

SILVA, Karla. *¿Qué es el carding y los bineros?*. En línea: Recuperado en fecha 30/09/21 de https://kueski.com/blog/finanzas-personales/dinero-economia/que-es-carding/. 2020.

SOFTWARELAB. *¿Qué es spam?*. En línea: Recuperado en fecha 30/09/21 de https://softwarelab.org/es/que-es-spam/.

SUBIJANA ZUNZUNEGUI, Ignacio José. *El ciberterrorismo:una perspectiva legal y judicial*. En línea: Recuperado en fecha 30/09/21 de https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf. San Sebastián, 2008.