Universidad de Valladolid

Facultad de Derecho

Grado en Criminología

Técnicas de vigilancia y contra-vigilancia para la prevención de los ataques ciber-terroristas

Presentado por:

Alberto González Toro

Tutelado por:

Dra. Dª. Beatriz Sainz de Abajo

Valladolid, julio de 2019

Reconocimiento-No comercial-Sin obras derivadas.

Reconocimiento-No comercial-Sin obras derivadas.

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra, **bajo las condiciones siguientes**:
- **Reconocimiento**: debe reconocer los créditos de la obra de la manera especificada por el autor, pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra;
- **No comercial**: no puede utilizar esta obra para fines comerciales;
- **Sin obras derivadas**: no puede alterar, transformar o generar una obra derivada a partir de esta obra.
- Si reutiliza o distribuye esta obra, tiene que dejar bien claro los términos de la licencia.
- Alguna de estas condiciones puede no aplicarse si obtiene el permiso del titular de los derechos de autor.
- Esta licencia no menoscaba ni restringe los derechos morales del autor.

TITULO: Técnicas de vigilancia y contra-vigilancia para la prevención de los ataques ciber-terroristas

AUTOR: D. Alberto González Toro

TUTORA: Dra. Dª. Beatriz Sainz de Abajo

COMISIÓN EVALUADORA:

PRESIDENTE: Dra. Dª. Beatriz Sainz de Abajo

VOCAL 1: Dr. D. Miguel López-Coronado Sánchez-Fortún

VOCAL 2: Dra. Dª. Isabel de la Torre Díez

SUPLENTE 1º: Dr. D. Carlos Gómez Peña

SUPLENTE 2º: Dr. D. Jesús Poza Crespo

SUPLENTE 3ª: Dra. Dª. María García Gadañón

CONVOCATORIA: JULIO 2019

RESUMEN

Este Trabajo de Investigación, pretende dar a conocer el amplio campo que integra el concepto de ciberterrorismo, junto a las estrategias de Investigación de las diferentes Agencias de Inteligencia Estatales. Desarrollaremos las estrategias de vigilancia y contravigilancia en la lucha de este fenómeno y la forma de combatir esta amenaza virtual tan presente en nuestros días. Haremos un recorrido sobre las técnicas de investigación cibernéticas de los diferentes Organismo Oficiales, mostrando los riesgos y amenazas producidos mediante ataques cibernéticos, así como los mecanismos para paliar los daños producidos por estos.

ABSTRACT

This research work shows the concept of cyberterrorism, along with the research strategies of the different State Intelligence Agencies. We develop surveillance and counter-surveillance strategies in the fight against this incident and how we can combat this virtual threat so present in our days. We do a tour of the cybernetic research techniques of different Official Organizations, showing the risks and threats produced by cyber-attacks, and the mechanisms to mitigate the damages produced by them.

PALABRAS CLAVE

Ciberterrorismo, Criminal, Ataques, Agencia de Inteligencia, Ciberdelincuencia.

KEYWORDS

Cyberterrorism, Criminal, Attacks, Intelligence Agency, Cybercrime.

AGRADECIMIENTOS:

En primer lugar agradecer a Dª Beatriz Sainz, la tutora de este proyecto, gracias por su paciencia y comprensión ante los imprevistos surgidos en este trabajo, agradeciendo su total profesionalidad y su alta exigencia, así como los consejos de orientación para poder finalizar este TFG. Por supuesto siempre estaré en deuda con los pilares de mi vida, mi familia, sin su apoyo la fecha de publicación seria muy posterior.

Índice de ilustraciones

Índice de tablas

Índice de gráficos

1 INTRODUCCIÓN

Este trabajo ofrece una idea del reto al que se enfrenta nuestra sociedad actual, donde bajo el concepto de ciberterrorismo, englobamos una multitud de actos y acciones producidas o bien por Organismos Estatales o por agentes de índole terrorista. Se aportará la lucha desde el punto de vista Estatal, sobre las disciplinas de investigación llevadas a cabo tanto por las Agencias de Seguridad Estatales, impulsadas por las nuevas tecnologías, como por las Fuerzas Policiales de los diferentes países donde desarrollan a diario una guerra que no se ve, que no se observa, pero que es considerada como el quinto terreno de lucha, siendo conocido como el campo cibernético, junto a los ya conocidos como tierra, mar, aire y espacio.

Bajo el nombre de la seguridad y de la lucha contra el terrorismo, la sociedad civil demanda más poder para poder investigar y prevenir atentados. Una respuesta fácil sería restringir la libertad sin mesura. Sin embargo, en la defensa de nuestra sociedad frente al terrorismo, no debemos erosionar los derechos, los valores y las libertadas que las hacen merecedoras de semejante defensa.

La definición de ciberterrorismo no es precisa y está lejos de llegar a un acuerdo que delimite claramente su ámbito, confundiéndose con el ciberdelito. No deja dudas que este concepto es la nueva cara del terrorismo tradicional, pero con el uso de las nuevas tecnologías. Como consecuencia de una masiva y sistemática filtración de información clasificada nunca antes vista, se ha visto incrementada la tensión en la relación entre Estados, siendo el punto de inicio la grave crisis creada a raíz de las filtraciones de Edward Snowden[1] , ex- técnico de la CIA, que desveló los distintos *modus operandi* de investigación global llevados por EE.UU, creando los conceptos hoy tan moda de ciberespacio, ciberespionaje de Estado y finalmente el de ciberterrorismo, este último objeto de estudio en este TFG.

Este episodio de filtraciones marca el doble ámbito al que debemos enfrentarnos para entender las investigaciones de las diferentes Agencias de Inteligencia, en aras de nuestra propia seguridad y de los límites a la violación de nuestra intimidad. Se polarizan los ideales éticos que señalan a Snowden como un traidor que filtró secretos oficiales, que afectaban directamente a la seguridad nacional, y, por otro lado, los que lo consideran un héroe, alguien que arriesga no sólo su posición, sino su vida y la de su entorno, para denunciar actuaciones

[1] Edward Snowden. Wikipedia 2019. https://es.wikipedia.org/wiki/Edward_Snowden (Consulta 6 de abril de 2019).

fuera de la ley, por la falta de trasparencia de un sistema de vigilancia, almacenamiento y captación de información nunca visto en la historia.

Estamos viviendo esta etapa como la era post 11-S, encaminando todo el esfuerzo de los gobiernos en la búsqueda, obtención y acumulación de información para posteriormente ser tratada y analizada de forma automática por los servicios de Inteligencia, sembrando la duda sobre su ética, sobre su operativa y, en especial, la finalidad que se le da a esa información. Las agencias de los países más importantes están siendo cuestionadas sobre los medios que utilizan siendo llamadas ante los diferentes parlamentos para dar explicaciones sobre estas prácticas. Como ejemplo las comparecencias de los directores del MI6[2], MI5[3] y GCHQ[4] ante el Comité de Inteligencia del Parlamento de Reino Unido. En este sentido en España, el propio general Félix Sanz Roldán, Secretario de Estado, Director del CNI español, tubo en noviembre de 2013 que comparecer[5] ante la Comisión de Secretos Oficiales.

Toda esta alarma social producida por las filtraciones de Snowden obligó a llevar a cabo estas comparecencias, para despejar o vetar estas praxis policiales de espionaje, asumiendo como reto el sometimiento de la actuación de los diferentes servicios de inteligencia a sus respectivos ordenamientos jurídicos.

El espionaje y sus diversas técnicas operativas constituyen una actividad que hunde sus raíces en la más temprana antigüedad. El espionaje ha sido y es una modalidad en la formulación del secreto en las sociedades organizadas (Navarro, 2009).

---

[2] El Espectador. *¿Qué es el MI6?*.25 de julio de 2018 https://www.elespectador.com/noticias/el-mundo/que-es-el-mi6-el-servicio-de-inteligencia-que-segun-uribe-lo-investigo-articulo-802361. (Consulta 27 de abril de 2019).

[3] Wikipedia. "*Servicio de Inteligencia MI5*".2018 https://es.wikipedia.org/wiki/MI5 (Consulta el 2 de mayo de 2019).

[4]Agencia de Inteligencia "*GCHQ*" 2019. https://www.gchq.gov.uk/section/news/welcome-to-gchq (Consulta 25 de marzo de 2019).

[5] RTVE. *"Félix Sanz Roldán, se ha mostrado dispuesto a ir a la comisión de secretos oficiales del Congreso si se le llama para hablar del supuesto espionaje de EEUU".* 29 de Octubre 2013. http://www.rtve.es/alacarta/videos/la-noche-en-24-horas/felix-sanz-roldan-se-mostrado-dispuesto-ir-comision-secretos-oficiales-del-congreso-si-se-llama-para-hablar-del-supuesto-espionaje-eeuu/2108909/#. (Consulta 27 de abril de 2019).

El informe[6] *Threat Horizon* 2020 del *Information Security Forum* (ISF), expone cómo grupos terroristas, criminales organizados, hacktivistas y *hackers* se unen con un fin colaborativo, para trabajar de manera conjunta y agrandar cada vez más el dominio cibernético, lanzando ataques contra infraestructuras críticas nacionales, lo que podría causar destrucción generalizada y caos en la sociedad atacada.

El papel actual de la Inteligencia en general y, muy especialmente, de las operaciones de espionaje y contraespionaje en el mundo contemporáneo, se están centrando en los diversos ataques considerados como ciberterrorismo de Estado, creando planteamientos restrictivos de amigo vs. enemigo o de secreto vs. abierto.

Las técnicas de vigilancia y contravigilancia no son más que una tipología de amenaza agresiva con repercusiones en varios ámbitos de la seguridad y la defensa de los intereses nacionales, por lo que la adaptación ágil y efectiva a las nuevas tecnologías es constante, aunque el fin de estas medidas es la protección ante el robo de secretos oficiales de índole económico, industrial, bancario, etc. En el informe publicado por el *Center for Strategic and International Studies* (CSIS)[7] en 2013 titulado *The Economic Impact of Cybercrime and Cyberespionage*, las pérdidas económicas por actividades de ciberdelincuencia y ciberespionaje suponen entre el 0,5 y el 2% del PIB de una nación, adaptándose los Estados soberanos a fomentar estrategias de ciberseguridad, ciberguerra y ciberdefensa.

La dificultad añadida de estudiar y documentar la vigilancia al ciberterrorismo surge con la cuestión de jurisdicción, y de los diversos ordenamientos jurídicos de los países, lo que conforma una traba difícil de saltar. Es necesario tomar medidas reales para la unificación de criterios ante la lucha ciberterrorista, detener las amenazas que nos acechan, tales como la ciberguerra, considerada como el principal problema de Seguridad al que nos enfrentamos.

---

[6] La ISF. "*Informe anual Threat Horizon*".2018 https://www.securityforum.org/research/threat-horizon-2s-start-to-shake/. (Consulta el 12 de abril de 2019).

[7] McAfee. "*Economic Impact of Cybercrime— No Slowing Down*". Febrero 2018 https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email (Consulta el 12 de abril de 2019).

El Centro Criptológico Nacional[8], define que "*la sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional*". (Centro Criptológico Nacional, 2019). Para ellos debemos mejorar la resiliencia digital ante los ciberincidentes. En el Informe de Amenazas y Tendencias del año 2018[9] se mostró un aumento del 26,55% en el año 2017, con respecto al año anterior, gestionando este centro 26.500 incidentes.

El FBI ya alertó en el año 2012, tras los atentados del 11-S, que nos enfrentamos a la mayor amenaza para nuestras democracias, estando muy presente los grupos de ciberterroristas que pueden confundirse con conceptos arraigados a la ciberdelincuencia. La CCN delimita a ocho los agentes más importantes (CCN, 2017):

1. Los Estados. A través de actividades de ciberespionaje (económico y/o político y estratégico) y cibersabotaje. Es difícil probar la autoría rondando siempre un hilo de sospecha sobre ciertos países.

2. Crimen organizado u otro tipo de agentes. Utilizan Internet como medio para obtener un beneficio económico. Se apoya en servicios de *hackers* profesionales y en lo que se ha denominado el cibercrimen como un servicio (*Cybercrime as-a-service*). Este modelo se repite en otros agentes.

3. Ciberactivismo. Justifican sus acciones con motivos ideológicos y su propósito es visibilizar o reivindicar una causa. Un ejemplo es *Anonymous*[10].

[8] El Centro Criptológico Nacional. *Funciones* del CCN 2019https://www.ccn.cni.es/index.php/es/menu-ccn-es/funciones-del-ccn (Consulta el 3 de junio de 2019).

[9] El Centro Criptológico Nacional. "*El 2017 acabará con más de 26.500 ciberincidentes en el Sector público y empresas estratégicas españolas, un 26% más que el año pasado*". https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5362-el-2017-acabara-con-mas-de-26-500-ciberincidentes-en-el-sector-publico-y-empresas-estrategicas-espanolas-un-26-mas-que-el-ano-pasado.html (Consulta el 14 de junio de 2019).

[10] RTVE. "*Anonymous'. ¿quiénes son y cómo actúan*?" 28 de febrero de 2012. http://www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml (Consulta 14 de marzo de 2019).

4. Grupos terroristas. Usan Internet para financiarse, radicalizar a su comunidad, realizar propaganda o coordinar la actuación de sus grupos de ataque. Las actividades de ataque contra servicios esenciales usando el ciberespacio por ahora es escasa.

5. Estados que utilizan los ciberataques en el marco de conflictos y/o guerras con otros países para desestabilizarlos.

6. Investigadores y particulares que actúan como un reto o una diversión a la hora de descubrir vulnerabilidades.

7. Actores internos que suelen ser empleados o ex-empleados descontentos que, por razones económicas, políticas o personales, manipulan deliberadamente los sistemas.

8. Organizaciones privadas que pueden tener como objetivo dejar fuera de juego a los sistemas de la competencia.

El ciberterrorismo encuentra un marco sencillo y preciso, pero de amplitud ilimitada donde convergen el terrorismo y el ciberespacio, acomodándose a numerosas definiciones. Valga como ejemplo la definición que hace Wikipedia[11] de este concepto como "*el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente"*. No debemos englobar todos los tipos de ataques cibernéticos como actos de ciberterrorismo, puesto que nos estaríamos alejando de la realidad, si bien el resultado de algunos ciberataques puede generar daños considerados como acciones ciberterroristas.

Existe una amenaza real y persistente ya que la tecnología monitoriza nuestra forma de vida, y, por tanto, nos puede acechar cualquier tipo de incidencia o ataque, ya sea a nuestra seguridad o a la Seguridad Nacional, presentándose como una amenaza latente, veraz y persistente en el tiempo, que no entiende de horarios ni lugares físicos, encontrando en la red su medio de ataque e intromisión.

Nos levantamos a diario con noticias relacionadas con este tipo problemas, desde ataques a servidores, suplantaciones de identidad, robos de claves, o delitos cibernéticos. Su dinámica

[11] Wikipedia. "*Concepto de ciberterrorismo*" 2019.https://es.wikipedia.org/wiki/Ciberterrorismo.(Consulta el 15 de mayo de 2019).

y rápida adaptación crea la sensación de que las diferentes normativas legislativas para el control y lucha efectiva contra este fenómeno llegan tarde.

Tanto Europa como España están adaptando sus leyes para minimizar riesgos y adelantarse a los ataques. La aprobación de Normativas y Organismos es esencial, unido a la colaboración e investigación conjunta entre países para determinar la magnitud de los ataques, tanto entre entes Estatales como empresas privadas.

El concepto de guerra lo tenemos visualizado como un frente de tanques, bombas, soldados y material militar, donde los Estados invierten miles de millones en armamento para la defensa y ataque en beneficio de la libertad y seguridad. Este concepto no deja de estar presente en nuestros tiempos, si bien deberíamos de ampliarlo a la inversión que se está desarrollando en la nueva era digital, debiendo diferenciar el ataque informático del ataque de índole ciberterrorista.

Si bien no toda conducta en la red es ilegal o debe ser considerada como criminal, tal como señala el Dr. Acurio del Pino[12], que acomoda el delito informático como: "*todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera*".

Esta guerra digital utiliza otro tipo de armas, como la creación de software espía y virus informáticos, con efectos que abarcan desde la paralización de hospitales o aeropuertos hasta la misma destrucción de una planta nuclear, todo esto a golpe de clic. Como ejemplo la noticia del País[13], con la paralización de los sistemas informáticos de Baltimore, debiendo valorar este ataque como un referente en la capacidad de realizar estragos, en caso de orientar estos ataques hacia infraestructuras más críticas.

Este trabajo se extenderá de manera más específica sobre los medios de investigación de las agencias de Inteligencia y los Cuerpos Policiales, que emplean técnicas de vigilancia y contravigilancia para controlar, identificar y, en algunos casos, detener a los ciberterroristas.

---

[12] Acuario del Pino, Santiago. Delitos Informáticos: Generalidades. Págs. 10-11. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf (Consulta el 14 de junio de 2019).

[13] Laborde, A. (2019). Un 'hacker' paraliza Baltimore desde hace un mes. https://elpais.com/internacional/2019/06/08/actualidad/1560014584_865307.html?id_externo_promo=enviar_email. (Consulta el 12 de junio de 2019).

La especial problemática que se tiene a la hora de documentarse, es el escaso fondo registrado existente sobre técnicas de vigilancia y contravigilancia sobre ciberterrorismo, más concretamente en el entorno cibernético. Sobre seguimiento electrónico es comprensible, por tratarte de información clasificada y de difícil acceso, por lo que es necesario reorientar la búsqueda de información hacia el ciberespionaje.

El robo de información entre Estados en la nueva era digital se personaliza con la implantación de todo tipo de alta tecnología, algunas de ellas difícilmente imaginables, para proteger al Estado o para la detención de los ciberterroristas.

La característica principal de los programas y técnicas espías/investigación es la sofisticación, por los que los agentes deben tener un conocimiento y formación especializada en estos programas, así como de la interpretación de los datos obtenidos. Estos profesionales deben ser un garante de éxito que finalizará con la detención de los ciberterroristas y posterior puesta a disposición judicial.

Este tipo de información se obtiene de libros sobre ciberdelincuencia, videos de seguridad cibernética en YouTube, canales especializados en ciberseguridad y podcast alojados en la App de Android iVoox, llegando a la misma conclusión que la respuesta obtenida por parte de la web www.realinstitutoelcano.org, donde se solicitó información sobre defensa y ciberseguridad, respondiendo vía email los expertos en esta materia "*que la mayoría de información sobre ciberseguridad se encuentra declarada como Reservado, por lo que no pueden remitir ni aconsejar información específica*", si bien si nos remitían a encontrar en fuentes abiertas.

Al ser materia sensible para la Seguridad Nacional de un país es necesario precisar conceptos como ataques a ciertas infraestructuras. Este aspecto se desarrollará en el segundo capítulo.

Por lo tanto, para el análisis documental para este TFG, se utiliza una investigación cualitativa, con una técnica descriptiva, desarrollando el método hipotético-deductivo para formular los posibles *modus operandi* de los servicios de inteligencia Estatales.

La primera línea por desarrollar será centrar y delimitar el concepto de ciberterrorismo, definir sus formas y los ataques de este tipo, que se han dado a lo largo de historia moderna.

Los sistemas tecnológicos utilizados por los investigadores en materia y conocimientos son muy específicos de los Grados de Informática o de la rama de Telecomunicaciones, siendo muchos conceptos de gran tecnicidad, por lo que se han sintetizado para su mejor entendimiento y compresión en el amplio campo de la Criminología.

No cabe duda de que las empresas privadas deben invertir en sistemas de seguridad, llegando a ser hoy una parte vital y capital de toda empresa para estar protegidos ante posibles ataques de terceros, ya sea para prevenir la usurpación de información o para protegerse ante un daño gratuito de la competencia.

2 DEFINICION Y MANIFESTACIONES DE CIBERTERRO-RISMO

2.1 Definición.

La difícil delimitación conceptual del ciberterrorismo y las diferentes definiciones que se puedan dar influyen hasta en el tratamiento que se da en el ámbito jurisdiccional. Las manifestaciones del ciberterrorismo, son su principal marco para definirlo, por ello, la cita de Eloy Velasco Núñez, Juez de la Audiencia Nacional en la Ponencia[14] , lo define como el " *uso de Internet como instrumento o medio del que se vale una organización terrorista para estructurar parte de sus actividades encaminadas a sus objetivos de perturbación de la paz social o la subversión del sistema político que ataca"*, siendo una breve pero concisa explicación del amplio abanico de posibilidades destructivas de los ciberterroristas hacía la desestructuración de la seguridad en todos los frentes de un Estado.

El terror creado en forma de ciberterrorismo presenta multitud de caras, y ataca por todos los frentes desde la propia economía de un país, hasta la posible contraseña de Facebook de un usuario para la difusión o ataque de contenidos terroristas.

El primer problema es el acomodo lingüístico de la propia definición de terrorismo, existiendo multitud de propuestas[15] , dándose la misma problemática en la Asamblea General de Naciones Unidas, debido a la complejidad y amplitud del término[16] .

Por ello, la concienciación de los gobiernos sobre los ciberataques debe ser una prioridad estatal para hacer frente a intrusiones con efectos devastadores, tanto de los ámbitos civiles como militares, y dotar de recursos y soportes legales para la protección de infraestructuras

[14] Poder Judicial. Ponencia "Ciberterrorismo" http://www5.poderjudicial.es/CVdi/TEMA10-ES.pdf (Consulta 2 de mayo 2019).

[15] Ya en un estudio de 1988 se identificaban 22 elementos distintos en 109 definiciones discutidas. Vid. SCHMID, A.P. y JONGMAN, A.G., Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories and Literature, Transaction Books, New Brunswick, 1988, p.5

[16] Para un análisis de las propuestas en el seno de la Asamblea General de Naciones Unidas, Vid. SAMUEL, K.L.H., "The Rule of Law Framework and its Lacunae: Normative, Interpretative and/or Policy Created?", en SALINAS DE FRÍAS, A.M., SAMUEL K.L.H. y WHITE N.D., Counter Terrorism: International Law and Practice, Oxford University Press, New York, 2012, pp.16-21.

críticas, por el bien de la energía, los servicios básicos, el transporte, banca, etc., de esta sociedad actual.

Otra definición de este concepto es la de Mark Pollit[17], agente del FBI que estudió y desarrolló la siguiente definición operativa: "*el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos*", esta definición está enfocada más al ámbito operativo pero desgrana la complejidad de ser investigada.

Por otro lado, Centeno (2015) lo define como: "*el ciberterrorismo, también denominado terrorismo electrónico, podemos definirlo como la forma de terrorismo que más utiliza las tecnologías de información para intimidar, coaccionar o para causar daños a grupos sociales, con objeto de lograr una serie de fines políticos o religiosos*".

La magnitud de este comportamiento de generación de terror, ya sea a ataques a Estados o a la población en general, debe ser considerada como prioridad por los Gobiernos. Actualmente se puede mencionar como la guerra permanente en la red, bien por el interés en el robo de información de los Gobiernos Estatales o por las organizaciones criminales al servicio de terceros países para el mismo fin.

En España se introduce este concepto en el código penal desde el 1 de julio de 2005. Expresamente el ciberterrorismo, en el Art. 573, donde se consideran delitos de terrorismo, cuando se cometan acciones indicadas en él mediante el uso de delitos informáticos, siendo estos:

- El *hacking* y la interceptación de datos informáticos regulados en el Art. 197bis.
- El *malware malicioso* o código malicioso regulado en el Art 197 ter.
- El *cracking*, los daños informáticos y el ataque contra infraestructuras críticas, Art 264.

Actualmente, el CCN contacta con otros agentes estatales para la precoz detección de amenazas reales. Esta guerra híbrida se da cada día y se hace más presente con la rápida capacidad de adaptación de los medios de ataque.

[17] Universidad de Florida. "*Entrenamiento ciber-verdades*". https://www.ucf.edu/pegasus/training-cybersleuths/. (Consulta el 7 de abril de 2019)

En el año 2017 se detectó los ataques para intentar debilitar la democracia en vísperas de procesos electorales o promoviendo el conflicto civil. La investigación sobre el papel de Rusia[18], implicado con la llegada a la presidencia de los Estados Unidos de Donald Trump, nos muestra la alta capacidad de un ataque o manipulación y su amplia repercusión en una cita electoral. Estos ataques no cesan, tal como muestra el nuevo informe[19] del año 2018. Los ataques son de una mayor sofisticación, virulencia y osadía. Este informe nos pone en alerta sobre el ciberespionaje, como una de las amenazas más graves para la seguridad Interior. Como prueba de ello el grupo de *hackers "Shadow Broker"* consiguió, mediante un código dañino, acceder a material clasificado de Estados Unidos, llegando a revelar cómo algunos archivos sustraídos tenían el poder de ciberespionaje y facilitaba los ataques firewalls.

En el año 2017, Wikileaks informó de otra filtración[20], donde aportaba más datos sobre una wiki interna usada por la CIA, lugar donde se publicaban las herramientas de *hacking* y el código dañino producido por esta Agencia de Inteligencia. Esto nos hace ver la capacidad de intrusión que tienen tantos los organismos oficiales como los *hackers*.

Este tipo de ataques busca la información, ya sea de Estados soberanos o empresas de diferentes ramas, en especial Defensa y Tecnología, pero se pueden dirigir a personas. Como el IPhone de Ahmed Mansoor, que fue infectado por el software espía "*Pegasus*", pudiendo acceder para espiar su cámara, comunicaciones y posicionamientos GPS. En la imagen se muestra.

[18] La investigación de la injerencia rusa en las elecciones de EE. UU. en las que venció Trump en 300 palabras. (22 de marzo de 2019). https://www.bbc.com/mundo/noticias-internacional-46400948. (Consulta 14 de mayo de 2019).

[19] Centro Criptológica Nacional. Informe de Ciberamenazas y Tendencias 2018. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html. (Consulta el 1 de junio de 2019).

[20] WikiLeaks. *"Materia Oscura"* 23 de marzo de 2017. https://wikileaks.org/vault7/#Dark%20Matter (Consulta el 28 de mayo 2019).

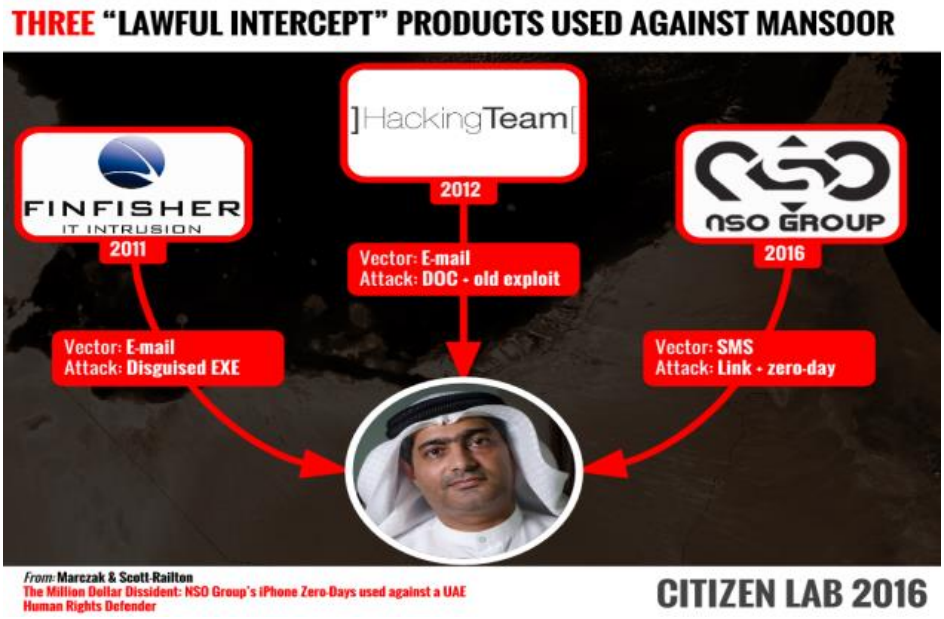

Ilustración 1. Ahmed Mansoor, the "Million Dollar Dissident"[21]

2.2 Ciberataques a infraestructuras informáticas.

Muchos ataques están tratando de acceder a los sistemas internos de las Tecnologías de la Información y Comunicación (TIC), para dañar la conexión entre la tecnología y la realidad que representan. Dependiendo del ataque pueden ser o bien a infraestructuras informáticas o a infraestructuras físicas. Midiendo su intencionalidad se clasifican en dos tipos.

1. **Ciberataques con un fin de apoderamiento del sistema informático.** Este tipo se realiza mediante *botnet*. Estos penetran en los ordenadores para controlar de manera remota el equipo. "*La palabra botnet es la combinación de los términos "robot" y "network" en inglés. Los cibecriminales utilizan virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados en una red de "bots" que el cibercriminal puede gestionar de forma remota*"[22]

[21] The Million Dollar Dissident. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (Consulta el 14 de mayo de 2019).

[22] ¿Qué es un botnet? - Definición. https://www.kaspersky.es/resource-center/threats/botnet-attacks (Consulta 13 de marzo de 2019)

Los cibercriminales utilizan redes zombis, que posteriormente venderán o alquilarán a terceros, para la emisión de *spam* o cualquier otro tipo de ataque o utilidad. Para evitar que nuestros equipos sean utilizados a modo de red o equipo Zombi, es necesario la instalación de software antimalware.

Uno de los ataques más asiduos es producido con *Denial of service* (DoS)[23], teniendo como principal función el bloqueo de una red, ordenador o servidor ajeno.

Una vez obtenido el control de los servidores de las empresas, estas envían *spam* o mensajes no solicitados para hacer propaganda, influir e infundir terror en cualquier acción, o alterar hasta un proceso electoral siendo utilizado como herramienta de uso ciberterrorista.

La contratación de personal cualificado es vital. El trabajo de *hackers* no diferencia en el modo de proceder entre el delincuente y el que intenta evitar que delincan, ya que el trabajo consiste básicamente en buscar fallos de seguridad, en aplicaciones, servidores web. En este sector tenemos a profesionales con reconocido prestigio como Sergio de los Santos[24], malagueño y máximo responsable de la división de ciberseguridad de la compañía Telefónica. Otros grandes desarrolladores de programas como Francisco López de la compañía Hispasec, presentó un antivirus llamado "Koodous"[25], que se define como un antivirus social que evoluciona por la aportación de la comunidad virtual, a través de voluntarios previamente registrados. De esta manera cuando un usuario se descarga la aplicación para Android, la App analiza la información y con los servidores de Koodous mira las coincidencias en su base de datos con otros antivirus para ser analizado posteriormente por voluntarios. De más de 15 millones de aplicaciones chequeadas, más de 4 millones tenían *malware* oculto.

La industria de la ciberseguridad se estima que gastará en torno a los 175.000 millones de euros. Así lo refleja el *Future Trends Forum* (FTF)[26] en su vigesimoquinto informe, que plantea

---

[23] Wikipedia. Definición de Ataque de Denegación de Servicio. 2019 https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio (Consulta 23 de marzo de 2019)

[24] Diario sur. Nuria TRIGUERO. "*El líder del laboratorio de ciberseguridad de Telefónica, responsable de innovación de Eleven Paths*". 2019. Noviembre.2017.https://www.diariosur.es/tecnologia/internet/sergio-santos-hacker-20171118220853-nt.html

[25] Web https://koodous.com/

[26] Fundación Bankinter. Formado por más de 500 expertos internacionales y multidisciplinares, el Future Trends Forum detecta y analiza las tendencias de innovación que cambiarán nuestro futuro próximo.19

la ciberseguridad como arma para combatir los retos de la era digital. Recomendándonos que ante la escalada futura de ataques cada vez más frecuentes, masivos, complejos y peligrosos debemos seguir y valorar las siguientes recomendaciones de FTF:

- Trabajar conjuntamente entre Estados para reducir costes.
- Diseñar la seguridad y la privacidad en las soluciones tecnológicas cumpliendo unos protocolos de obligado cumplimiento.
- Generalizar la tecnología de autenticación de doble factor que verifica 2 veces la identidad digital.
- Educar a los ciudadanos, proponiendo campañas de concienciación global donde colaborarían gobiernos, empresas y la red académica.
- Formar al consumidor digital en seguridad.
- Proteger los datos Nacionales. Crear un Órgano que vele por la ciberseguridad con la unión de los países para mantener su integridad más allá de sus fronteras.
- Exigir una responsabilidad penal para los softwares que no tengan unos estándares mínimos de seguridad.
- Elaborar e impulsar normas y leyes para estrategia de ciberseguridad a nivel global, exigiendo a los gobiernos una resolución de obligado cumplimiento.
- Relación multilateral en el ámbito público-privada para garantizar la ciberseguridad.

Resumiendo, debemos estar preparados y unidos para el desafío mundial y global al que nos enfrentamos ante estas amenazas tecnológicas. El delito y el terrorismo en la red ha pasado a estar íntimamente ligado. Debe ser combatido para asegurar la paz y la seguridad global, no haciendo dejación de funciones por ninguna de las partes con responsabilidad en la materia. De ahí la vital importancia de la colaboración público-privado para limitar el poder de las organizaciones terroristas donde la Oficina de las Naciones Unidas contra la Droga y el

Febrero 2018.https://www.fundacionbankinter.org/blog/noticia/future-trends-forum/future-trends-forum-el-think-tank-de-ciencia-y-tecnologia-de-la-fundacion-innovacion-bankinter

Delito y la Prevención del Terrorismo (UNODC)[27], ya distingue como diferentes formas de financiación del terrorismo, la recaudación directa, el comercio electrónico, el empleo de servicios de pago en línea, las contribuciones a empresas fantasmas y la financiación fraudulenta, lo que hace necesario la lucha en todos sus frentes si se quiere bloquear y tener unos niveles reales de Seguridad tanto en la red como en la vida cotidiana.

Así se creó el instituto *Search for International Terrorist Entities* (SITE)[28], un grupo de élite estadounidense que analiza la actividad on-line de los grupos terroristas, destacando que existía una campaña de reclutamiento por parte del grupo terrorista Al Qaeda, a través de la red, para viajar a Irak y atentar contra las tropas americanas desplegadas.

2. **Ciberataques con intención de obtener información confidencial**. Los terroristas vulneran la confidencialidad accediendo a los sistemas informáticos para sustraer la información confidencial y personal mediante programas informáticos.

El *spyware* es el software más característico, ya que consigue compilar información confidencial de un equipo informático sin que el dueño sea consciente de ello. Se define como *"un software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario. Recopilándose datos confidenciales (como contraseñas, números PIN y números de tarjetas de crédito), la supervisión de las pulsaciones de teclas, el rastreo de los hábitos de navegación y la recopilación de direcciones de correo electrónico"* [29].

La rápida detección de este tipo de ataque debe ser una máxima para cualquier organismo, ya que posee verdadero poder de espionaje sobre el equipo infectado. Los *spyware* los clasificamos en 4 categorías a reseñar:

1. *Spyware* troyano, capaz de infectar los ordenadores en forma de malware troyano, camuflándose en muchas ocasiones como softwares legítimos.

2. *Adware* es sinónimo de *spyware*. Se utiliza para supervisar ordenadores y dispositivos.

---

[27] La Oficina de las Naciones Unidas contra la Droga y el Delito y la Prevención del Terrorismo. 2019. https://www.unodc.org/unodc/es/terrorism/index.html (Consulta el 12 de abril de 2019).

[28] Wikipedia. "El Instituto de Búsqueda de Entidades Terroristas Internacionales".2019. https://en.wikipedia.org/wiki/SITE_Institute (Consulta el 26 de mayo de 2019).

[29] ¿Qué es el spyware? - Definición. https://www.kaspersky.es/resource-center/threats/spyware (Consulta el 16 de abril de 2019).

3. Archivos de cookies de rastreo. Consisten en rastrear los discos duros de los usuarios de la red.

4. Supervisores de sistema. Diseñados para supervisar cualquier actividad en un ordenador y capturar datos confidenciales, como pulsaciones de teclas, sitios visitados, correos electrónicos y mucho más. Este último es utilizado por los Estados como medio para vigilar las acciones de ciudadanos potencialmente peligrosos o que pudieran atentar contra la Seguridad Nacional, ya que pueden controlar el correo electrónico de ciberterroristas, observar los sitios visitados y el tipo de información que este sujeto demanda. Ya se sabe que todo lo que consultamos en los buscadores queda guardado, saltando las alarmas según qué tipo de palabras e información busquemos. A modo de ejemplo, introducir palabras claves pueden llevarnos a ser investigados por las agencias de Inteligencia Estatales, como confirma la web[30], en la entrevista realizada a Elinor Mills afirmando que Google "*confirmó esta semana que mantiene y recopila estos resultados, lo que significa que la compañía puede ser obligada a divulgarlos bajo una orden judicial*".

La gran problemática que refleja la instrucción de un *spyware* es tanto el robo de la información que poseamos, como la sustracción de claves de acceso, contraseñas de correo, etc. Lo que es utilizado, en ocasiones, para crear una doble identidad al tener todos los datos personales de la víctima, causando un perjuicio de gran magnitud.

A esto hay que añadir el daño al equipo del usuario, ya que se ralentizan las aplicaciones, se producen continuos bloqueos del ordenador o sufre sobrecalentamiento que afecta de manera irreversible al equipo.

La pregunta que se nos presenta es cómo debemos protegernos, tanto Gobiernos como particulares, ante este tipo de ataques, siendo lo recomendable empezar por no descargar archivos adjuntos de los correos electrónicos que recibamos, aunque sean de organismo solventes. La instalación de programas antivirus actualizados es uno de los ejes fundamentales para limpiar el equipo informático infectado. Existen proveedores de seguridad que ofrecen programas e información para la eliminación de *spyware*.

[30] "Usted podría ir a la cárcel por googlear ciertas palabras clave. "Blog Elinor Mills. 25 de julio de 2006. http://trueconspiracyblog.blogspot.com/2006/07/you-could-go-to-jail-for-googling.html (Consulta el 22 de abril de 2019).

La amenaza que supone para una sociedad el ataque a actividades cotidianas donde todo está conectado, como el control del fluido eléctrico, la red telefónica, el tráfico aéreo, la señalización semafórica o el propio sistema financiero, obliga la creación de unidades especializadas tanto de índole policial como militar, para dar una respuesta operativa y eficiente que dé garantías de control y seguridad ante posibles ataques a la red y a la seguridad Nacional. Se citan a diario muchas noticias en blogs y web especializadas relacionadas con ataques provenientes del ciberterrorismo en el entorno informático como:

- Corte de la electricidad y descontrol de las centrales nucleares, lo que nos llevaría a una tragedia sin precedente.
- Colapso de la red telefónica y sistemas de comunicación, ya se están produciendo alertas de que es posible que esté ocurriendo actualmente este tipo de acciones, como demuestra la caída de grandes compañías como WhatsApp, Instagram o Facebook, tal como revela la noticia del periódico digital la Vanguardia[31]
- Desarrollo contra sistemas militares de comunicación.
- Tentativas de provocar caos financiero como la paralización de bolsas, borrado de cuentas corrientes o supresión de clientes bancarios.
- Intervención del control del tráfico aéreo para provocar colisiones.
- Destrucción de grandes bases de datos estatales que pudieran ser tan sensibles como las bases de la Policía o la Guardia Civil.

En el año 2005 la asociación Americana de Ingenieros IEEE-USA[32], formada por expertos en el conocimiento avanzado de las nuevas tecnologías, divulgaron en sus estudios la vulnerabilidad de muchas redes y sistemas en Estados Unidos, dando pie a la pérdida del control, radicando aquí la gravedad de ciertos tipos de ataques con consecuencias graves y de resultado inimaginable.

---

[31] Periódico la Vanguardia. *WhatsApp, Facebook e Instagram sufren una caída a nivel mundial de dos horas.14 marzo de 2019*. https://www.lavanguardia.com/tecnologia/20190414/461640411274/whatsapp-instagram-facebook-caen-nivel-mundial.html (Consulta el 1 de junio de 2019).

[32] IEE. Instituto de Ingenieros Eléctricos y Electrónicos. 2019. https://www.ecured.cu/IEEE (Consulta el 28 de abril de 2019)

2.3 Ciberataques a infraestructuras físicas

La seguridad física de estas instalaciones debe incorporar una serie de medidas extremas para la prevención y detección de amenazas, para preservar los recursos y la información confidencial de estas.

Este compendio de recursos debe abarcar tanto los controles y mecanismos de seguridad interior y perimetral del Centro de Proceso de Datos, junto a los medios de acceso remoto que puedan detener y proteger el hardware y los medios de almacenamiento de datos de posibles ataques cibernéticos.

Diversas fuentes[33] señalan posibles escenarios críticos como pueden ser los "ataques bluetooth". En el área critica de la Seguridad de los Aeropuertos, el autor Simón Roses[34], menciona el ataque Blueborne[35], como un agujero de seguridad de bluetooth descubierto hace un año, que procede de las debilidades de la tecnología Bluetooth, que ha provocado que actualmente millones de móviles y ordenadores estén desprotegidos. La compañía Armis lo señalo como el nuevo vector que denomina BlueBorne[36], dando una explicación más técnica y sofisticada caracterizando su capacidad de propagarse por el aire y atacar a dispositivos a través de Bluetooth.

Armis también reveló ocho vulnerabilidades relacionadas, cuatro de las cuales están clasificadas como críticas BlueBorne, permite que los atacantes tomen el control de los dispositivos, accedan a datos y redes corporativas, con capacidad de penetración en redes seguras con huecos de aire y diseminen *malware* lateralmente a dispositivos adyacentes. Un

---

[33] "*Ataques inalámbricos, y el desconocimiento general de la sociedad*". Pablo F. Iglesias. .https://www.pabloyglesias.com/mundohacker-bluetooth/ . (Consulta el 3 de mayo de 2019).

[34]El Confidencial. "*Amenaza ciberterrorista en España: estos son los escenarios (y cómo nos defiende*). Merce Molist 15/10/2018.https://www.elconfidencial.com/tecnologia/2018-10-15/ciberterrorismo-ciberseguridad-guardia-civil-hackers_1630141/ (Consulta el 11 de junio de 2019).

[35] Xataba. "*BlueBorne, así es la vulnerabilidad de Bluetooth que afecta a 5.000 millones de dispositivos* "Yubal FM. (09/10/2017).https://www.xataka.com/seguridad/blueborne-asi-es-la-vulnerabilidad-de-bluetooth-que-afecta-a-5-000-millones-de-dispositivos (Consulta el 11 de junio de 2019).

[36] Jesús Antón. *4 de marzo de 2019. "BlueBorne RCE en Android 6.0.1* "https://jesux.es/exploiting/blueborne-android-6.0.1/ (Consulta el 2 de junio de 2019).

atacante podría introducir virus a través de este agujero. Roses explica que: "*Podría realizar este ataque en un lugar muy transitado, como aeropuertos, para instalar malware en miles de dispositivos*".

Como usuarios, la mejor defensa ante este tipo de peligro es tener el móvil actualizado siempre que sea posible, y el bluetooth apagado, si bien el desconocimiento de estas medidas por parte de los ciberterrorista podría ser utilizado como una técnica de vigilancia por parte de los agentes de Inteligencia.

Ramón Vicens, responsable técnico de Blueliv[37], firma especializada en contrainteligencia digital para ciberdefensa, define un escenario con dos componentes clave: infraestructuras críticas más la llamada guerra híbrida, que combina ataques en el ciberespacio y el mundo real.

Desde este enfoque, se cree posible un ataque contra los sistemas de energía de una ciudad. Otro ataque podrían ser los sistemas de emergencia, el bloqueo de las comunicaciones de la policía o de la maquinaria de atención sanitaria, u otro tipo de escenarios como el control de las compuertas de una presa, lo que nos llevaría a un escenario catastrófico. Para defender este frente es necesario que el Estado ayude a estas empresas a obtener una plena seguridad, apoyándolas económicamente y en su caso un asesoramiento integral, colaborando en la prevención y detección precoz de los autores de estos ataques.

Se debe igualmente invertir en tratar de filtrar y detectar lo que se conoce como *insiders*, que no es sino empleados actuales de empresas o Agencias de Inteligencia, que han obtenido acceso a datos por su posición y que utilizan para dañar ya sea a la empresa o al País que los contrató. Entraríamos en la ética profesional o vital como el caso Snowen. De esta manera, el huido, héroe o villano, según quién lo describa, tuvo total acceso a las bases de datos de la NSA, publicando posteriormente la información a la que tuvo acceso.

En los últimos años, se ha visto como el nivel de ataques graves aumenta considerablemente haciéndose eco la prensa nacional e internacional, proviniendo principalmente de potencias extranjeras, siendo actualmente los países de Centro-América, Brasil y China los que concentran el mayor número de ataques ciberterroristas, ya sea por su laxa legislación penal sobre esta materia como por la gran habilidad y formación de este tipo de individuos con alto conocimiento del ciberespacio.

[37] Empresa Blueliv. https://www.blueliv.com/ (Consulta el 13 de junio de 2019):

La actual guerra que se libra en el espacio virtual busca el total control de la información, tanto de los usuarios como de los Estados, a través de los Servicios de Inteligencia, que con procedimientos informáticos y tecnológicos intentan adquirir información confidencial del Gobierno atacado. Esta gran cantidad de información a la que acceden los servicios secretos obtienen unos parámetros reglamentados que pueden llegar a ocasionar o a controlar nuestro estilo de vida y monitorizar a sociedades enteras.

Estos ataques a través de la red proporcionan un anonimato característico, alejado de otros delitos, cometiendo estos actos ilícitos de manera individual o de manera grupal, con un fin determinado, en ocasiones con connotaciones económicas y otras más graves como ataques ciberterroristas para su posterior difusión y propaganda en la red.

El objetivo que analizaremos es hacer ver la estrategia que han desarrollado países en su entorno militar y policial para obtener una considerable ventaja en la inhabilitación de sistemas o bien para la defensa en conflictos armados.

CCN, CCN-CERT-IA-09/15, simplifica en categorías los tipos de agentes que representan una amenaza seria y consistente de criminales cibernéticos con consecuencias que pueden ser considerados como ciberataques por cibercriminales:

- Cibervandalos y *script kiddies*. Son individuos con conocimientos técnicos que actúan por ego personal para demostrar sus conocimientos, por lo que suelen demostrarlos públicamente. Realizan sus acciones como un modo de rebeldía, sin medir las consecuencias legales que estos hechos les acarrea. Se plasma este tipo de sujetos en el estudio de la empresa McAffe[38], señalando como preocupante el aumento de sus acciones y la aparición de *malware* desfasados.

- *Insiders*. Constituye uno de los mayores peligros tanto para empresas privadas como agencias estatales de Inteligencia, ya que se tratan de ex empleados de estos, que, con un fin económico, político o como una venganza, poseen datos sensibles o acceso a ellos que podrían dañar gravemente. Estos sujetos son los más requeridos por los gobiernos espías, mafias u organizaciones criminales para la infección de la red y equipo de la empresa o para la filtración de información.

[38] "McAfee CTO @ RSA: ¿Atrapando un rayo en una botella o quemando puentes hacia el futuro?" Steve Grobman el 14 de marzo de 2019.

- Ciberinvestigadores. El conocimiento y su posterior publicación de los datos de los estudios realizados por las personas que se encargan de descubrir las vulnerabilidades de la red puede ayudar a terceros malintencionados, sirviéndose de dichos conocimientos para su mejora en los posibles ataques.

- Organizaciones privadas. Ataques de ciberespionaje a la competencia para repercutir en su economía o para dañar o robar información de terceras compañías. Actualmente están apareciendo una gran cantidad de empresas para prestar este tipo de servicios por encargo con funciones de ciberespionaje industrial.

2.4 Ciberataques a infraestructuras críticas.

Está tan presente en nuestros días un posible ataque terrorista, que no somos conscientes de ello. Sólo hay que leer la prensa digital para encontramos noticias relacionadas con los ciberataques y los daños producidos por estos individuos. La mayoría están orientados más a los ciberdelitos, pero que dependiendo de la intensidad de los ataques pueden ser considerados ataques ciberterrorista si nos atenemos a su definición. Existen noticias impactantes como la publicada por el periódico digital La Razón[39], donde analiza la posible paralización de un marcapasos por parte de *hacker*s, lo que nos llevaría a pensar que cierto tipo de acciones dirigidas hacia una persona con relevancia política, económica o con responsabilidad en ciertos ámbitos críticos, daría origen a lo que se conoce como ataque ciberterrorista.

Incidentes llamativos los encontramos en ciertos pensamientos o rumores sobre formas de ejecución de acciones ciberterroristas, como ataques[40] con drones. Esta modalidad fue detectada por el Gobierno Ruso en los pasados mundiales del futbol celebrados en Moscú, donde pretendían controlar mediante software el control de los drones para dirigirlos como armas contra los hinchas de los diferentes equipos de futbol presentes.

[39] La Razón. Jorge Alcalde. "Ciberataques en el hospital: ¿los piratas pueden "hackear" un marcapasos?" 15 de abril de 2019. https://www.larazon.es/sociedad/ciberataques-en-el-hospital-los-piratas-pueden-hackear-un-marcapasos-NO22863385 (Consulta el 3 de abril de 2019).

[40] La Sexta. "Rusia desarticuló atentados terroristas que incluían ataques con drones durante el Mundial".2018 " https://www.lasexta.com/noticias/deportes/futbol/rusia-desarticulo-atentados-terroristas-que-incluian-ataques-drones-mundial_201811075be3222f0cf2bc7539b6c948.html (Consulta 6 de abril de 2019).

Un ataque cibernético que causa temor es la posible alteración de las compuertas de presas. Hay que tener en cuenta que las instalaciones eléctricas están en manos de empresas privadas, en un 80%, lo que provoca que los Gobiernos trabajen de manera coordinada para imponer el máximo grado de seguridad en instalaciones críticas.

El robo producido en la compañía aérea British Airways fue muy conocido. Se comunicaba al cliente que la aplicación móvil había sido hackeada entre los días 21 de mayo y el 5 de septiembre, consiguiente los ciber atacantes la sustracción de información confidencial de los datos personales de los usuarios, así como de los diferentes datos de las tarjetas utilizadas para el pago de los billetes de avión de los aproximadamente 380.000 usuarios de la compañía. La empresa de ciberseguridad RisklQ analizó este ataque[41], rebelando el sencillo *modus operandi* para conseguir el robo y acceso a la base de datos de British con la introducción de un pequeño código que alojaron en la web de British Airway. Detrás de este ataque está un grupo conocido como Magecart[42], que lleva activo desde el año 2015, utilizando como modo de acceso al sistema la inscripción de un script con 22 líneas que introdujeron en los servidores de JavaScript de la web de British Airways para así poder acceder a los datos de los clientes de la compañía.

Otro tipo de amenaza menos sofisticada son los producidos en la red, tal como recoge la web www.policiah50.com[43], promovidos por el autodenominado Estado Islámico[44], llamando a cometer atentados terroristas con motivo de la Semana Santa en España y utilizando la red para difundir sus ideas y crear una sensación de inseguridad en la población.

---

[41] RISKIQ. "*Dentro de la violación de Magecart de British Airways: cómo 22 líneas de código reclamaron 380,000 víctimas*". Yonathan Klijnsma. 11 de septiembre de 2018 https://www.riskiq.com/blog/labs/magecart-british-airways-breach/ (Consulta 3 de abril de 2019).

[42] Grupo de hacker http://descargar.cnet.com/news/magecart-hacker-group-caught-stealing-credit-cards-from-popular-online-shopping-plugin/ (Consulta 4 de abril de 2019).

[43] Web Policial. *"Llamada del Estado Islámico a atentar contra la Semana Santa"*. (Consulta 15 de marzo de 2019). https://www.policiah50.com/llamada-del-estado-islamico-a-atentar-contra-la-semana-santa/?fbclid=IwAR0Y5iB-rVLh-Q_uwZCmXmWzdtRoqG-C-paGTuJn5anDttmt3Wmq7ojOO7 (Consulta el 20 abril de 2019).

[44] Wikipedia. *"El estado Islámico*". https://es.wikipedia.org/wiki/Estado_Isl%C3%A1mico (Consulta el 12 de abril de 2019).

Los responsables de las FCSE ya alertan de este tipo de acciones tal como indica Luís Fernando Hernández García, del Área Técnica de la Jefatura de Información de la Guardia Civil "*se esperan acciones de alto impacto y efectos impredecibles, se habla del Pearl Harbor digital o de los ciberhuracanes, que son situaciones extremadamente complicadas"*. Es necesario leer su comparecencia[45], donde narra una visión realista del actual estado de la ciberseguridad en España.

Existe un Internet que no es accesible a los motores de búsqueda tradicionales. Es conocido como Internet profundo o invisible (*deepweb*). Es inaccesible desde los buscadores tradicionales en los que se mueven la mayoría de los usuarios. A esta web se accede con una contraseña, mediante la cual se accede a documentos en formatos irreconocibles a contenidos que requieren un control de acceso para ingresar en la base de datos. Se cree que es 500 veces más grande que la web tradicional. Los buscadores tradicionales no rastrean el 99% del contenido existente en Internet. Así se muestra en el informe de investigación sobre algoritmos para web profunda, de Brian Wai Fung[46], analizada en el blog de Columbia digital[47].

Las más conocidas son TOR e I2P. Tor se creó con el fin de proteger las comunicaciones gubernamentales, ocultando la verdadera IP del PC, impidiendo que la ubicación del usuario sea localizada. Aquí las Agencias de Inteligencia tienen su campo de trabajo moviéndose por otras normas y sistemas ocultos de datos. En este ciberespacio los ciberterroristas encuentran un lugar para seguir realizando sus actividades con mayor discreción y que les proporciona más seguridad e impunidad.

Pero no todos los datos del Internet invisible son malos o delictivos. Como ejemplo curioso ponemos las Web de la Biblioteca del Congreso de EEUU, y en España la Web de la Real Academia de la Lengua, que sólo utilizan su buscador, lo que las convierte en invisibles para

---

[45] Congreso de los Diputado. "*Comisión Mixta de Seguridad Nacional Sesión N.º 19*". 9 de Octubre de 2018..http://www.congreso.es/wc/wc/audiovisualdetalledisponible?codSesion=19&codOrgano=319&fechaSesion=09/10/2018&mp4=mp4&idLegislaturaElegida=12 (Consulta el 12 de abril de 2019).

[46] Bibliografía de Brian Wong Wai Fung 2009. http://people.csail.mit.edu/b_wong/

[47] Colombia digital. *"¿Qué es Internet invisible o Internet profunda?* "Adriana Molano 8 de enero. https://colombiadigital.net/actualidad/articulos-informativos/item/6296-que-es-internet-invisible-o-internet-profunda.html (Consulta el 1 de mayo de 2019)

los buscadores generales, lo que choca con el fin que supuestamente persiguen de divulgación de la información.

A la hora de buscar en la web profunda se utilizan metabuscadores para encontrar según qué tipo de información. Entre los ellos destacan:

- *Scirus*. Se usa para los ámbitos científicos y documentos más técnicos.
- *Freelunch*. Se usa para buscar datos de carácter económico.
- *Infomine*. Este presenta gran utilidad para la búsqueda de material escolar.

En la siguiente imagen se señalan los distintos niveles de la Internet profunda:

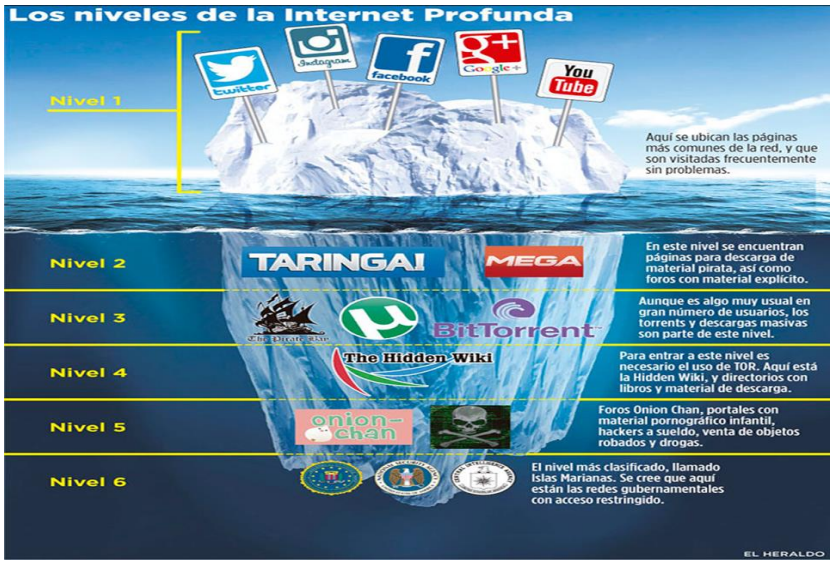

Ilustración 2. Niveles de la Internet Profunda[48]

Las mayores empresas de la red adoptan protocolos de alerta e información al usuario en caso de ser objeto de ataques o tener algún tipo de incidencia:

WhatsApp[49]. En las condiciones de servicio de esta App previenen contra el ciberterrorimo, en cuanto prohíben la difusión de contenidos que amenacen, inciten al odio o fomenten conductas criminales. Señala la prohibición del uso de medios susceptibles de generar sobrecarga en el servicio, recolectar información de terceros, así como la difusión de spam o

[48] TECNOLOGIA EN INFORMACION Y COMUNICACIONES" http://jmwtcol.blogspot.com/p/lo-que-conocemos-de-la-web-es-menos-del.html (Consulta el 2 de mayo de 2019)

[49] Web. http://whatsapp.com/contact/ (Consulta el 2 de mayo de 2019)

la suplantación de identidad, dando como solución un canal de contacto para denunciar estos hechos

YouTube. Este canal es utilizado, aunque en menor medida para la difusión de videos de propaganda terrorista. No sólo es denunciable el video, sino los comentarios que son visualizados y pueden ser la propaganda de organizaciones terroristas de toda índole. Pudiendo denunciar estos contenidos para que YouTube adopte medidas protectoras por hechos ilícitos o incitaciones de odio, amenaza o incitación a cometer ataques terroristas mediante el: marcaje de un video, marcar un comentario y marcar un canal. Para llevar a cabo estas acciones se denunciara en https://www.youtube.com/intl/es-419/yt/about/policies/#community-guidelines, donde YouTube se compromete en el plazo de 24 horas a revisar minuciosamente el video.

La mayoría de las plataformas mantienen líneas directas para denunciar estos hechos, pero no sólo servidores y páginas web son objeto de los ciberterroristas. PlayStation, consola habitual utilizada en los domicilios españoles donde se puede interactuar en red con jugadores de cualquier lugar del mundo, puede ser aprovechada para cometer ciberconductas de alcance terrorista al difundir ideología radical o conductas ilícitas. Si bien en el servicio de Sony previenen del uso inadecuado de los usuarios que incluye actividades o declaraciones discriminatorias contra la raza, sexo, ideología, etc., se detectan casos de captación e instrucción de carácter yihadista, por lo que es necesario las medidas de control a nuestros hijos focalizando la atención en el modo de jugar y la supervisión de estos, ya que la propia normativa restringe el acceso a ciertos juegos, debiendo denunciar los tutores legales del menor a la dirección de *Sony Computer Entertainment Europe Limited*, en 10 Great Marlborough Street, London, Reino Unido.

Los datos del Instituto Nacional de Ciberseguridad[50] (INCIBE) son sintomáticos en España. Se gestionaron 123.064 incidentes de seguridad en 2017, un 6,77% más que 2016. Estos ataques suelen ser de menor gravedad o intensidad, pero 431 fueron contra operadores críticos. Estas empresas gestionan infraestructuras esenciales para el funcionamiento del sector económico. Estos ataques deben evaluarse para cribar los que tenga un enfoque ciberterrorista. Los expertos señalan el auge en los próximos años. Cuando se aborda un

[50] INCIBE resuelve más de 123.000 incidentes de ciberseguridad en 2017.https://www.incibe.es/sala-prensa/notas-prensa/incibe-resuelve-mas-123000-incidentes-ciberseguridad-2017

ciberataque, es necesario tratar también cuatro puntos clave, como señala John Lyons, presidente de Alianza Internación de protección de Seguridad Cibernética[51] (ICSPA).

"El verdadero riesgo proviene ante todo del ciberterrorismo. Numerosos profesionales con conocimientos en programación, informática o con formación profesional como ingenieros, o informáticos con talento estarían totalmente dispuestos a realizar este tipo de actos si están bien pagados, lo cual podría tener consecuencias importantes en los países atacados", según informaba Eugene Kasperky, líder de reconocido prestigio en el campo de la seguridad[52], poniendo el énfasis en el aumento exponencial que se dará en los próximos años con el objetivo de obtener notoriedad y recaudar importantes cantidades de dinero.

En España se creó en 2007 el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)[53], el cual depende de la Secretaria de Estado de Seguridad. Este centro se encarga del impulso, coordinación y la supervisión de las actividades para la protección de infraestructuras críticas.

El marco normativo Internacional.

Los Estados han luchado desde siempre contra los ataques de organizaciones terroristas. Con la llegada de las nuevas tecnologías deben actualizar su normativa para acoplar el concepto de ciberterrorismo. En este camino se encuentra la Resolución 2178[54] del Consejo de Naciones Unidas donde:

> *"Exhorta a los Estados Miembros a que mejoren la cooperación internacional, regional y subregional, si procede mediante acuerdos bilaterales, a fin de prevenir los viajes de combatientes terroristas extranjeros*

[51] Nace la alianza internacional de ciberseguridad. José Tomás. 13 de abril de 2018 https://www.innovaspain.com/telefonica-alianza-internacional-ciberseguridad/ (consulta el 15 de abril de 2019).

[52] Ciberterrorismo, una amenaza latente para el mundo: Kaspersky. 1 de marzo de 2017. https://www.eleconomista.com.mx/tecnologia/Ciberterrorismo-una-amenaza-latente-para-el-mundo-Kaspersky-20170301-0054.html (Consulta el 3 de junio de 2019).

[53] El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) http://www.cnpic.es/ (Consulta el 3 de junio de 2019).

[54] Aprobada Resolución por el Consejo de Seguridad en su 7272a sesión, celebrada el 24 de septiembre de 2014 https://www.un.org/sc/ctc/wp-content/uploads/2015/06/N1454802_ES.pdf .(Consulta el 1 de abril de 2019).

desde o a través de sus territorios, entre otras cosas mediante un mayor intercambio de información con el fin de identificar a los combatientes terroristas extranjeros, intercambiar y adoptar las mejores prácticas, y comprender mejor las pautas de viaje seguidas por los combatientes terroristas extranjeros, y a que los Estados Miembros cooperen entre sí al adoptar medidas nacionales para impedir que los terroristas se aprovechen de tecnologías, comunicaciones y recursos para incitar al apoyo de actos terroristas, respetando al mismo tiempo los derechos humanos y las libertades fundamentales y cumpliendo otras obligaciones dimanantes del derecho internacional" (Organización de Naciones Unidas, 2014). En este punto de la Resolución ya plantea la necesidad de impulsar medidas para luchar contra los terroristas que se aprovechen de las tecnologías y de los recursos cibernéticos para los ataques terroristas o como medio para su financiación. Hemos visto como la cooperación entre países debe ser una máxima en las investigaciones contra actos terroristas, en particular la ayuda entre Organismo Estatales que veremos en el Capítulo 5 de este trabajo, y las agencias de Interpol, Cepol o Enisa.

El Código Penal no pierde esta visión de las posibles conductas ciberterroristas. Nuestro país, por una larga experiencia en la lucha contra ETA o Grapo, ha sabido adaptarse a los cambios normativos necesarios, focalizándose en tres modificaciones legislativas:

1. El capítulo VII del Título XXII del Libro II de la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal, se divide en dos secciones y comprende los artículos 571 a 580.[55]

[55] La sección 1ª lleva por rúbrica «De las organizaciones y grupos terroristas» y mantiene la misma lógica punitiva que la regulación hasta ahora vigente, estableciendo la definición de organización o grupo terrorista y la pena que corresponde a quienes promueven, constituyen, organizan o dirigen estos grupos o a quienes se integran en ellos.

La sección 2ª lleva por rúbrica «De los delitos de terrorismo» y comienza con una nueva definición de delito de terrorismo en el art. 573 que establece que la comisión de cualquier delito grave contra los bienes jurídicos que se enumeran en el apartado 1 constituye delito de terrorismo cuando se lleve a cabo con alguna de las finalidades que se especifican en el mismo artículo

Destacar el art. 575, que tipifica el adoctrinamiento y el adiestramiento militar o de combate o en el manejo de toda clase de armas y explosivos, incluyendo expresamente el adoctrinamiento y adiestramiento pasivo, con especial mención al que se realiza a través de internet o de servicios de comunicación accesibles al público, que exige, para ser considerado delito, una nota de habitualidad y un elemento finalista que no es otro que estar dirigido a incorporarse a una organización terrorista, colaborar con ella o perseguir sus fines. También se tipifica en este precepto el fenómeno de los combatientes terroristas extranjeros, esto es, quienes para

2. Ley Orgánica 1/2015[56] de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, Código Penal.

3. La Directiva 2013/40 UE, relativa a los ataques contra sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal[57], y de la directiva 2014/42/UE.[58]

Estas reformas legislativas pretenden regular de una manera más específica y acorde a los tiempos actuales las herramientas de lucha para los delitos informáticos en el marco de las normativas europeas y de los acuerdos suscritos de carácter Internacional.

El marco normativo de la UE.

En la UE se han dado pasos para erradicar uno de los puntos más importantes para derrotar al terrorismo, que no es otra que limitar su capacidad económica. Por ello, se ha modificado la directiva de la UE sobre el blanqueo de capitales o la financiación económica de estos grupos, la Directiva (UE) 2015/849 [59]del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y modifica el Reglamento de capitales (UE)

integrarse o colaborar con una organización terrorista o para cometer un delito de terrorismo se desplacen al extranjero.

Por último, mencionar que el art. 580 contempla que, en todos los delitos de terrorismo, la condena de un juez o tribunal extranjero será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia. Ley Orgánica 10/1995 https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3440 .(Consulta el 15 de abril de 2019).

[56] Ley Orgánica 1/2015. https://www.boe.es/buscar/act.php?id=BOE-A-2015-3439 .(Consulta el 25 de abril de 2019).

[57] DIRECTIVA 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 elativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejohttps://www.boe.es/doue/2013/218/L00008-00014.pdf .(Consulta el 25 de abril de 2019).

[58] DIRECTIVA 2014/42/UE del Parlamento Europeo y del Consejo de 3 de abril de 2014 sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea https://www.boe.es/doue/2014/127/L00039-00050.pdf .(Consulta el 25 de abril de 2019).

[59] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32015L0849 .(Consulta el 18 de abril de 2019).

Nº648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo (texto pertinente a efectos del EEE). Como novedades importantes de esta directiva está la del castigo a los que ayuden, colaboren o sean cómplices de delitos terroristas. Esto ha supuesto un arma muy eficaz de la lucha contra el ciberterrorismo y su financiación.

Este tipo de regulaciones viene a abarcar el sentido amplio de ciberterrorismo para erradicar esta lacra tan dañina. No se entiende el terrorismo sin el uso de las nuevas tecnologías, por lo que esta inseguridad nos afecta a todos, independientemente de nuestro rol o estatus en la sociedad.

Urueña Centeno (2015) define los ciberataques como "*la mayor amenaza actual*", por el grado de dependencia a las nuevas tecnologías, donde *"cualquier fallo o intrusión en un sistema informático puede causar daños irreparables*".

La UE es consciente de la dependencia de sus ciudadanos a la tecnología digital, al uso diario de la red y por tanto es necesario ofrecer un clima de seguridad a la sociedad europea. Todo el entramado depende de la necesidad de implementar medidas para la protección de las infraestructuras vitales para un Estado, como ya hemos visto en capítulos anteriores, por lo que es necesario trabajar todos los Estados miembros en una misma dirección basándonos en las estrategias enumeradas en la Tesis doctoral de Vicente Pons Gamon[60]:

- Enfoques del Mercado Único Digital.
- La estrategia global.
- La Agenda Europea de Seguridad.
- El marco conjunto para contrarrestar las amenazas híbridas.

[60] Tesis Doctoral 2018. Ciberterrorismo; Amenaza a la seguridad. Respuesta Operativa y Legislativa, Nacional e Internacional. http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf (Consulta el 12 de junio de 2019).

La política que se lleva a cabo en la UE está encuadra en varios niveles[61] para detectar los ataques en la Red, algunos de ellos son:

- La obtención masiva de datos personales.
- La manipulación de la opinión pública a través de redes sociales en procesos electorales.
- Uso de Internet para la preparación y consecución de ataques terroristas.

Aún desconocemos el alcance de nuestros Gobiernos sobre la dependencia tecnológica que presentan con las Empresas privadas encargadas de fabricar equipamiento, software, firmware o sistemas operativos, por lo que se abre otra puerta de vulnerabilidad al disponer de cierta dependencia sobre estas Multinacionales. Pero la estrecha colaboración hace que se pueda mejorar, sin perder de vista la legalidad del acceso a la información que estos soportes informáticos posean por parte de los servicios de Inteligencia. Algunas vulnerabilidades son producidas intencionadamente: *zero-day*.[62]

Desde el año 2011 se vienen armonizando la legislación en paralelo a la Unión Europea, pero debemos centrarnos en diciembre del año 2017, donde se marca claramente las necesidades de la Seguridad Nacional. En su presentación lo refleja como *"la Seguridad Nacional es un Servicio público objeto de una Política de Estado, que, bajo la dirección y liderazgo del Presidente de Gobierno, es responsabilidad del Gobierno, implica a todas las Administraciones Publicas y precisa la colaboración de la sociedad en su conjunto"*.

Las líneas para seguir se basan en la colaboración Internacional, la coordinación, la sincronización y priorización de las herramientas del Estado para la toma de decisiones para asegurar una respuesta no solo eficaz y solvente, sino también para la detección de ataques y

[61] Wegener Henning, "la ciberseguridad en la Unión Europea "Instituto Español de Estudios estratégicos. 14/07/2014. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf (Consultado el 12 de junio de 2019).

[62] Wikipédia. "*Dia Cero*" 2019. https://en.wikipedia.org/wiki/Zero-day_(computing) (Consulta el 6 de junio de 2019).

posibles respuestas a estos. En el esquema[63]siguiente mostramos las amenazas y desafíos a los que se enfrentan la Seguridad Nacional.

Ilustración 3. Amenazas y Desafíos de la Seguridad Nacional. Fuente DSN.

De igual forma se creó la Directiva NIS[64], considerada la primera parte de la legislación de la Unión Europea sobre ciberseguridad. Esta directiva proporciona medidas legales para impulsar un nivel óptimo de seguridad, obligando a los Estados Miembros a trasponer a sus legislaciones, debiendo identificar a los operadores de servicios esenciales. Estas medidas deben aumentar el nivel de ciberseguridad:

- Obligando a los Estados a contar con un equipo de profesionales para dar respuesta a incidentes. En España se crea CSIRT, para dar respuesta a incidentes de seguridad informática.

[63] Gobierno de España." *Estrategia de seguridad nacional 2017 un proyecto compartido de todos y para todos*" 2017.https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (Consulta el 6 de junio de 2019).

[64] La Comisión Europea. "La Directiva sobre seguridad de redes y sistemas de información (Directiva NIS)." (24 de agosto de 2018) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Consulta el 13 de junio de 2019).

- Creación de un grupo de cooperación, para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros, promoviendo una cooperación operativa rápida y efectiva en incidentes específicos de ciberseguridad y compartir información sobre riesgos.

- Implementar una cultura de seguridad en todos los sectores que son vitales para nuestra economía y nuestra sociedad, haciendo hincapié en las empresas que presten servicios esenciales, las cuales deberán tomar las medidas de seguridad adecuadas y comunicar los incidentes graves a la autoridad competente, al igual que los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea) deberán cumplir con los requisitos de seguridad y notificación.

Estrategia de seguridad del Estado Español

En la estrategia de la seguridad el Estado español sigue unas líneas de acción:

- Mejorar las capacidades de investigación e inteligencia, asegurar el desarrollo tecnológico de los servicios de inteligencia e información, para hacer frente al uso intensivo de las nuevas tecnologías por parte de los grupos terroristas, e impedir el acceso a las capacidades y materiales necesarios para cometer atentados.

- Reforzar los instrumentos legales en la lucha contra el terrorismo, también a nivel internacional, especialmente con el apoyo de la creación de un Tribunal Penal Internacional en materia de terrorismo (DSN, 2017, pág. 91).

Estas técnicas de ataque/defensa provienen en muchos casos de *hackers*, o cibercriminales, donde se han perfeccionado más rápido que los mecanismos oficiales, con un profundo conocimiento de la red, de la programación y de la innovación tecnológica. Avanzan en la vanguardia yendo dos pasos por encima de los medios Oficiales. Según la web www.tuexperto.com,[65] la Policía Nacional y el CNI habría contratado a *hackers*, a través de la compañía *Hacking Team,* con sede en Italia, encargada de vender herramientas de vigilancia e intrusión ofensiva a Gobiernos con sistemas de control remoto, permitiendo el control de

[65] Web Tuexperto. "*El gobierno español podrí-a haber contratado a un equipo de hackers"* Víctor S. Manzhirova. (6 julio 2015). https://www.tuexperto.com/2015/07/06/el-gobierno-espanol-podria-haber-contratado-a-un-equipo-de-hackers/ (Consulta el 1 de mayo de 2019).

las comunicaciones por la red o el descifrado de archivos y correos electrónicos, grabar llamadas de Skype y otras comunicaciones de VoIP, y activar remotamente micrófonos y cámaras en ordenadores y dispositivos móviles.

Los protocolos de seguridad son fruto de los ataques ciberterrorista producidos a infraestructuras críticas (energía, servicios básicos o banca) de las que los Estados son absolutamente dependientes y que necesitan mecanizar la respuesta para dotarla de rapidez, eficacia y eficiencia.

En España vamos a analizar el Esquema Nacional de Seguridad, y la utilización de medios electrónicos en su conjunto. Si bien algunas tienen carácter reservado, podemos ver las herramientas que se han creado para determinar los riesgos y vulnerabilidades para ofrecer una ciberseguridad efectiva.

Los objetivos del Estado abarcan varios ámbitos y la estrategia de Seguridad Nacional los divide en cinco:

OBJETIVO I: Desarrollar el modelo Integral de gestión de crisis.
OBJETIVO II: Promover una cultura de Seguridad Nacional.
OBJETIVO III: Favorecer el buen uso de los espacios comunes globales.
OBJETIVO IV: Impulsar la dimensión de seguridad en el desarrollo tecnológico.
OBJETIVO V: Fortalecer la proyección internacional de España.

Tabla 1. Objetivos Seguridad Nacional Española.

En la definición de esta Estrategia para cumplir objetivos se sirven de "*los principios rectores de la política de Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia*".

Estos objetivos conseguirán implementar unos servicios de Inteligencia con más capacidad de prevención, detección y de respuesta ante ciberataques, por lo que es necesario reforzar y agilizar la implantación de la legislación para una mayor protección a las infraestructuras críticas, sin dejar de invertir y colaborar con las empresas privadas en el desarrollo de sistemas tecnológicos que permitan la persecución del ciberterrorismo.

En la actualidad existen numerosos ataques considerados como vectores de ataque desarrollados. En el TFG[66] de Álvaro Andrés de la Cuadra, sobre "*Amenazas al personal de las FAS por medio de la ingeniería social, mediante ciberataques dirigidos, utilizando información adquirida de fuentes abiertas y redes sociales",* se indican algunos vectores que pueden ser útiles a la hora de investigar a los ciberterroristas:

- *Eavesdropping*. Consiste en interponerse entre la comunicación de dos usuarios. El objetivo es obtener la información, cuando se realiza sobre medios de la red se denominará "network sniffing" y, si se hace sobre una comunicación de voz digital.

- *Trashing*. Analiza los "desechos" o "basura" de una entidad u organización físicamente, o accediendo al equipo para obtener la información de "desecho".

- *Shoulder surfing*: Empleo de medios audiovisuales para obtener la información de interés. Un ejemplo es la intrusión en el circuito cerrado de cámaras de seguridad de una empresa determinada.

[66]TFG. "*Amenazas al personal de las FAS por medio de la ingeniería social, mediante ciberataques dirigidos, utilizando información adquirida de fuentes abiertas y redes sociales*" Andrés de la Cuadra, Álvaro.2016.http://calderon.cud.uvigo.es/handle/123456789/207 (Consulta el 12 de junio de 2019).

3 LUCHA CONTRA EL CIBERTERRORISMO Y ATAQUES INFORMATICOS.

3.1 Las TIC como herramienta de uso terrorista.

Desde finales del siglo pasado, se habla de conceptos nuevos como ciberseguridad, ciberespacio o ciberterrorista, este nuevo espacio virtual aparentemente abstracto ha sido desarrollado por nuestra sociedad marcando tendencia sobre uso y costumbres que condicionan nuestra vida.

Los terroristas no son ajenos a estos avances y al uso de las nuevas tecnologías, lo que ha llevado a dañar el ciberespacio de igual forma que un atentado terrorista cometido en un espacio físico.

El nuevo concepto de ciberterrorista pretende causar un daño internacional perpetrado al dañar los sistemas de seguridad informáticos de cualquier empresa Estatal o empresas privadas que puedan causar estragos en una sociedad, ya sea por colapso del servicio que presten o por la propia seguridad Nacional de un país.

Aunque el beneficio de las TIC es conocido por todos, los ciberterroristas han sabido hacer uso de las características que presentan estas para cometer delitos y realizar actividades terroristas. Estos ciberterrorista utilizan como arma cibernética, tal como señala el Autor 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*"[67].

Entre las características que presentan las TIC, la rapidez con la que fluye la información a todos los niveles, la propaganda de diversos actos en apenas minutos en cualquier lugar del mundo, ha dado pie a ser utilizada como arma de guerra, aunque este concepto está muy difuso por el enfoque que queramos darle. La realidad es que la ubicuidad y el bajo coste de estas hacen una herramienta actualmente esencial de los ciberterroristas, por facilitarle un anonimato que en otro espacio carece, y poner en difícil situación sus capturas por las

[67] Gómez de Ágreda, A., «*El ciberespacio como escenario de conflictos. Identificación de las amenazas*», en El ciberespacio. Nuevo escenario de confrontación, Madrid, Monografías del CESEDE Gutiérrez, A., «*¿Cómo el terrorismo islamista usa Internet*?», en file://Dialnet-Como ElTerrorismoIslamistaUsaInternet-4111887.pdfN, 2012, p. 180.

Fuerzas Policiales, debido al acceso gratuito y relativamente fácil de herramientas informáticas que obtienen a un precio reducido, facilitando el acceso a nuestra Información. Fuentes expertas[68] señalan que "el 80% de la información que busca un enemigo se encuentra en fuentes abiertas"

Desde la misma aplicación *Telegram*, se acoge multitud de comunicaciones de terroristas, tal como indica los estudios de los atentados de Paris de Charlie Hebdo en enero de 2015, donde las comunicaciones de los terroristas se habían producido por la aplicación telegrama.

La difusión posterior de estos ataques terroristas busca crear disfunciones e inseguridad en todos los aspectos de un país. La preparación no tiene porqué llegar a realizarse de manera física, sino con el alcance a los sistemas informáticos. Se pueden realizar daños inimaginables a una determinada población. Estos ataques específicos dan pie a la creación de virus informáticos, piratería de software, etc., lo que ha llevado a la regulación de los delitos tipificados en la Red, al señalar los nuevos *modus operandi* de cometer delitos como pueden ser los "*sabotajes a sistemas de seguridad, el robo de la propiedad intelectual o las actividades sobre inteligencia de personas o proyectos*"[69].

La difusión de propaganda por parte de las TIC es utilizada por los ciberterroristas para proyectar sus ideas y creencias, dándole una imagen más atractiva y atrayente. Esta técnica es muy empleada por los terroristas islamistas, utilizando todos los canales posibles para expandir sus tesis radicales. Twitter es el canal privilegiado de estos criminales, tal como menciona Carlos Suarez-Mira Rodríguez, señalando la red como *"un prodigioso instrumento de propagación y ejecución*"[70], lo que demuestra lo dicho por fuentes expertas señalando que el 60% de los terroristas detenidos entre el año 2004 y el 2010 manifestaron haber utilizado la red y en especial las redes sociales como medio en su proceso de radicalización. Esto no ha hecho nada más que crecer hasta nuestros días, por lo que es necesario prevenir la radicalización

[68] Que es Telegram. 2019 http://telegram.com.es/

[69] «Cyber War: Definitions, Deterrence, and Foreign Policy», Hearing Before The Committee On Foreign Affairs House of Representatives. First Session, September 30, 2015, p. 12

[70] Suárez-Mira Rodríguez, C., «Internet y el Derecho Penal: Viejos y nuevos delitos», en Fernández Rodríguez, J. J. (dir.), Internet, un nuevo horizonte para la Seguridad y la Defensa, Santiago de Compostela, Servicio de Publicaciones de Intercambio Científico de la Universidad de Santiago de Compostela, 2010, p. 122

por medio del ciberespacio. La puesta en práctica del Plan[71] Estratégico Nacional de Lucha contra la Radicalización Violenta arroja algunas novedades tal como refleja la imagen:

Ilustración 4. Plan Estratégico contra la Lucha contra la Radicalización violenta.

Este plan presenta como característica una única estructura nacional de carácter interministerial que será coordinado desde el M.I. que implementará y desarrollará el plan en todo su ámbito.

3.2 Actividades terroristas en Internet. Concepto de *hackers*.

El experto en ciberseguridad Álvaro Gómez Vietes desarrolla en su ponencia[72], los diferentes *hackers* que podemos encontrarnos en la red:

Hackers

Los *hackers* se dedican a estas acciones por hobby, tomándoselo como reto técnico personal, intentando entrar en sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. En ocasiones acceden a datos e información confidencial, por lo que su actividad podría ser tipificada como delito en algunos países. El perfil de estos suele ser el de una persona joven, con amplios conocimientos de la informática y de Internet, con alta cualificación e interés en las nuevas tecnologías y sus análogos como pueden ser el

[71] Gobierno de España. PLAN ESTRATÉGICO NACIONAL DE LUCHA CONTRA LA RADICALIZACIÓN VIOLENTA http://www.interior.gob.es/documents/10180/3066463/CM_mir_PEN-LCRV.pdf/b57166c1-aaaf-4c0d-84c7-b69bda6246f5

[72] EDISA. "TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS "Álvaro Gómez Vieites. 2014. https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf (Consulta el 11 de abril de 2019).

conocimiento técnico de lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, a los que dedican gran cantidad de tiempo en estas materias.

Crackers ("blackhats")

Los *crackers* son sujetos que pretenden atacar un sistema informático para obtener beneficios económicos de forma ilegal o provocar un daño motivado por intereses económicos, políticos, religiosos, etcétera.

Sniffers

Los *sniffers*, este tipo de individuos rastrean la red para tratar de acceder y descifrar los mensajes que originan los ordenadores en Internet.

Phreakers

Especializados en sabotear la red telefónica para realizar llamadas gratuitas.

Spammers

Conocidos por el envío masivo de email no solicitados a diferentes cuentas de Internet, para producir el colapso de los servidores, así como la bandeja de entrada de las cuentas de email. Algunos de estos correos contienen un virus informático o intentar realizar con falsos enlaces estafas para el apoderamiento de claves o acceso a cuentas bancarias.

Piratas informáticos

Especializados en acceso y pirateo de programas y contenidos digitales, sobrepasando la legislación sobre propiedad intelectual, cayendo en muchos casos en acciones delictivas.

Creadores de virus y programas dañinos

Son personas con alto conocimiento en programación e informática cuyos conocimientos lo emplean en la construcción de virus y otros programas dañinos, lanzándolos a la red a de Internet provocando su rápida propagación para llegar al máximo números de internautas.

Se vienen desarrollando virus cada vez más dañinos y perfeccionados que actúan con un fin delictivo vulnerando los sistemas de seguridad de las víctimas para el robo de datos personales como pueden ser sus cuentas bancarias, información confidencial o sensibles o el uso indebido de sus tarjetas de crédito.

Lamers ("wannabes"): "Scriptkiddies" o "Click-kiddies"

Se les conoce como *"script kiddies" o "click kiddies"*. Realizan ataques informáticos a través de determinados programas o herramientas que se han bajado de Internet, pero sin tener conocimientos técnicos de cómo funcionan.

Ex-empleados

Los ex-empleados bajo un móvil de venganza o despecho consiguen lo que se conoce como "bombas lógicas" una vez han accedido a los servidores de la empresa/compañía para provocar daños en los sistemas informáticos, como pueden ser el borrado de archivos, de ficheros o el envío de información confidencial a la competencia o cualquier postor que esté interesado en dicha Información. Este tipo de personas son de los más problemáticos y difíciles de detectar al tener un acceso a priori con las garantías de seguridad, por lo que con abuso de confianza se aprovechan para provocar un daño con ánimo de venganza o económicos.

Intrusos remunerados

Esto individuos son expertos informáticos que son contratados por terceros por tener un alto grado de conocimiento informático para orientarlo a la sustracción de información confidencial o producir diferentes tipos de sabotajes informáticos.

3.3 Ataques específicos.

Ya desde la guerra fría se conoce que el enfrentamiento entre Estados para tratar de influir mediante ataques en zonas de conflicto. Estos conflictos fueron utilizados por ambos bandos como un banco de pruebas, destacándose la emisión de emisiones electromagnéticas, impidiendo la comunicación del enemigo y prevalencia de la propia, lo que dio pie a lo que se conoce como COMINT[73], esta es una subcategoría de la inteligencia de señales que como misión pretende captar y tratar e los mensajes o información de voz derivada de la intercepción de comunicaciones extranjeras. Este cambio de ataques trajo consigo un cambio de mentalidad con el uso de nuevas técnicas tanto militares como de inteligencia para inhabilitar al enemigo.

[73] Wikipedia Programa de Espionaje COMINT 2019 https://es.wikipedia.org/wiki/Inteligencia_de_se%C3%B1ales#COMINT. (Consulta 1 de abril de 2019).

Un ejemplo claro es en la Primera Guerra del Golfo en el año 1991, lo militares antes de la Invasión de EEUU, recibieron correos electrónicos (email), donde el CENTCOM, una unidad Militar de Estado Unidos, les informaba de la inminente invasión de Irak así como la recomendaciones que debían de seguir, dejando a los militares Iraníes en la tesitura de si luchar o ayudar al enemigo, fruto de estos email la cadena de mando Iraní se quedó sin Oficiales y produjo una generación de dudas ante el cumplimiento de órdenes, a esto se unió el ataque con señales Electrónicas Equivocas, que produjeron la inhabilitación de los sistemas de alerta y seguridad Iraní al bloquear los centros de mando de las bases aéreas llevando a EE.UU a una entrada triunfal a comienzos de la Guerra del Golfo.

Cabe pensar que se podría atacar los ataques económicos y financieros del país, si bien debido a la política americana no se atacaron los activos financieros del régimen de Sadam Hussein, posiblemente para no dar pie a un ataque ciberbancario, lo que produciría un impacto económico a nivel mundial.

En Estonia se produjo otro incidente por la estatua del Soldado del ejército Rojo, lo que produjo un conflicto en el ciberespacio, con ataques a los servidores de las páginas webs más utilizadas en Estonia, con graves ataques DDoS, procedentes de Rusia bloqueando las paginas Oficiales.

Los estonios pensaron que se trataba de *hacker* rusos descontentos, pero la dimensión del ataque continuo con ataques a los servidores DNS, el control de la red telefónica así como el sistema de verificación del comercio electrónico, llevando a un millón de ordenadores a estar participando en esta acción, todo esto a lo largo del tiempo, teniendo que solicitar ayuda a la OTAN[74]., que con un grupo de expertos respondió con contramedidas que consiguieron

[74] Diario el País." *Los ciberataques a Estonia desde Rusia desatan la alarma en la OTAN y la UE*". RICARDO MARTÍNEZ DE RITUERTO. 18 de mayo 2017 "https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html (Consulta el 19 de abril de 2019).

identificar el origen de los ataques que los llevo hasta Rusia, como era lo esperado, con un software empleado en los BOTNETS[75], desarrollado por Cirílico[76].

Un tercer ejemplo fue el Estado de Israel con el ataque y destrucción de la planta nuclear en Siria en AL Kibar, los expertos dan como teoría más real, el ataque por parte de expertos israelíes localizando la fibra óptica de la red de defensa antiaérea Siria, consiguiendo saltarse los sistema de defensa antiaérea que permitieron un ataque no detectado por la inteligencia Siria, esta operación fue fruto del *hackeo* al software ruso, esta teoría como es lógico no está confirmada por ninguno de los Estados afectados.

En China se produjo el ataque a información clave de diversas áreas, siendo el ataque un *spyware*, que estaría actuando desde el año 2006, la afirmación provocaba acusaciones cruzadas de países tales como Corea del Sur, Japón, EE. UU y países europeos como Francia, Alemania y Reino Unido.

El mayor incidente se produjo entre las acusaciones de EEUU[77] a China por parte de militares responsable de ciberespionaje y del robo y sustracción a empresa americanas del sector enérgico estadounidense, defendiéndose el Gobierno chino de que estas afirmaciones se producen sin ningún tipo de prueba o argumento sólido.

En Georgia se dio otro de los más importantes ataques cibernéticos, con un gran esfuerzo este país intento neutralizar los ataques DDos, intentando evitar la conexión rusa si bien los atacantes modificaron la conexión para aparentar que procedían de China, estando los BOTNETS, en Moscú.

De tal gravedad fue este ataque que Georgia perdió su dominio, teniendo que trasladar todas su páginas y servidores fuera del país, produciendo que la banca desconectara los servidores para proteger tanto el capital como la información , si bien no tuvo mucha fortuna ya que los atacantes siempre fueron un paso por delante del Gobierno de Georgia y aparentando

---

[75] Kaspersky. *¿Qué es un botnet?* 25 de abril de 2013. https://www.kaspersky.es/blog/que-es-un-botnet/755/ (Consulta el 13 de junio de 2019).

[76] The Guardian. *"Rusia acusada de desencadenar la guerra cibernética para deshabilitar a Estonia.*Ian Traynor. 17 de mayo de 2017. https://www.theguardian.com/world/2007/may/17/topstories3.russia (Consulta el 07/05/2019).

[77] El PAIS. "Washington acusa a cinco militares chinos de ciberespionaje industrial. MARC BASSETS". 19 mayo 2014 https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html

ser ataques desde este país a webs bancarias internacionales lo que causaba el automático bloqueo de acceso a estas, lo que afecto a la cancelación de las líneas telefónicas y de las tarjetas de crédito.

Este caso junto al de Estonia son los dos primeros casos de ciberguerra entendida como ataques entre Estados en la red, si bien a pesar del análisis de toda la información se tomó como ataques de ciberactivistas rusos.

Lo que varió y asentó los conceptos de ciberguerra fue la denuncia del Gobierno Iraní[78], por medio de IRNA, la agencia oficial iraní, por la que detectó que ordenadores de las estaciones nucleares estaban infectadas por el gusano Stuxnet[79]. Esto consistía en el control de la información de no sólo la planta nuclear, sino la de miles de centrifugadoras de uranio en otras ubicaciones, siendo el Estado de Israel el señalado como el responsable de tal infección. Las características de este ataque fueron la capacidad de reprogramar los parámetros de funcionamiento e inhabilitarlos.

Estas dinámicas de daño hacia instalaciones, a través de la red, no son más que el uso de armas cibernéticas. Kaspersky[80] desarrolla en el boletín de seguridad 2012, las armas cibernéticas *Stuxnet* y *Duqu*, lo que dio lugar a graves problemas que nos permiten hablar de forma clara de armas cibernéticas.

Esto deja ver la multitud de acusaciones entre Estados por posibles ataques con ciberterroristas Estatales, y acusaciones de robo de información confidencial por parte de los Servicios de Inteligencia, así como la creación en la mayoría de los países de equipos de ciberguerra.

Algunos casos muy recientes son los cortes de fluido eléctrico del gobierno de Venezuela, los cuales achaca a las potencias enemigas por medio de ciberataques. Se produjo un hecho

---

[78] "Stuxnet worm hits Iran Nuclear plant staff computer" BBC (26/09/2010)https://www.bbc.co.uk/news/world-middle-east-11414483 (Consulta el 7 de mayo de 2019).

[79] El Gusano Stuxnet Ataca Planta Nuclear Iraní, Pero ¿Quién lo Creó? LoneStar https://www.enigmasoftware.es/gusano-stuxnet-ataca-planta-nuclear-iani-quien-lo-creo/ (Consulta el 2 de mayo de 2019).

[80] BOLETÍN DE SEGURIDAD DE KASPERSKY "*Las armas cibernéticas*". Diciembre 2018 https://securelist.lat/kaspersky-boletn-de-seguridad-2012-las-armas-cibernticas/72217/ (Consulta el 17 de marzo de 2019).

similar en Turquía[81] donde un apagón eléctrico afecto a 40 millones de ciudadanos acusando a Siria de estar detrás de este corte por el apoyo turco a los rebeldes de Yemen.

Otra forma de ataque a Estados es la contratación en el mercado negro de un ataque a un tercero, proyectando un ciberataque previamente contratado como ocurrió en la TV francesa en el canal TV5Monde.

La tensión entre países por estos continuos ataques, con acusaciones mutuas de espionaje y sabotajes, da un giro más formal y directo por la acusación de EEUU a militares chinos formulado por el Fiscal General Eric Holder, donde presenta la primera denuncia penal contra funcionarios oficiales de un País, en este caso China, que es el país más señalado por sus continuas acusaciones de ciberespionaje y ciberterrorismo.

Esta acusación formal basada contra la unidad 61398 del Ejército Chino, demostraba en el concepto de *Advanced Persisten Threat* (APT)[82], conocidas como el conjunto de actividades y técnicas que permiten mantener en el tiempo un ciberespionaje, dentro de una estrategia de captación de información militar, social, política y económica de un país, que la carrera por controlar la información acarrea este tipo de estrategias de seguridad.

Quien controle los sistemas del enemigo tiene gran parte de la guerra ganada, ante un posible conflicto ya sea por inhabilitación de material de guerra o por ataques a infraestructuras críticas.

Esta estrategia es conocida como el dominio de la información, misión que tenía la unidad mencionada del Ejército Chino, ante una posible intervención militar americana en China.

Existen actualmente otro tipo de APTs, (amenaza avanzada persistente), de contenido más técnico y complejo, como se observa en la Figura del ciclo de vida de una APT.

[81] Pierluigi Paganini. "*Iran accused of the blackout that paralyzed the Turkey"*. Security Affairs. 04/05/2015. https://securityaffairs.co/wordpress/36536/cyber-warfare-2/iran-accused-blackout-turkey.html (Consulta el 9 de mayo de 2019).

[82] Kaspersky. *"¿Qué es una APT*?" https://www.kaspersky.es/blog/que-es-una-apt/966/ (Consulta el 10 de mayo de 2019).

Ilustración 5. Ciclo de vida de una APT[83]

La empresa Securelist facilita todas las APTs, en un censo propio donde recoge toda la información captada por Kaspersky LABs desde 2004.

España ha sido acusada de infectar a otros gobiernos como Marruecos, Brasil y Cuba, entre otros, con el Troyano Careto, que fue descubierto por Kaspersky. Debido a la excesiva dependencia de las nuevas tecnologías es necesaria la formación y contratación de expertos.

Otro factor en el que debemos de hacer hincapié es el control gubernamental de varios como gobiernos por controlar las redes sociales, los foros de internet para marcar una línea de opinión acorde al gobierno, actualmente se promueve en España una ley para paralizar las *fake news*[84], al igual que ocurre en la Unión Europea, que ya cuenta con dos grupos de trabajo para evitar las manipulaciones y posibles bulos en unas elecciones.

Rusia va más allá y controla los medios de comunicación y ataca editoriales donde se cuestionan sus políticas en Georgia y Ucrania.

[83] Wikipedia. "*Ciclo de vida de una APT*". 2019.

https://en.wikipedia.org/wiki/Advanced_persistent_threat#/media/File:Advanced_persistent_threat_lifecycle.jpg (Consulta el 18 de marzo de 2019.

[84] RTVE. "*El Gobierno ultima una unidad contra las 'fake news' y el ciberterrorismo de cara a las elecciones*". (11 de marzo de 2019). http://www.rtve.es/noticias/20190311/gobierno-ultima-unidad-contra-fake-news-ciberterrorismo-cara-elecciones/1899380.shtml (Consulta el 1 de abril de 2019).

China actualmente es el único país del mundo que controla totalmente su red nacional, con la posibilidad de, ante un eventual ataque, limitar total o parcialmente su respuesta.

Un ataque hacia Google fue lanzado por China, quien creó una operación de ataque contra esta, denominada. Op. AURORA[85], basada en su política Zhixinquan, por la cual filtra y censura todo contenido que salga o entre en China a través de Great Fire Wall, (refiere a la gran Muralla junto a los cortafuegos Firewall). Consistía en ataques que duraron desde junio de 2009 hasta diciembre de 2009. Estudiando este tipo de ataque la empresa McAfee, descubrió que "*el objetivo principal del ataque era obtener acceso y modificar potencialmente los repositorios de código fuente en estas compañías de alta tecnología, seguridad y defensa*". La magnitud de esta Operación llegó a robar parte de las cuentas de acceso a Gmail, de disidentes chinos, apoderándose de toda la información que dispusieran.

Países como Rusia y Holanda están catalogados como críticos en cuanto a distribución de *malware* y las conexiones hacia esos países deberían estar especialmente controladas. Según Kaspersky Labs, deberían de acrecentarse los controles con variados métodos y técnicas que pueden complementar nuestros IDS/IPS y sistemas de monitorización de tráfico (en el caso de que no nos proporcionen geolocalización), para alertarnos de según qué conexión geográfica se ubique, facilitándonos el trabajo de inteligencia a la hora de ayudar a detectar *malware* dirigido.

3.4 Consecuencias de los fallos y ataques en las empresas.

La detección de incidentes se realiza con herramientas conocidas como IDS/IPS. Es un sistema de detección de intrusos. Dos son los tipos de sistema que vamos a ver: (Beltrán, 2015)

NIDS (Network IDS), de cierta complejidad este sistema contiene un sensor virtual que analiza el tráfico de red y lo compara con ataques e información conocida de actividades sospechosos, como paquetes malformados, escaneo de puertos, etc. Además de revisar y el comportamiento lógico o no del tráfico en la red. Esta herramienta se acompaña de un *firewall*, para que se ejecute de manera automática e informe de las incidencias que detecte.

[85]Wikis." *Operación Aurora"* https://wikis.fdi.ucm.es/ELP/Operaci%C3%B3n_Aurora (Consulta el 22 de mayo de 2019).

De igual forma pueden implicar respuestas automáticas ante ciertos ataques, pero pueden suponer un gran problema cuando se ejecutan en un entorno de Java, ya que esta necesita una actualización permanente de acceso a las bases de datos y a la información, llevando a interpretar erróneamente por el NIDS como un ataque.

HIDS (Host IDS), o IDS de servidor. Este sistema consiste mediante sondas de software analizar las anomalías que se producen en el equipo, emitiendo este sistema una alerta sobre el intento de desbordamiento de un búfer contra un servidor de base de datos.

Este sistema busca archivos con caracteres inusuales con antivirus que intentan analizar los logs para detectar cambios en la configuración host, como se ve entramos en una materia mucho más sofistica y técnica que requiere de expertos en ciberseguridad.

Se está trabajando en la formación del personal tanto de empresas privadas como estatales en la formación permanente y continua de los empleados para asegurar en la medida de los posibles los ataques de ciberterrorismo que puedan ser víctimas y reducir estos o moderar sus indecencias y daños en el ente.

Como en la vida misma, la seguridad en la red no es total, y estamos lejos de conseguirla ante los ciberdelincuentes y su gran dominio del entorno en el que actúan, hacen difícil su detección como es el caso de las APTS *(Advanced Persisten Threats)*, ya que emplean sofisticados métodos de ocultación, persistencia y sobre todo basadas en el anonimato.

Existen herramientas creadas para la detección y gestión de manera efectiva de la capacidad de anticipación y respuesta a las vicisitudes que detecte en una escala de peligrosidad como es la Herramienta Lucia. Vemos el Nivel de Peligrosidad de los ciberincidentes, en relación con la amenaza que suponen, del informe obtenido del CCN[86]:

[86] Gobierno de España. "Ciberamenazas y Tendencias Edición 2018" https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html (Consulta el 17 de marzo de 2019).

	Víctimas		
Agentes de las amenazas	Sector Público	Organizaciones privadas	Ciudadanos
Estados	Ciberespionaje político	Ciberespionaje económico	Ciberespionaje
	Ciberconflictos / Ciberguerra / Guerra híbrida		Guerra híbrida
	Capacidades ofensivas. Sustracción y publicación de información	Capacidades ofensivas Sustracción y publicación de información	
	Perturbación del funcionamiento de instituciones o procesos democráticos		Fake News
Organizaciones criminales	Disrupción de sistemas	Disrupción de sistemas	Disrupción de sistemas
	Robo y publicación o venta de información	Robo y publicación o venta de información	Robo y publicación o venta de información
	Manipulación de la información	Manipulación de la información	Manipulación de la información
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Organizaciones privadas		Sustracción de información (Ciberespionaje industrial)	Abuso comercial o reventa de información corporativa
Ciberterroristas (incluyendo a los ciberyihadistas o grupos terroristas de motivación ideológica o religiosa)	Disrupción / toma de control de sistemas Ataque a Infraes. Críticas	Disrupción / toma de control de sistemas Ataque a Infraes. Críticas	
	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación
Ciberactivismo	Robo y publicación de información	Robo y publicación de información	
	Desfiguraciones	Desfiguraciones	
	Disrupción de sistemas	Disrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Ciervándalos y script kiddies	Robo de información	Robo de información	Robo y publicación de información
	Disrupción de sistemas	Disrupción de sistemas	
Actores internos	Robo y publicación o venta de información	Robo y publicación o venta de información	
	Disrupción de sistemas	Disrupción de sistemas	
Ciber-investigadores	Publicación de información	Publicación de información	Publicación de información

Código de colores:	No han aparecido nuevas amenazas. o Existen suficientes medidas para eliminar la amenaza o No han existido incidentes apreciables derivados de la amenaza.	Se han observado nuevas tendencias o fenómenos asociados con la amenaza. o Existe un conjunto de medidas limitadas para eliminar la amenaza o El número de incidentes derivados de la amenaza no ha sido especialmente significativo	Existen claros desarrollos relacionados con la amenaza o Las medidas desplegadas tienen un efecto limitado en la amenaza o El número de incidentes derivados de la amenaza ha sido significativo

Tabla 2. Agentes de amenazas más significativas en 2017, tipología de sus acciones y sus víctimas[87]

Hemos desarrollado las incidencias desde la perspectiva de los ciberincidentes. Su actuación responde a un ciclo de vida escalonado, variando en función del nivel de dificultad y de los

[87] Cyber Security Assessment Netherlands. CSAN 2017. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html (Consulta el 17 de marzo de 2019).

objetivos a conseguir, siendo los más comunes las intrusiones (son ataques dirigidos a explotar vulnerabilidades e introducirse en el sistema) y el código dañino (troyano o *spyware*).

Se debe actuar de manera rápida y eficaz ya que la lentitud en dar respuesta adecuada a las vulnerabilidades agrava aún más los posibles daños, así, en dos de las crisis más conocidas de este año (la herramienta de desarrollo de aplicaciones web de Apache Struts o el ransomware WannaCry) los primeros ataques se dieron dos meses después de conocer la vulnerabilidad.

Tal como indica el informe[88] emitido por el CERT Gubernamental Nacional, ante la crisis más mediática de la historia de la ciberseguridad, la infección del WannaCry, llego a más de 230 000 de equipos Windows de todo el mundo, muchos de instituciones del gobierno y hospitales, es el ataque de *ransomware* más extendido en la actualidad, https://www.avast.com/es-es/c-wannacry se desarrolló un parche en tiempo récord, descargando dicho parche países entre ellos España, Estados Unidos, Gran Bretaña, Francia, Bélgica o Portugal.

La seguridad física de estas Instalaciones debe tomar medidas extremas para la prevención y detección de amenazas, para preservar los recursos y la información confidencial.

Este compendio de recursos complejos debe abarcar los controles y mecanismos de seguridad Interior y perimetral del Centro de proceso de datos, y de los medios de acceso remoto para proteger el hardware y los medios de almacenamiento de datos.

Diversas fuentes señalan como posibles Escenarios de crítica como puede ser "Ataques bluetooth" en aeropuertos el autor Simón Roses menciona este "ataque Blueborne", como un agujero de seguridad en *bluetooth* descubierto hace un año y aún con millones de móviles y ordenadores desprotegidos. Un atacante podría introducir virus a través de este agujero, explica Roses: "Podría realizar este ataque en un lugar muy transitado, como aeropuertos, para instalar *malware* en miles de dispositivos".

Como usuarios, la mejor defensa ante este tipo de peligro es tener el móvil actualizado siempre que sea posible, y el *bluetooth* apagado.

---

[88] Centro Criptologico Nacional."*Informe Código Dañino CCN-CERT ID-17/17*" https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2169-ccn-cert-id-17-17-codigo-danino-wannacry-1/file.html (Consulta el 18 de abril de 2019).

Ramón Vicens, responsable técnico de Blueliv[89], firma especializada en contra-inteligencia digital para ciberdefensa, define un escenario con dos componentes clave: infraestructuras críticas más la llamada guerra "híbrida", que combina ataques en el ciberespacio y el mundo real.

Desde este enfoque, cree posible, por ejemplo, un ataque contra los sistemas de energía de una ciudad, "y cuando esté a oscuras, realizas un ataque físico", otro ataque podría ser los sistemas de emergencia, como policía o atención sanitaria, y dejarlos sin comunicaciones por radio. O bien, una presa controlada por sistemas informáticos, abierta en plenas lluvias torrenciales.

Las presas son infraestructuras críticas que podrían ser objeto de un ciberataque. (Reuters). "*Son sistemas que están cada vez más informatizados y controlados por empresas privadas*", explica Vicens. Para defender este frente es necesario *"que el Estado ayude a estas empresas a obtener una plena seguridad apoyándolas económicamente y en su caso un asesoramiento integral"*. Además de realizar tareas de prevención consistentes en monitorizar a los actores y grupos que podrían realizar estos ataques.

Muchas empresas se ven abocadas al cierre, a la quiebra o la desaparición total como consecuencia de los daños ocasionados por los ataques cibernéticos.

El impacto total es bastante complejo ya que entra en juego la gravedad del ataque y el tiempo que se tardó en detectarlo, pero si podemos evaluar una serie de prejuicios que sufrirá la empresa como son:

- Horas invertidas para la reparación y reconfiguración de los equipos y redes.
- El coste por no poder hacer uso de los equipos informáticos
- El robo de información confidencial y sensible
- Como consecuencia de la filtración de información personal, nos enfrentamos a multas por los incumplimientos del deber de custodia necesario, según marca la normativa vigente.

[89] Web. https://www.blueliv.com/ (Consulta el 18 de abril de 2019).

- El daño a la credibilidad y a la propia imagen de la empresa supondrá una pérdida de confianza que afectará a corto, medio y largo plazo a la viabilidad de la empresa.

- En ciertos tipos de empresas se podrían dar pérdidas de vidas humanas por manipulaciones o alteración de protocolos.

- El pago de indemnizaciones por daños y perjuicios a los clientes afectados ya que a las empresas se les exige una seguridad adecuada para proteger sus redes. El incumpliendo llevaría a posibles responsabilidades civiles e incluso penales.

4 PLAN DE RESPUESTA A INCIDENTES Y ATAQUES.

4.1 Constitución del CSIRT.

Los equipos de Emergencias Informáticas dan respuesta a incidentes de Seguridad y buscan generar el mínimo daños en las organizaciones que lo sufren (Mendoza, 2015).

El nombre de CSIRT proviene de *Computer Security Response Team* y su finalidad es la detección del ataque o, una vez ya producido, mitigar los daños que pueda causar. Es fundamental contar con un equipo de respuesta ante posibles incidentes, así como coordinar una rápida recuperación de los datos afectados en un ataque, para restablecer en el menor tiempo posible la normalidad a la empresa u organismo.

Otra característica es que debe prevenir posibles ataques a causa de incidentes menores, para poder anticiparse a unos resultados negativos, una vez aprendida la dinámica de ese hecho y de poner soluciones, para tomar medidas para que no se repitan.

Debe ser un valor en inversión contar en las empresas con un CSIRT, para reducir riesgos y minimizar las consecuencias de un ataque, lo que reduciría los costes y gastos por los daños ocasionados, y la pérdida de confianza de los ciudadanos.

En la web www.welibesecurity.com, valora como un retorno de inversión[90], donde se desarrolla "*un modelo diseñado para calcular al momento de invertir no solo los costes directos sino realizar una evaluación más completa de todo el dinero necesario*".

4.2 Detección de un Incidente de Seguridad.

Para desarrollar este punto es fundamental la lectura del autor y especialista en esta materia Álvaro Gomez Vieites[91], con su obra Seguridad Informática, donde detalla los fundamentos a la hora de implantar un plan de Sistema de Gestión de la Seguridad de la Información. A grandes rasgos señala que cualquier anomalía, degradación o interrupción del sistema que afecte a la confidencialidad o integridad de la información es lo que se considera un "Incidente de Seguridad". Los incidentes normalmente vienen causados por agentes o bien

[90] WELIVESECURITY.Retorno de Inversión en Seguridad, abril 2010 https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/ (Consulta el 5 de mayo de 2019).

[91] https://es.linkedin.com/in/alvarogomezvieites/es

internos de la propia empresa o por un atacante externo por diversas motivaciones como puedes ser:

- Pura diversión sin más fin que el mero entretenimiento.
- Ideología. Ataques encaminados a empresas o Website gubernamentales, normalmente llevan un componente político.
- Auto- realización
- El más habitual es por consideración económica, ya sea para extraer información confidencial, para vender a terceros o para dañar el sistema de la empresa atacada.

Existe otra importante motivación que es el reconocimiento de la comunidad virtual, que otorga el realizar según que, tipo de acciones.

Independientemente del tipo de motivación que tenga el ataque, se deben de dar 3 factores denominados el "*Triángulo de la Intrusión*", que son:

Ilustración 6. Triángulo de la Intrusión [92]

Para la instalación de un Plan de Respuesta a Incidentes, este debe contar con personas expertas y con la formación necesaria para actuar ante ataques, incidencias y desastres que pudieran afectar al organismo perjudicado.

Actualmente solo las grandes empresas disponen de personal cualificado. Faltan por cubrir cerca de 3.5 millones de empleos en ciberseguridad[93]. Estas personas deberían ser las

[92] Gómez, A. https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf (Consulta 3 de mayo de 2019).

[93] MIT technology Review. "La falta de expertos en ciberseguridad obliga a recurrir a estudiantes" Erin Winick , El 26 de Octubre de 2018..https://www.technologyreview.es/s/10614/la-falta-de-expertos-en-ciberseguridad-obliga-recurrir-estudiantes (Consulta el 12 de junio de 2019).

encargadas de solventar las incidencias que se detecten y minimizar los daños que pudieran producirse debiendo estar formadas para marcar las pautas de respuesta del resto de personal ante un posible incidente de Seguridad:

- Precursores de un ataque. Se deben reconocer todas las acciones del sistema informático y proceder al revisado y escaneo de posibles vulnerabilidades e intrusiones en nuestros servidores, así como verificar los sistemas operativos y sus aplicaciones.

- Alarmas generadas en los Sistemas de Detección de Intrusiones (IDS). Se utilizarán los cortafuegos y el software antivirus.

- Observar el registro de actividad extraña en los *logs* de servidores y dispositivos de red o el aumento considerable de entradas en los *logs*.

- Estar atento a la aparición de programas, carpetas o algún fichero de origen desconocido en nuestros servidores. Estas se pueden detectar por programas diseñados para la revisión de nuestros equipos informáticos.

Sospechar de reinicios inesperados, fallos en el servicio e incremento considerable de errores en la carga de nuestro equipo o anomalía de la memoria del sistema, cambios de las políticas de seguridad. Álvaro Gómez Vieites aconseja "la *activación de nuevos servicios, puertos abiertos que no estaban autorizados, activación de las tarjetas de red en modo promiscuo* "pudiendo así capturar todo el tráfico que circula por la red interna mediante *sniffers.*[94]

De vital importancia es la detección de algún software no autorizado.

Hay que estar atentos al movimiento de nuestro equipo en horarios anormales, pudiendo aparecer conexiones en horas nocturnas o poco frecuentes o la utilización de cuentas privadas desde varios equipos a la vez, debiendo estar atentos a los avisos en los fallos de autenticación y el lugar de acceso de estos ataques.

En diversas web y portales se informa de fallos en los sistemas informáticos, debiéndonos poner en alerta para corregir estas incidencias.

[94] Universidad VIU. *"¿Qué es un Sniffer?* 6 de diciembre de 2017.https://www.universidadviu.es/que-es-un-sniffer/ (Consulta el 29 de abril de 2019).

Detección de procesos extraños en ejecución dentro de un sistema, que se inician a horas poco habituales o que consumen más recursos de los normales (tiempo de procesador o memoria). Generación de tráfico extraño en la red: envío de mensajes de correo electrónico hacia el exterior con contenido sospechoso, inusual actividad de transferencia de ficheros, escaneo de otros equipos desde un equipo interno.

Prever la posible existencia de ataques desde el interior de equipos de la propia red.

Existen herramientas muy sofisticadas que pueden detectar incluso dispositivos que capturen las pulsaciones del teclado en nuestro equipo, lo que podría llegar a conseguir información sensible de nuestro equipo.

Se sabe que la complejidad de los ataques ciberterroristas son cada vez más sofisticados y de una extrema complejidad, por lo que detectarlos a tiempo no es siempre posible y el tiempo corre a su favor, la instalación de respuesta automáticas ante estos ataques no parece ser la manera más acertada de pararlos, por la mutación que pueda mostrar el ataque, todos estos problemas se agravan con los conocidos como falsos positivos, que ocasionan pérdida de tiempo y de recursos por lo que es necesario mecanismo que filtren la detección y señale la clasificación de incidentes según qué tipo de características posean dichos ataques. Debemos analizar los incidentes desde el Plan de respuesta y plantear las siguientes cuestiones: ¿qué redes, servidores, equipos han sido afectado?, ¿han conseguido acceder a información clasificada y que afecte a la empresa o clientes?, y ¿ha afectado a terceras personas?

A continuación, los expertos emplearán una matriz de diagnóstico para obtener información acerca de una institución o empresa.

Síntoma	Código malicioso	Denegación de Servicio (DoS)	Acceso no autorizado
Escaneo de puertos	Bajo	Alto	Medio
Caída de un servidor	Alto	Alto	Medio
Modificación de ficheros de un equipo	Alto	Bajo	Alto
Tráfico inusual en la red	Medio	Alto	Medio
Ralentización de los equipos o de la red	Medio	Alto	Bajo
Envío de mensajes de correo sospechosos	Alto	Bajo	Medio

Tabla 3. Ejemplo matriz de diagnóstico.

Una vez tengamos detectado el incidente deberíamos marcar unas prioridades, pudiendo seguir los documentos[95] y guía para desarrollar una seguridad informática que se priorizan en 5 puntos:

1. Proteger la vida humana y su seguridad.
2. Proteger tanto la información como los datos que disponga la organización.
3. Proteger los datos e info sensible debe ser una máxima de la organización.
4. Proteger mediante la prevención los posibles daños en los sistemas informáticos.
5. Minimizar los daños ofrecidos a clientes y usuarios.

Si el equipo de respuesta detectara que la intrusión pudiera ser motivo de daños graves de la empresa se procederá al apagado de los equipos afectados, así como su desconexión de la red informática, todo ello para evitar el acceso a información clasificada o confidencial.

Otra opción más arriesgada es intentar retrasar la contención para intentar llegar al atacante, pero correríamos el riesgo de desencadenar mayores daños a los equipos infectados.

A este tipo de estrategia se suma otra más compleja como es aquella que está controlada por un *cracker*[96] que se encargaría de realizar *pings*, comprando las posibles desconexiones de los equipos a la red, automáticamente se encarga de eliminar las pruebas del disco duro, por lo que aumentaría el impacto negativo en los equipos y en la empresa.

4.3 Identificación de atacantes

Algunas empresas e incluso Estados no persiguen legalmente a los ciberdelincuentes o ciberterroristas por el gran esfuerzo necesario tanto de recursos humanos como económicos, que se han de emplear, nos encontramos ante un numero cuantioso de hechos lentos y tediosos que ocasiona que no se le dé la respuesta rápida, y eficaz que requiere al perderse en trámites judiciales, publicación en los medios, perdidas por el ataque, y escasa colaboración de los países que normalmente provienen los ataques, con escaso o nulo interés en colaborar por lo que una posible extradición de estas personas queda lejos de materializarse.

[95] Este manual es una guía para desarrollar políticas de seguridad informática y Procedimientos para sitios que tienen sistemas en internet https://www.ietf.org/rfc/rfc2196.txt (Consulta 2 de junio de 2019).

[96] Wikipedia. ¿Qué es un Craker? 2019 https://es.wikipedia.org/wiki/Cracker (Consulta 7 de junio de 2019).

Aun con estos impedimentos existen técnicas para determinar que equipos y desde donde se han llevado a cabo como son:

Utilización de herramientas como *Ping*, donde se observara la forma de interactuar con otros elementos a través de la red, la latencia y el ping se convierten en dos factores vitales para medir la calidad de la conexión a través de la han realizado el ataque, por eso cuando ejecutamos *ping* enviamos un mensaje ICMP en un paquete IP desde nuestro ordenador, que incluye un código, un número identificador, una secuencia de 32 bits y un espacio opcional de datos que deben coincidir con el mensaje de respuesta, así podemos calcular el tiempo que tarda en ir y volver .

Utilización de "Traceroute"[97], la definición de Wikipedia señala como" *una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red"*). Esta herramienta nos es de suma importancia ya que nos ayudaría a localizar a los posibles atacantes.

Consultar en los registros inversos de servidores DNS, Esta herramienta permite la traducción de direcciones IP a nombres porque cada dirección IP puede tener solo un nombre asociado.

De todas formas, como vamos a ver ahora, no es tan sencillo llegar a saber el punto de origen o inicio de los atacantes ya que estos nos pondrán ciertas trabas para evitar utilizar este tipo de herramientas o bien desvirtuar el resultado de ellas. Una de las taras que nos va a dificultar la investigación para llegar a ellos son:

- Mediante técnicas *IP Spoofing* se puede manipular la dirección en algunos tipos de ataque.
- Los atacantes fruto de su alta capacidad y sofisticación podrían estar utilizando terceros equipos para realizar acciones, sin el consentimiento del dueño del equipo.

[97] Wikipedia. Traceroute. https://es.wikipedia.org/wiki/Traceroute .(Consulta 07 de junio de 2019).

- Existe muy frecuentemente el hecho que el atacante emplee una dirección IP dinámica, es decir esta es asignada de manera aleatoria por un proveedor de Internet.

- Otro modo también muy sofisticado de contra vigilancia es que el equipo del atacante utiliza los servidores PROXY con el servicio Nat activo, llegando a compartir una dirección IP publica con otros de la misma red, por lo que deberíamos solicitar la colaboración tanto del proveedor de internet como del responsable de la red utilizada por los ciberdelincuentes.

- Un paso de vital importancia es analizar los escaneos de puertos y vulnerabilidades en el sistema, para ver si estos han podido ser registrados por *logs*[98], definiendo este concepto como un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático.

Una vez podemos llegar a ellos, si se han superado todos los obstáculos e impedimentos que presentan los ciberdelincuentes/ciberterroristas, las empresas deberán poner en manos de las Autoridades competentes que en este caso son tanto la Guardia Civil como las unidades especializadas de la Policía Nacional, encargadas de proceder si cabe a la detención de los autores.

Todo esto que hemos visto nos debe llevar a evaluar a posteriori las causas para evitar que se repitan incidentes, debiendo seguir a grandes rasgos estas recomendaciones:

- Destinar recursos para la formación tanto del personal directivo como de los empleados para la seguridad cibernética.

- Dominio de la tecnología que se emplea en la empresa y alto grado de compromiso para la autoseguridad en la red, por parte de toda la plantilla.

- Mantenimiento eficaz y periódico de todos los equipos de la empresa, con estrictas normas de uso ajenas al trabajo de la empresa.

[98] Ankama Support. *"¿Qué es un log?* 2015 https://support.ankama.com/hc/es/articles/203790076--Qu%C3%A9-es-un-log- (Consulta el 11 de junio de 2019).

- La limitación de accesos a las diferentes áreas que disponga la empresa u Organismo.
- Actualización permanente de los Software y Hardware de la empresa.
- Control exhaustivo del uso de los empleados propios, muchos ataques y robos de información provienen del interior de la empresa.

4.4 Seguimiento electrónico para la localización de ciberterroristas.

Las técnicas que se usan por los diversos grupos y equipos de vigilancia y seguimiento de espionaje son muy diversas y suelen combinar diversas técnicas para llegar al objetivo planteado, si bien, una primera fase es una captación de información en aplicaciones de mensajería, chats, foros y correo.

Todos los Estados están invirtiendo en la creación de malware, no solo recae en los grupos de ciberdelincuentes. Así lo demostró Shadow Brokers al liberar varios *exploits* supuestamente creados por la agencia de seguridad americana (NSA), quien ya había sido acusada previamente de otros casos de espionaje.

La observación a nivel europeo del crecimiento de los ataques de ciberespionaje, político y económico, que atenta a las escuras del estado del bienestar de la Unión Europea.

Por lo que es necesario adoptar medidas para defender, y neutralizar las agresiones encubiertas, en especial las que provienen del ciberespacio, ya vengan de terceros Estados, de organizaciones terroristas o de servicios de Inteligencia dirigidas a la obtención ilegal de información.

En el informe[99] Anual de Seguridad Nacional del año 2018, se estudia el periodo comprendido entre el 2013-2018, manifestando como los servicios de inteligencia utiliza métodos cada vez más agresivos y clandestinos intentan sustraer la información estratégica de los Estados, como hemos visto anteriormente se corresponde con "*Operaciones Hibridas*".

[99] Gobierno de España, Departamento de Seguridad Nacional."Informe Anual de Seguridad de 2018" https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-anual-seguridad-nacional-2018 (consulta el 2 de abril de 2019).

El robo de esta información tan relevante va encaminada a la obtención de planes de desarrollo e información sobre posiciones de los países en negociaciones abiertas de naturaleza militar, política o estratégica.

Otro de los ataques que atentan especialmente a nuestro Estado son, el ciberespionaje económico, en especial a los que afectan a las áreas de Defensa, Tecnología, Energía, Salud y Química, debido a la gran repercusión que tiene cualquier avance en esta materia, estos ataques pueden provocar desde una Guerra hasta alteraciones del orden económico, procediendo estos ataques de ciertos Gobiernos y de empresas extranjeras.

Las características como hemos visto de los ataques presentan unas características como son su bajo coste, su gran rentabilidad y los limitados riesgos que son fácilmente asumidos, debido al complejo proceso de investigación para llegar a ellos.

En España se están tomando medidas debido a la creciente información clasificada manejada por los Ministerios, por lo que su protección debe ser una máxima en nuestra legislación.

La Oficina Nacional de Seguridad (ONS), con competencias en esta materia, guía en el programa del proyecto Galileo, donde se toman medidas para la protección de la información clasificada.

El proyecto Galileo de creación civil y financiado por la UE pretende a corto plazo ser el sistema de navegación por satélite de la Agencia Espacial Europea, con este sistema que contará con 24 satélites operativos y una infraestructura de tierra para proveer servicios de posicionamiento, navegación y determinación de la hora, los primeros satélites fueron lanzados el 21 de octubre de 2011, por lo que dejaremos de tener la dependencia del GPS (siglas en inglés de *Global Positioning System*) y del sistema Ruso GLONASS, al menos esta es la intención de la ESA de completar la constelación el próximo año.

En España se han tomado medidas muy efectivas para que las empresas que trabaja con el Ministerio de Defensa, que tengan contratos, proyectos, o acceso a documentación clasificada que pudiera ser objeto de espionaje, será necesario que personal obtengan la correspondiente Habilitación de Seguridad de Empresa y Establecimiento, y el personal que trabaje en estas las habilitaciones Personales de Seguridad.

España se marca como reto irrechazable garantizar una seguridad ante los ataques hostiles por parte de los ciberterroristas o Estados con diferentes intereses al nuestro, por lo que es necesario un Servicio de Inteligencia, que emplee el mayor número de recursos mediante la

coordinación y la eficacia dar una respuesta clara con la ayuda de los diferentes países europeos, así como empresas privadas ante un posible ataque, adoptando medidas de Contrainteligencia tanto a nivel nacional como Internacional. En el marco de la Contrainteligencia, se han realizado actividades para neutralizar la labor de control de los servicios de Inteligencia extranjeros sobre sus nacionales en territorio español, algo que supone una injerencia en la soberanía nacional.

Es muy importante la actividad de Contrainteligencia de los gobiernos especialmente por el uso de tecnologías avanzadas por parte de todos los Estados, destacando las acciones de ciberespionaje como las más complejas para ser detectadas, por ello como indican el informe Anual de Seguridad 2018 se han tomado las siguientes medidas:

- Aumento y refuerzo de los Órganos de Inteligencia, así como la sensibilización y divulgación de los Servicios de Espionaje de otros países y su efecto en la Administración Pública.

- Protección de la información clasificada, mediante la formación a los responsables de la seguridad de la información en organismos y empresas y altos cargos de la Administración.

- Se han incrementado el número de instalaciones acreditativas para el manejo de información clasificada ya sea por parte de la Administración Pública como privada.

- En el caso de las empresas privadas se ha implementado un sistema digitalizado de inspección continua de su infraestructura de protección de información clasificada.

- En el área internacional se están desarrollando procedimientos para impedir que personal extranjero tenga acceso a información clasificada a través de empresas habilitadas.

A grandes rasgos estos son algunas de las medidas tomadas, todas ellas en sintonía con los acuerdos bilaterales suscritos por España que se encuentra vigentes que son:

- 49 tratados internacionales, siendo 44 con carácter bilateral y 5 multilaterales.

- 36 acuerdos, actualmente en fase de negociación o tramitación.

Como queda reflejado en estos acuerdos y los que están pendientes de firma, la cooperación Internacional para el trabajo conjunto en operaciones e investigaciones de ciberterrorismo es fundamental si se quiere llevar a buen término y combatir con la máxima eficacia la lucha contra estos ataques. Por ello el CNI y el Centro Criptológico Nacional (CCN), participan de manera conjunta en multitud de investigaciones que afecten a incidencias que puedan afectar a los intereses de España.

Como nuevo reto se plantea dotar al Centro Criptológico Nacional (CCN), de la implementación de Centros de Operaciones de Seguridad Virtuales para la mejora en los sistemas de información y comunicación, dándole más relevancia a entidades como Diputaciones y Ayuntamientos sobre posibles ataques e incidentes que observen, lo que lograra una respuestas mucho más ágil, rápida y eficiente.

Existe otro reto implementado en la Directiva NIS, que ha sido traspuesta al ordenamiento jurídico nacional en el Real Decreto-Ley 12/2018 de 7 de septiembre de seguridad de redes y sistema de información, donde a grandes rasgos regula la obligación de establecer un sistema de notificación de incidencias en las empresas para la mejora de la seguridad de la red.

A nivel europeo se está trabajando para crear protocolos específicos que permitan ante ataques graves y de ciberterrorismo a gran escala, dar una respuesta unida por parte de los diferentes Estados miembros.

En España para la detección de incidentes e intrusiones en el 2018 el CCN ha desarrollado el Sistema de Alerta Temprana en sus 3 vertientes:

- La intranet administrativa (SAT SARA), que dispone de 50 áreas de conexión.
- La Conexión a Internet de los organismos (SAT INET), disfrutando más de 200 organismos y empresas.
- El servicio de Alerta Temprana para sistemas de control Industrial, que permite detectar en tiempo real las amenazas en el tráfico de una organización.

El organismo INCIBE-CERT[100], ha gestionado en el año 2018, 111.519 de incidentes, de los que 722 corresponde al ámbito de los Operadores estratégicos y críticos, el mayor número es parte de las empresas y ciudadanos con 102.414 y 8.383 a la red académica.

Existe multitud de datos que nos deben poner en alerta sobre el crecimiento exponencial de ataques ciberincidentes como queda reflejado en los 38.192 que contabilizo el Centro Criptológico Nacional, de los que el 57% el vector de ataque fue la intrusión.

Gráfico 1. Crecimiento exponencial de ciberincidentes.

Avanzamos hacia una sociedad que ha de promover la cultura de la ciberseguridad, prueba de ello es la web habilitada por el Centro Criptológico Nacional[101], donde se ha desarrollado un plan de formación para la mejora del conocimiento cibernético, en esta web www.ccn.cni.es

Los estudios realizados en este campo son a grandes rasgos muy poco profundos o excesivamente técnicos que dificulta aún más si cabe el modus operandi de la seguridad en la red, tras observar las web oficiales de empresas de reconocido prestigio como KASPERSKY, SYMANTEC O, McAfee, donde se encuentra numerosa información sobre

[100] Centro Cristológico Nacional." *Ciberamenazas y Tendencias Edición 2018* " https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html (Consulta el 11 de junio de 2019).

[101] Centro Criptologico Nacional. Formación. 2019. https://www.ccn.cni.es/index.php/es/menu-formacion-es (Consulta el 9 de junio de 2019).

cibercrimen, sin dejar de lado que nadie está exento de sufrir una vulneración en su seguridad como ya ocurrió con la Multinacional Microsoft[102] donde fue víctima de un *hackeo*.

Estos ataques se están creando con software y tecnología avanzada por los grandes beneficios económicos que obtienen los atacantes.

Debemos mencionar si este tipo de protección estatal en algunos Estados conlleva unos riesgos y realidades como son el excesivo control del Gobierno sobre los ciudadanos, persiguiendo de forma sistemática cualquier actividad crítica contra el Estado o limitando la información pública en aras de una supuesta Seguridad.

Este claro ejemplo de intromisión se ve claramente en Estados Unidos de América, con la ley *Protect America Act* (PAA), que habilita sobre objetivos extranjeros con valor para los servicios de inteligencia, y protege los derechos de los ciudadanos estadounidenses siempre que no sea un obstáculo para los servicios secretos, aun mas se acrecienta con la creación de la Ley Fisa[103], que da total poder a los servicios de espionaje, en especial la NSA, a realizar actividades de vigilancia masiva y a la recopilación ilimitada de datos personales, llegando a autorizar sin ningún tipo de control judicial a un individuo durante 168 horas, especialmente a americanos que hayan estado en países susceptibles.

En muy importante valorar que, a pesar de las críticas por estos excesos, actualmente los servicios de inteligencias americanos cuentan con una protección Operativa e Inmunidad Legal, algo impensable en nuestra legislación Europea.

En estos momentos entraríamos en confrontación si existe base legal para que exista el sistema PRISM que permitiría acceder a las bases de datos de los usuarios de empresas de Internet más importantes, como Microsoft, LinkedIn, Instagram o Amazon, fruto de la estrecha colaboración entre empresa/Estado, se desarrolla la instalación de software en los equipos y soportes de estas empresas, como ejemplo muy significativo estaría la captación

[102] Softzone. "Microsoft ocultó un importante hackeo sufrido el pasado 2013" David Onieva. 17 de Octubre de 2017.https://www.softzone.es/2017/10/17/microsoft-oculto-importante-hackeo-2013/ (Consulta el 11 de junio de 2019).

[103] Jorge, M. (2019). FISA: "*la ley que permite espiar sin orden judicial se renueva hasta el 2017*". Retrieved from https://hipertextual.com/2012/12/fisa-ley-espionaje-estados-unidos (Consulta el 12 de junio de 2019)

de lo que ocurre en tiempo real en un hogar por medio de las televisiones[104] Samsung que son utilizadas a modo de espía, utilizando lo que se oye a través de los equipos para posteriormente remitirlos a las agencias de espionaje como son la CIA americana o el MI5 británico.

- **PRISM**, es la herramienta preferida de la NSA, y por otros gobiernos europeos como Dinamarca, Francia, España, países bajos, Noruega, Bélgica, Italia y Suecia entre otros, estos países forman lo que se conoce como "Fourteen Eyes", oficialmente SIGINT Seniors Europe, junto a estas herramientas tenemos:

- **Muscular,** esta herramienta que interceptaría las comunicaciones privadas que unen los centros de datos de estas empresas para acceder a la base de datos de los correos electrónicos.

- **XKeyscore** es una herramienta capaz de detectar la nacionalidad de los extranjeros mediante el análisis del lenguaje utilizado en los correos electrónicos, este software nos da una idea de hasta donde son capaces de llegar los servicios de Inteligencia para saber Todo sobre los usuarios de la red.

Estas tres herramientas actúan de manera coordinada actuarían como una parte del programa ECHELON, cuya definición de Wikipedia es *"la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia (Inteligencia de señales, en inglés: Signals intelligence, SIGINT). Controlada por la comunidad UKUSA (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda), ECHELON puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones*". Se estima que ECHELON es capaz de la interceptación de tres mil millones de comunicaciones cada día.

La saturación informativa sobre los delitos cibernéticos se ha colocado en las encuestas de la mayoría de los países desarrollados como la preocupación del ciberterrorismo ocupando en EE.UU, la sexta posición en el ranking de preocupaciones de los estadounidenses, por delante del paro o de un propio atentado del ISIS, esta percepción negativa parece que no repercute en las inversiones de las empresas pues solo se persiguen el 1% de los ataques

[104] El Mundo. *"Así espía la CIA a través de tu Smart TV o tu teléfono móvil"*. Pablo Pardo. 8 de marzo de 2017. https://www.elmundo.es/internacional/2017/03/08/58bf1e0de5fdea49618b45a9.html (Consulta el 10 de junio de 2019).

cibernéticos, al entender las empresas que la inversión en seguridad es grande en comparación con el beneficio que no se obtiene a corto plazo.

Debemos entender que las empresas deben reducir la exposición al robo cumpliendo con las normativas legales e incrementar en la seguridad de sus sistemas para una detección y respuesta rápida ante un ataque o amenaza para la vital información confidencial de las empresas, así como de sus activos, tomando especialmente la concienciación de los trabajadores del uso de la red, la minimización de los riesgos y aplicación de automatismo y protocolo ante ataques cibernéticos.

Existen empresas muy especializadas en este ámbito como son IPM, que ofrece seguridad a empresas, así como gestión y formación de empleados, algunas medidas que ofrecen, aunque sencillas son muy eficaces como la "*Autentificación de usuarios*" IPM ayuda a implementar métodos de autenticación, incluyendo *tokens* de hardware, de software, autenticación basada en el riesgo y autenticación de SMS a petición o una combinación de todos ellos, bajo una consola de administración central.

Existe otro modus operandi de vigilancia que se podría utilizar contra la lucha ciberterrorista es conocida como la "*inteligencia de señales"* es la obtención de información mediante la intercepción de señales, sea sobre señales electrónicas no usadas directamente en comunicaciones o una combinación de ambas.

La inteligencia presenta 3 recursos como indica[105] Wikipedia donde lo engloba:

- Inteligencia de comunicaciones (COMINT): supone la utilización de toda clase de comunicaciones conocidas, tales como el teléfono, la radio, Internet, etc.

- Inteligencia electromagnética (ELINT): supone la utilización de campos eléctricos (cargas y corrientes eléctricas) y campos magnéticos. Un sistema electrónico importante es la radio de detección y medición de la distancia, que al reflejar las ondas electromagnéticas se puede detectar la presencia de objetos o superficies en un amplio radio, así como su posición exacta.

[105] Wikipedia. Inteligencia de señales. 2019.https://es.wikipedia.org/wiki/Inteligencia_de_se%C3%B1ales (Consulta el 12 de abril de 2019).

- Inteligencia telemétrica (TELINT): su función es la detección de imágenes, medidas y radiaciones mediante imágenes ópticas".

En contraposición a la alta tecnología y sofisticación de los medios de investigación actuales se muestra el recuadro [106] a modo de contraste sobre la contravigilancia en el año 1995, facilitado por Wikipedia: https://en.wikipedia.org/wiki/Intelligence_cycle_security

Disciplina	Ofensiva CI	Defensa defensiva
HUMINT	Contra-reconocimiento, contraespionaje ofensivo.	Engaño en la seguridad de las operaciones.
SIGINT	Recomendaciones para el ataque cinético y electrónico.	Radio OPSEC, uso de teléfonos seguros, SIGSEC, engaño.
IMINT	Recomendaciones para el ataque cinético y electrónico.	Engaño, contramedidas OPSEC, engaño (señuelos, camuflaje) Si es accesible, use los informes SATRAN de los gastos generales de los satélites para ocultar o detener las actividades mientras se visualizan

Tabla 4. Roles de CI contra las Disciplinas de Colección de Inteligencia, doctrina de 1995[107]

A nivel europeo existe otra herramienta de apoyo en la lucha contra el terrorismo como es el sistema europeo de Registro de Pasajeros (PNR), este instrumento permite almacenar la información de los datos privados recopilados durante la reserva del vuelo y la facturación en las distintas compañías aéreas, figurando: las fechas del viaje, itinerario, medio de pago utilizados y datos de contacto.

Los datos son utilizados por las FCSE y muestra una eficacia real y respaldado jurídicamente por la Unión Europea, definida por el Eurodiputado Timothy Kirkhope en sede parlamentaria como, "*una herramienta importante para luchar contra los terroristas y traficantes., Mediante la recogida, intercambio y análisis de los datos PNR, nuestros servicios de Inteligencia pueden detectar patrones de comportamiento sospechoso que merecen seguimiento. La directiva PNR no es una fórmula mágica, pero los países que ya tienen sistemas nacionales de registro han demostrado que es un instrumento muy efectivo*.".

[106] https://en.wikipedia.org/wiki/Intelligence_cycle_security (Consulta el 12 de mayo de 2019).

[107] Wikipedia. https://en.wikipedia.org/wiki/Intelligence_cycle_security (Consulta el 12 de mayo de 2019).

En junio de 2011 surge otro proyecto liderado por la empresa española S21sec Información Security Labs S.L., cofinanciado por la Unión Europea, conocido como *Proyecto Casper*.

Este proyecto tiene como objetivo la creación de un Software a nivel internacional para la prevención de la delincuencia organizada, a través del acceso a millones de datos extraídos de internet y de las agencias de inteligencia internacionales, llevando el análisis automatizado de contenidos multilingües y audiovisuales de manera colaborativa entre distintas agencias de seguridad y otros cuerpos policiales.

Este proyecto se desarrolla por las necesidades de las FCSE, que son las beneficiarias de este sorprendente Software, este proyecto terminó en junio del año 2014, desconociendo hasta la fecha el resultado de este, si se mostró la capacidad de identificar a un individuo ficticio a través de todos los datos existentes en fuentes abiertas, esta información encontrada en los autores Alejandro Pozo, Camino Simarro y Oriol Sabat del Informe[108] sobre Relaciones comerciales militares, armamentísticas y de seguridad entre España e Israel.

Nos encontramos ante el punto más complejo e interesante de este TFG, las inversiones realizadas en este tipo de tecnología de seguimiento y detección de ciberterroristas, la formación completa y eficaz con la que se debe formar a las diversas unidades especializadas de las Fuerzas Cuerpos de Seguridad del Estado, así como las Agencia de Inteligencia, marcaran el camino de una eficiencia aceptable en materia de seguridad exterior e interior. Debemos estar preparados para el peor de los supuestos, por lo que el desarrollo, la innovación en nuevas tecnologías de vigilancia, seguimiento, así como el respaldo Judicial que debe tener dicha tecnología va a marcar el éxito de la seguridad de un País.

A la hora de investigar e indagar sobre las técnicas de los diferentes países, nos encontramos con escasa información de la materia o muy poco desarrollada, como es lógico se debe a información clasificada y que requiere de ciertos niveles de acceso para acceder a estos conocimientos.

Al no existir una legislación común, ni homogénea nos encontramos con diferentes técnicas que si bien en países como EE.UU, o Inglaterra disponen de una legislación más abierta, dando casi carta blanca a los agentes de Inteligencia, en otros países se necesitan como

[108] Studylib." *Defensa, Seguridad y Ocupación como Negocio*". Alejandro Pozo, Camino Simarro y Oriol Sabaté. https://studylib.es/doc/1094796/defensa--seguridad-y-ocupaci%C3%B3n-como-negocio (Consulta el 12 de mayo de 2019).

veremos a continuación, un control a juicio de este alumno de excesivo control, lo que devalúa la propia investigación o medida de ciberseguridad, debiendo primar en primer lugar la rapidez de la medida de manera que sea Eficaz y Eficiente, sin perjuicio del control judicial o estatal que a la postre se deba dar.

Lo primero que se debería tener a nivel internacional es un consenso de lo que se debe entender por ciberterrorismo. Deberíamos de coger como referencia el estudio[109] que presento el *National of Justice* (NIJ), del Departamento de Justicia de los Estados, donde muestra los 10 puntos críticos donde debemos trabajar para llegar a la plena colaboración entre la Administración de Justica y su relación con las nuevas realidades de los delitos cibernéticos siendo estas medidas:

1. Concientización del público.
2. Estadísticas y datos sobre delitos informáticos.
3. Entrenamiento uniforme y cursos de certificación para investigadores.
4. Asistencia en sitio para las unidades de lucha contra el delito informático.
5. Actualización del marco normativo.
6. Cooperación con los proveedores de alta tecnología.
7. Investigaciones y publicaciones especializadas en crímenes de alta tecnología.
8. Concientización y soporte de la gerencia.
9. Herramientas forenses y de investigación criminal informática.
10. Estructuración de unidades de lucha contra el delito informático.

A grandes rasgos estas medidas deben ir encaminada a agilizar y fortalecer el Estado de Derecho en consonancia con nuestro derecho a la Intimidad, no tener en cuenta la problemática que existe actualmente en la legislación solo nos lleva a dar más poder a los ciberterroristas y fomentar practicas más invasivas para corregir el déficit de seguridad Jurídica que respalde las investigaciones tecnológicas de los diversos Estados.

[109] Departamento de Justicia de EE.UU. "U.S. Department of Justice Office of Justice Programs" https://www.ncjrs.gov/pdffiles1/nij/186276.pdf (Consulta el 4 de marzo de 2019).

En esta línea de cooperación y seguridad Jurídica, el grupo G8, desarrolla una serie de recomendaciones [110] de cara a una estrategia de coordinación Internacional para la protección de infraestructuras de información crítica, a continuación, señalaremos algunas para la protección de información crítica:

1. Todos los países deben contar con sistemas que alerten de posibles amenazas y ciber vulnerabilidades.

2. Los países deben aumentar el conocimiento y concientización de la importancia de las infraestructuras de información crítica.

3. Los países deberán analizar sus infraestructuras y coordinarse para aumentar su grado de protección.

4. Fomentar la alianza entre gobiernos y el sector privado para analizar las incidencias, los ataques graves y poner trabas a los riesgos que pudieran ocasionarse.

5. Los países fomentaran la comunicación ante una crisis y generar una cultura de prevención, para desenvolverse con soltura ante estas Incidencias.

Existe una realidad que debemos de matizar si no ponemos el máximo de esfuerzo en lograr una verdadera cooperación entre Estados, y una homogenización del concepto de ciberterrorismo estamos abocados a sufrir los efectos de este, la nueva realidad a la que nos enfrentamos es a un Ejército de Terroristas que no se ve, que libran una guerra en la que dominan el medio en el que se mueven de manera mucho más ágil, consiguiendo mimetizarse en la red, es decir en nuestro día a día, intentando conseguir su expansión, la captación de nuevos reclutamiento o la formación de terroristas virtuales nos lleva a plantear una guerra que no se ve, pero que se libra cada día en la red, es lo que se conoce como Guerra de la Información[111] .

España se han tomado en serio este asunto, en la especialización de ciberterrorismo, es decir no solo debe de existir más medios humanos para la lucha contra esta tipología, sino que

[110] Meridianprocess.org. " *Guía de buenas prácticas de GFCE-MERIDIAN sobre protección de infraestructuras críticas de la información para responsables de políticas gubernamentales* "Eric Luiijf

[111] 22 Long staff, T.; J. Ellis; H. Shawn; H. Lipson; R. McMillan; L. Hutz Pesante; D. Simmel; "Security of the Internet," en The Froehlich/Kent Encyclopedia of Telecommunications vol. 15, Marcel Dekker, 1997, p. 231-255, www.cert.org/encyc_article/tocencyc.html (Consulta el 25 de mayo de 2019).

deben ser investigados por personal especializado, que conozca las técnicas de vigilancia necesarias, así como el análisis y posterior remisión de las pruebas y evidencias electrónicas que presenten ante la autoridad Judicial competente, esto nos llevara a un aumento considerable de la resolución de los casos.

En el ámbito Judicial si bien hay ciertos avances el tema de la especialización de las TIC, pero debemos dotar a los jueves y fiscales de una mayor agilidad para el encausamiento Judicial de este tipo de delitos, debiendo conocer las técnicas, para ser conocedores del garante de las pruebas digitales que se pudieran aportar las Fuerzas y Cuerpos de Seguridad del Estado.

De máxima actualidad ha sido el reconocimiento por parte de Google de la infección[112] con virus con el sistema Android salidos de fábrica, este fallo fue detectado por el equipo de ciberseguridad de Google, quien confirmo que el virus conocido como Triada, mutuo y paso a ser un troyano que se introduce en la cadena de producción de los móviles, llegando a estar infectado de serie, dando Google recomendaciones para eliminar de los dispositivos las variantes de Triada[113].

Como se señalo se ha desarrollado numerosos organismos que desarrollaremos en el punto 5, para esta lucha ciberterrorista, pero a grandes rasgos algunos de estos son:

CEPOL, Es una agencia de la UE encargada de ofrecer la formación a los agentes policiales en asuntos relativos a la seguridad de la Unión Europea, siendo el cibercrimen uno de los asuntos más sensibles y desarrollados en la actual formación.

European Cybercrime Training and Education Group (ECTEG). Es un grupo de formación en materia específico de cibercrimen a miembros de las Fuerzas y cuerpos de seguridad de los Estados de la Unión Europea, así como a organismos policiales de otro país y a empresas privadas.

---

[112] El Mundo. "*Google admite que móviles Android salieron con virus de fábrica* " 8 de junio de 2019 https://www.elmundo.es/tecnologia/2019/06/08/5cfa8c26fdddff42298b45a0.html. (Consulta el 11 de junio de 2019).

[113] Kaspersky Daily. *"Triada: crimen organizado en Android"*. John Snow. 3 de marzo de 2016. https://www.kaspersky.es/blog/triada-trojan/7884/ (Consulta 10 de junio de 2019)

EUROPOL (J-CAT)[114], este proyecto J-CAT, que responde a las siglas Joint Cybercrime Action Task Force, o Grupo de Trabajo Conjunto de Acción contra el Cibercrimen, se encuadrará en la Unidad de lucha contra el Cibercrimen de Europol, conocida como European Cyber Crime Center, o por sus siglas, EC3.

Las diferentes unidades policiales que participan en la investigación de delitos informáticos de diferentes países: Estados Unidos (FBI y Servicio Secreto), Reino Unido, Australia, Colombia, Canadá, Alemania, Holanda, Austria, Italia y Francia. Además de estos miembros, el proyecto J-CAT contará con especialistas de los tres departamentos de analistas que forman el EC3: *malware* y *hacking*, fraudes en medios de pago y explotación sexual de menores."

No menos importante, aunque no es un organismo como tal, es la Red Judicial Europea (EUROJUST), creada en el año 2002, que pretende intensificar la lucha y la estrecha colaboración para combatir los delitos cometidos en el ciberespacio.

Las denuncias por ciberdelitos aumentan cada día y los ataques a las infraestructuras del Estado han aumentado por siete en dos años, según los datos del INCIBE.

En España, nos encontramos con unidades especializadas en el cibercrimen, tanto en la Guardia Civil como en la Policía Nacional.

En la Policía Nacional no encontramos ante la conocida como U.I.T, que es la brigada de Investigación tecnológica, con competencias para la lucha en todo tipo de delitos tanto en el ámbito nacional como internacional, su función es poner las pruebas obtenidas, perseguir y detener a los ciberdelincuentes y ponerlos a disposición judicial.

La Guardia Civil, dispone G.D.T (Grupo de Delitos Tecnológicos), fue creado para investigar, dentro de la UCO, cabe destacar en el trabajo del GDT, su presencia continuada en seminarios y conferencias internacionales, lo que le ha permitido crear con una red de contactos policiales muy importante a nivel internacional, esencial en la resolución de determinadas investigaciones. Es miembro activo en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Grupo de Europol.

Con las tecnologías de vigilancia que desarrollaremos en el siguiente punto veremos cómo tanto la PN como la Gc, y los servicios de Inteligencia CNI, luchan contra este tipo de delitos, entre los agentes terroristas más activos y populares se encuentra el grupo autodenominado Estado Islámico o Dáesh.

En el documental[115] de RTVE, sobre los servicios secretos en España, señalan que hay un Juez del Supremo adscrito al CNI, que autoriza las escuchas y la información de Metadatos, dando garantías judiciales a esta información.

En el Centro de Estudios de Propagación Radioeléctrica recibe Información con la NSA desde el Consulado en Barcelona colaboran para el estudio para ver a qué tipo de organizaciones terroristas se enfrentan los Estados, mostraremos el alto grado de sofisticación del grupo Terrorista ISIS, la web especializada en seguridad nos informa en su boletín[116] núm. 44 sobre este grupo radical. Ya la web especializada[117], nos muestra la creciente actividad en la red de esta Organización.

En 2019 el Estado Islámico avanza más rápido que algunos servicios de Inteligencia y desarrollan tácticas con la finalidad de *hackear* las cuentas de las redes sociales. El ISIS dispone de 4 divisiones para ejecutar acciones ciberterroristas:

1. Sección Fantasma del Califato.
2. Hijos del Califato.
3. Ciber Ejército Califato.
4. Equipo de Seguridad Kalachnikv.

A finales del 2018, se detectan en la Aplicación VIBER a miembros del Estado Islámico. Donde en apenas 48 horas, más de 223 miembros de esta aplicación se unieron al canal ISIS,

---

[115] RTVE. " *Así espían los servicios secretos de España*" http://www.rtve.es/alacarta/videos/telediario/estado-pretende-proteger-comunicaciones-para-evitar-atentados-terroristas/2110936/ (Consulta el 12 de mayo de 2019).

[116] Fuerzasmilitares.org. *"Boletín de Prevención y Seguridad ante el Terrorismo y las nuevas Amenazas*" Pag 10. 2018. http://www.fuerzasmilitares.org/triarius/Boletin-Triarius-0044.pdf (Consulta el 06 de junio de 2019).

[117] Martínez, D. (2019). "Ciberterrorismo". http://www.fuerzasmilitares.org/triarius/Boletin-Triarius-0044.pdf (Consulta el 23 de abril de 2019).

produciendo que las agencias de inteligencias de varios Estados pusieran su foco de atención en estos nuevos movimientos del Estado Islámico, con la ayuda de *hackers* anónimos conocidos como (cazadores de terroristas) en *Twitter hashtag #OpISIS*, luchando contra la propaganda del Estado Islámico en la red. Su trabajo lleva aparejado la ayuda a agentes de inteligencia estos infiltran en grupos de Telegram, monitorizan las redes sociales y derriban los servidores web que emiten la propaganda de ISIS.

Estos hackers trabajan para Detectar y denunciar la publicidad que los ciberterrorista pretenden difundir a través de Internet, provocando una ciberguerra de guerrillas donde participa agentes y simpatizantes de otros movimientos como Anonymous, en conjunto con las fuerzas de seguridad e Inteligencia estatales.

El Isis usa las redes sociales como ya hemos visto para difundir su ideología captar por medio de la red a otros yihadistas y como fuente de financiamiento.

Los Estados deben utilizar todos los frentes y herramientas posibles para luchar este tipo de ciberterrorismo. En esta guerra tecnológica contra el terrorismo se utilizan las siguientes herramientas tal como indica el coronel del Ejército de Uruguay, experto en ciberterrorismo, Daniel Martínez [118]:

1. Exploración de datos.
2. Contra-vigilancia.
3. Infiltración de las comunicaciones.
4. Gestión de crisis.
5. Análisis de datos masivos.
6. Rastreo de bitcoin.

[118] Daniel Martínez (Uruguay). Coronel retirado. Arma de Infantería. Diplomado en Estado Mayor. Misiones de Paz de Naciones Unidas: Angola, Georgia, Haití y R.D. del Congo. Cursos: Terrorismo y Antiterrorismo (EE. UU), Estrategia (Alemania). Seguridad Pública y Privada ante Amenazas Transnacionales (Uruguay). Actualmente se desempeña como asesor en el área de seguridad y analista militar. Docente en institutos civiles y militares.2018. http://www.fuerzasmilitares.org/triarius/Boletin-Triarius-0044.pdf (Consulta el 2 de mayo de 2019).

7. Monitoreo de e-mails.
8. Búsqueda por palabras claves.
9. Lingüística.
10. Análisis predictivo.
11. Cálculo de riesgo.
12. Investigación del terrorismo.
13. Vigilancia de sitios.
14. Búsqueda de vulnerabilidades informáticas.
15. Infiltración del chat encriptado Alrawi.
16. Desarrollo del *hackeo* ético.
17. Base de datos de perfiles extremistas en las redes sociales.
18. Sitios de la web profunda, internet invisible u oculta.
19. Recolectar datos sobre amenazas eventuales.
20. Desarrollar análisis informático avanzado.
21. Estrategias de ofensiva y vigilancia.

Existe grupos como el *Ghost Security Group*[119], dedicados a la lucha antiterrorista que, poniendo en jaque a estos ciberterroristas, nos indican consejos para las vigilancias y contravigilancia como son:

- No es aconsejable suspender miles de cuentas por apología o promoción del terrorismo, porque es insuficiente para obstaculizar a los ciber yihadistas.
- Aunque es necesario cerrar cuentas, es realmente sencillo abrir nuevas cuentas para los ciberyihadistas.

[119] Ghost Security Group. https://ghostsecuritygroup.com/(Consultada el 6 de junio de 2019).

- Si Twitter u otras redes sociales vigilan a los ciberyihadistas estos utilizaran otras s aplicaciones más difíciles de vigilar, Telegram es menos propicia para ser investigada y fomenta la transmisión de mensajes cifrados.

- Los Servicios de Inteligencia optan por dejar los foros abiertos, para así poder vigilarlos y ver el tipo de personas que acceden a estos, siendo así preferible este medio antes que acaben utilizando redes o aplicaciones más sofisticadas en la *darkweb*.

Otros casos especiales y llamativos son la Instalación de Software espía, en el caso del espionaje sufrido por el activista Ahmed Mansoor[120], donde se le instalo a su teléfono móvil IPhone, un software llamada Pegasus[121], este programa permitió monitorizar su posicionamiento, espiar su micrófono y las comunicaciones.

Este Programa espía Pegasus se presenta disfrazada de aplicación solicitando un acceso a los servicios personales del usuario, sus funciones espías más destacadas son:

- Acceso al correo electrónico del espiado. los Email del Usuario

- Escuchar llamadas

- Opción de Capturar de pantalla

- Registrar claves, contactos e historial del navegador

Pegasus[122], presenta otra característica muy útil como es la capacidad de escuchar y leer archivos cifrados, ya que dispone de una herramienta tipo "keylogger" que da información sobre las pulsaciones en el teclado y tras ser analizadas pueden dar multitud de información del espiado.

---

[120] Wikipedia. "Ahmed Mansoor". https://en.wikipedia.org/wiki/Ahmed_Mansoor (Consulta el 2 de mayo de 2019).

[121] RT. México. ¿Cómo funciona Pegasus, el programa espía que vigila a periodistas y activistas en México? (20 de junio de 2017) https://actualidad.rt.com/actualidad/241759-pegasus-programa-espia-vigila-periodistas-mexico (Consulta el 3 de mayo de 2019).

[122] Pegasus. https://actualidad.rt.com/actualidad/241759-pegasus-programa-espia-vigila-periodistas-mexico (Consulta el 2 de mayo de 2019).

Es tan sofisticada que es utilizada por Gobiernos Estatales que, a fin de ocultar su presencia, si no consiguen comunicarse con algún servidor de red, en un periodo de 60 días, contiene la orden de autodestruirse para no ser detectado, lo que dificulta su seguimiento y detección.

Vivimos en un tensa calma donde lo que se conoce como guerra hibrida, está cada día más consolidado, fruto de esto numerosos estudios al respecto señalan como las multinacionales del sector tecnológico como Huawei, colabora con el gobierno chino dando cobertura y medios para poner en marcha lo que se conoce como "ciudad Segura", la propia compañía lo define "como el proyecto que combina la videovigilancia con la inteligencia artificial y el análisis de grandes cantidades de datos para ayudar a las autoridades chinas a combatir la delincuencia"

El Régimen chino ya utiliza una red masiva de cámaras de vigilancia mejoradas con inteligencia artificial, desplegadas por todo el país para controlar a los ciudadanos en tiempo real, aunque se enfoque a la delincuencia local o nacional, ya hay casos documentados de policías chinos que utilizan el sistema de vigilancia para localizar a disidentes y activistas de derechos humanos.

Huawei describe un sistema de gestión de contenido de vídeo (VCM, por sus siglas en inglés) para ayudar a la policía en el análisis y procesamiento en tiempo real de las imágenes de videovigilancia, siendo las funciones:

1. Recolección de datos grabados por múltiples cámaras dentro de una localidad en un mapa de SIG (sistema de información geográfica)

2. Análisis y procesamiento de datos en los videos de vigilancia.

3. Creación de un perfil del sospechoso y búsqueda de videos de vigilancia para localizarlo.

4. Utilización automática del reconocimiento facial y la toma de fotografías para localizar a los individuos o vehículos de transporte que están en la lista negra de las autoridades y reportar automáticamente la ubicación del objetivo.

5. Utilización de inteligencia artificial para reconocer mejor un objetivo.

Esta tecnología da una herramienta fundamental complementada con otras técnicas cibernéticas para la lucha contra el ciberterrorismo a la hora de una posible identificación de

los ciberterroristas, profundizar a pie de campo su posible detención, no tendría ningún sentido conseguir su localización e identificación y no poder materializar su detención,

Un pionero en dar un paso más en el desarrollo y ejecución de las nuevas técnicas de vigilancia y a la vez darle un marco legal es Reino Unido, con la aprobación de la ley conocida como "la Carta de Snooper"[123], dándole la capacidad de obtener y recopilar información parcial para no levantar sospechas y analizar posteriormente los datos obtenidos.

Los dispositivos de personas inocentes pueden ser pirateados de forma masiva para acercarse a objetivos no especificados, en nombre de una supuesta lucha contra el ciberterrorismo en nombre de la Seguridad.

Estos tipos de conductas no hacen sino aflorar después de muchos años de ocultismo, bajo el paraguas de la confidencialidad estatal.

A raíz del escándalo de Edward Snowden, como hemos visto que revelo lo que la NSA de EEUU y el GCHQ de Gran Bretaña estaban tramando, el proyecto de ley salió adelante como una actualización sensata de las leyes que habían quedado atrás con respecto a la tecnología digital, con nuevos poderes para hacer frente a las crecientes amenazas terroristas, esta ley tan polémica levanto el rechazo incluso de la ONU.

Esta ley finalmente entró en vigor introduciendo lo que se conoce como el "filtro", término que en realidad es un buscador para cruzar todos los datos de comunicación que se tengan de los ciudadanos., como ejemplo de la potente herramienta de control, se puede saber, por ejemplo, qué páginas estaban consultando todas las personas que se encontraban a una hora precisa en un mismo punto, a nivel policial y de seguridad es realmente excelente lo que debería de debatirse es si choca con el plano del derecho a la Intimidad.

---

[123] El Mundo (2016). Londres defiende su ley de Poderes de Investigación pese a ser criticada por la ONU". *CONXA RODRÍGUEZ.* https://www.elmundo.es/tecnologia/2016/03/16/56e992bc268e3ea6638b4641.html (Consulta el 2 de mayo de 2019).

En España, el Estado confiere al Centro Criptológico Nacional, a través de los Equipos de Respuesta ante Emergencias informáticas (CERT), los objetivos que marque la Estrategia de Ciberseguridad Nacional. Entre las funciones que tiene desarrolladas estos Equipos [124] son:

- Normativa. Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC (Guías CCN-STIC).
- Formación. Formar al personal del Sector Público especialista en el campo de la seguridad.
- Vigilar. Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
- Desarrollo. Coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad.
- Evaluación. Valorar y acreditar la capacidad de los productos de cifra y de los sistemas para manejar información de forma segura.
- Certificación. Constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad, de aplicación a productos y sistemas en su ámbito.
- Ciberseguridad. Contribuir a la mejora de la ciberseguridad española, a través del CCN-CERT, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a cualquier sistema TIC que procese información clasificada.
- Relaciones. Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Si bien es de cara a este TFG, donde analizaremos la Guía CCN-STIC-817, titulada "Esquema Nacional de Seguridad. Gestión de Ciberincidentes", donde elabora una serie de criterios para clasificar los ciberincidentes, estos factores son:

[124] Centro Criptologico Nacional. "Funciones del CCN".2019. https://www.ccn.cni.es/index.php/es/menu-ccn-es/funciones-del-ccn (Consulta el 13 abril de 2019).

- Tipo de amenaza: código dañino, intrusiones, fraude, etc.
- Origen de la amenaza: Interna o externa.
- La categoría de seguridad de los sistemas afectados.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.
- El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
- Los requerimientos legales y regulatorios.
- El intercambio de información y comunicación de ciberincidentes, debe darse al CCN-CERT, y en ocasiones los organismos públicos necesitarán comunicarse con terceros (Fuerzas y Cuerpos de Seguridad y medios de comunicación social, específicamente). El resto de las comunicaciones con otros actores (ISPs, CSIRTs, vendedores de software, etc.) se desarrollarán a través del CCN-CERT.
- En esta grafica de la Guía CCN-STIC-817, (pag 23), nos representa como deber ser la comunicación de Incidentes.

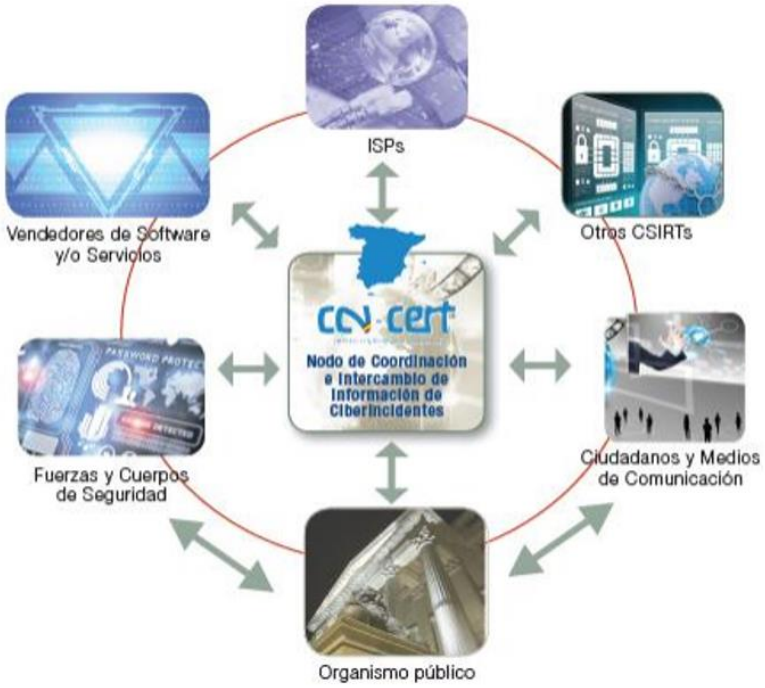

Ilustración 7. Comunicación a terceros de información a ciberincidentes

Actualmente tanto las empresas como las fuerzas de seguridad utilizan diferentes técnicas para la detección de errores en programas como son:

- *Fuzzing* son técnicas de pruebas de software para poner a prueba nuestro sistema, insertándole datos erróneos, inválidos, inesperados para comprobar la reacción de estos y así observar nuestras debilidades tales como caídas, aserciones de código erróneas, o para observar filtraciones de memoria, por donde los ciberterroristas pudieran afectar a nuestros equipos.

- El *ransomware* dirigido, donde la intrusión y el rescate se adapta a cada tipo de víctima. (Abad, 2019). En defensa de estos sistemas han aparecido complejas herramientas de detección, cuyos objetivos pretenden dar una respuesta de seguridad y protección a nuestro sistema.

La solución que se ha planteado como más útil y eficaz es el uso del método de control de acceso que va desde la autenticación, la verificación de la identidad del usuario y el control del acceso a los servicios, unido a las tecnologías basadas en el filtrado del tráfico de red.

Otros métodos se centran en la cooperación internacional, entre los países que deberán aportar y trabajar por el bien de las investigaciones complejas que acarrea la lucha contra el ciberterrorismo, empleando protocolos de obligado complimiento para garantizar la eficacia de los incidentes que estos produzcan. De especial interés es la creación de un base de datos

con imágenes de los presuntos ciberterroristas y terroristas que los proveedores de protocolos de Internet puedan detectar y eliminar contenido que induzca a actuaciones terroristas, así como aportar datos significativos de dirección IP, email, o posicionamiento de origen de estos ciberterroristas.

Otro sistema novedoso de investigación que es posible que los cuerpos y fuerzas de seguridad se hagan con los útiles servicios de aeronaves no tripuladas.

El fabricante asiático DJI cerraba un acuerdo para vender drones de vigilancia a los departamentos de Policía EE. UU., estos drones permiten mandar imágenes que serán trasferidas a la web evidence.com, donde la empresa AXON[125], diseño unos algoritmos encargados de tratar las imágenes registradas por los drones podrán ayudar a analizar escenas del crimen, llevar a cabo operaciones de búsqueda o rescate, o, detectar caras de posibles delincuentes o ciberterroristas previamente identificados.

Esta tecnología aplicada a la seguridad ya consta en un estudio[126] de la Universidad de la Universidad de Cambridge, donde identifica comportamientos violentos y sospechosos desde un dron.

Otras de las Grandes compañías multinacionales como Microsoft , uno de la empresas pionera de Internet, esta compañía estaba utilizando los servicios en la nube de Microsoft Azure para "utilizar capacidades de aprendizaje profundo para acelerar el reconocimiento y la identificación facial", lo que facilitaría el trabajo a las agencias de Inteligencia de los países que solicitaran el acceso a dicha nube, provocando injerencias y protestas por la venta y colaboración de las grandes empresas con los Organismos de Inteligencia estatales, como se puso de manifiesto en las quejas a Amazon que se negó a vender tecnología de reconocimiento facial[127] a la Policía. Este tipo de colaboraciones entre Multinacionales y

---

[125] El diario. "Tecnología para la vigilancia: estos son los nuevos 'juguetes' del Gran Herman". Álvaro Hernández. (El 20 de junio de 2018). https://www.eldiario.es/hojaderouter/tecnologia/Tecnologia-vigilancia-juguetes-Gran-Hermano_0_784272327.html (Consulta el 06 de junio de 2019).

[126] Universidad de Cambridge. "Eye in the Sky: Real-time Drone Surveillance System (DSS) for Violent Individuals Identification using ScatterNet Hybrid Deep Learning Network". https://arxiv.org/pdf/1806.00746.pdf (Consulta el 5 de junio de 2019).

[127] The New York Times. Amazon instó a no vender tecnología de reconocimiento facial a la policía. Jamie Condliffe .19 de junio de 2018 https://www.nytimes.com/2018/06/19/business/dealbook/amazon-facial-

Gobiernos es siempre muy cuestiono por la falta de transparencia en el uso de la información que pueda derivar de los datos Obtenidos, por ello es necesario la figura y control del sistema Judicial como ya hemos indicado en el sentido de dotarlos de una seguridad Jurídica en consonancia con los principios de eficacia y eficiencia.

La tecnología *blockchain* (cadena de bloques), favorece mediante un protocolo de intercambio las transacciones informáticas de criptomonedas escapando de cualquier autoridad Judicial que supervise estas operaciones, haciendo multitud de operaciones económicas que escapan de las reglas económicas , al usar criptomonedas en la mayoría de transacciones amparándose en el anonimato, para entender este tipo de tecnología tan compleja el autor Ricardo Pérez Marco, en el artículo[128] del País, donde explica este cadena de bloques:

> "*La nueva tecnología que está detrás de la red Bitcoin se llama "tecnología blockchain". El nombre proviene de que cada 10 minutos se produce, como venimos de explicar, un consenso (una votación) en la Red para establecer las nuevas transacciones válidas. Se reúnen en lo que se llama un "bloque" de transacciones. Luego estos bloques se "encadenan" criptográficamente de manera que no se puede reescribir ningún bloque sin reescribir todos los siguientes. Obtenemos así una "cadena de bloques", o blockchain en inglés, en la que reside la fiabilidad y verificabilidad de la contabilidad de la Red. Al no estar nadie al mando, la red Bitcoin se comporta como un organismo vivo*".

La cadena de bloques nos presenta para la estratificación de fondos, mediante compras y transferencias electrónicas en este mundo virtual que produce más opacidad a la hora de realizar el seguimiento e investigación de dudosas transacciones con criptomonedas.

Existe otro modelo que podría encuadrase como técnica de vigilancia y de ser utilizada en la lucha contra el ciberterrorismo, esta sería el reconocimiento por voz, una vez captados los audios podríamos llegar hasta la identificación del terrorista, como realiza el Grupo de Identificación de Voz de la Unidad[129] de Acústica Forense de la Policía Nacional, donde en

---

recognition.html?rref=collection%2Ftimestopic%2FSurveillance%20of%20Citizens%20by%20Government (Consulta el 15 de abril de 2019).

[128] El País. "La era del bitcoin y la tecnología blockchain". Ricardo Pérez Marco. 18 de diciembre de 2018. https://elpais.com/elpais/2018/12/11/eps/1544528073_261188.html

[129] Ministerio del Interior. Policía Nacional. "Comisaría General de Policía Científica" Acústica Forense. 2019 https://www.policia.es/org_central/cientifica/servicios/tp_acustic_foren.html

la propia web oficial de la policía, señala como competencias en el ámbito de la acústica forense investigando los siguientes:

1. Estudios sobre identificación de locutores.
2. Estudios sobre manipulación de registros, procesado y edición de la señal de sonido.
1. Estudios de pasaporte vocal. Consistente en:
2. Partiendo de un registro hablado establecer rasgos de identidad (edad, sexo, etc.), asociaciones diatópicas (área geográfica del hablante), diastráticas (estrato social), emocionales, conductuales, patológicas o toxicológicas.
3. Identificación de fuentes de registro.
4. Ruedas de reconocimiento de voz.
5. Análisis y determinación de falsificaciones y pirateo de soportes magnéticos de audio, en colaboración con otras Unidades (documentos, copia, vídeo).
6. Estudios de registros no vocales (sonidos, ruidos de fondo, etc.)
7. Acústica de disparos. Determinación de tipo de arma utilizada, ambiente acústico de la escena del crimen, etc.

A modo de ejemplo, se señala la eficacia de esta Unidad en la resolución y la detención de un presunto homicida en Santander[130] por el reconocimiento de voz, pudiendo llevar esta noticia al plano practico de este trabajo de TFG, enfocándolo a la detección de ciberterrorista una vez captada la voz de estos.

En China se está probando un nuevo sistema[131] para anticiparse a los crímenes y los delitos de terrorismo, que combina el reconocimiento facial y la inteligencia artificial. Mediante la captación de imágenes tanto en la vía pública como en entidades oficiales para crear una base de datos que analiza todas las variables de este individuo, analizando sus hábitos de comportamiento, su estilo de vida invadiendo en toda su amplitud su derecho a la Intimidad,

[130] El Mundo. "Criminales a los que la Policía caza por su voz". Ana María Ortiz. 20 abril de 2019. https://www.elmundo.es/espana/2019/04/20/5cb9fdeafc6c83411f8b45bb.html

[131] El País. "Lo que la tecnología puede hacer para combatir el horror" M. Victoria S. Nadal. 25 de agosto de 2017. https://retina.elpais.com/retina/2017/08/25/tendencias/1503654902_337040.html

dando datos tan específicos como cuántas veces ha pasado por una calle, en qué dirección, en que franjas de tiempo o si ha hablado con alguien más en varias ocasiones. Este sistema operativamente es de un valor incalculable pero choca con los derechos individuales al monitorizar el Estado todo nuestro movimiento.

La forma de combatir actualmente el ciberterrorismo debe combinar tanto la tecnología como estamos viendo y la investigación tradicional, la de calle, sabiéndose adaptar a los nuevos tiempos, por ello las redes sociales son un campo de investigación de gran valor, las grandes compañías han empezado a compartir información de en una base de datos única, compañías como Facebook, YouTube, Microsoft, han manifestado[132] su unión contra el Terrorismo, rompiendo estas multinacionales la dinámica de colaborar con las autoridades.

A grandes rasgos estas compañías han publicado un comunicado[133] en el que colaboraran para que aumente la lucha y la eficacia contra esta lacra y "*ayude a frenar la urgente cuestión global de contenidos terroristas en Internet".*

El proyecto DANTE

Detecting and Analysing Terrorist-related online contents and financing activities, es un proyecto dirigido al análisis de diferentes fuentes de información para prevenir posibles riesgos terroristas en tres áreas basado en inteligencia semántica: publicidad (reclutamiento, incitación, radicalización y desinformación), capacitación y recaudación de fondos.

El proyecto forma parte 18 socios de 10 países de la UE. Las características más importantes a nivel operativo son: extracción de datos, análisis de fuentes multimedia (audio, imagen, vídeo, texto) de web tradicional y de *deepweb* y recopilación de dichas fuentes de datos para los cuerpos de seguridad.

En España este proyecto recae sobre la compañía Expert System, cuyo trabajo lo define como "*la revisión en cinco idiomas innumerable material de texto y multimedia de Internet, que pueda encontrarse en países europeos como España, Francia, Italia o Bélgica*"

[132] El País. "Twitter, Facebook, YouTube y Microsoft se unen contra el terrorismo". Victoria S. Nadal. 2 de enero de 2017. https://elpais.com/tecnologia/2017/01/02/actualidad/1483356508_992114.html

[133] Facebook- Newsroom "Asociarse para ayudar a frenar la propagación de contenido terrorista en línea" (5 de diciembre de 2016) https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/

La información permite el control para el posterior análisis cruzando los datos y así establecer múltiples relaciones entre todos ellos, lo que facilitaría la investigación de las agencias de inteligencias para actuar con los ciberterrorista y su propaganda en la red.

La Inspectora de la Policía Nacional Silvia BARRERA experto en la investigación en la Red, desarrolla en una entrevista[134] publicada en YouTube, que las formas en las que trabaja la policía especializada en Delitos cibernéticos consisten en: *open source*, para hacer búsquedas, identificaciones en redes sociales y monitorizaciones de perfiles, de personas, de eventos.

Asimismo, esta agente nos cita otras herramientas de búsqueda más especializadas, sin facilitar ningún tipo de información, para preservar las técnicas de vigilancia de las FCSE.

El Instituto Nacional de Ciberseguridad, señala a España en el año 2017 como el tercer país más atacado del mundo, como refleja la noticia [135] donde el INCIBE, registro más de 115.000 mil incidencias por parte de particulares en el año 2016, lo que supone un aumento de un 130% con respecto al 2015, esta posición de bronce no es real, ya que muchos países del entorno se niegan a facilitar datos estadísticos de ataques e incidencias cibernéticas, estando según fuentes expertas en los mismo niveles de seguridad que países de nuestro entorno.

Un ataque relevante ocurrió en España fue el ataque [136] que dejo inoperante la página web del Banco de España, por un ataque de DNS, conocido como Dos, lo que nos hace ver que cualquier organismo está en el punto de mira de los ataques cibernéticos, este ataque proviene según fuentes expertas de Anonymous Catalunya, como respuesta a las detenciones de los líderes independentistas, estos utilizan los router de terceras personas que tras infectarlos con algún malware, utilizan a estos equipos para dirigirlos contra una web especifica como en este caso fue la del Banco de España.

---

[134] Youtube. "Cómo vigila la policía los delitos en internet? Silvia Barrera, de la UIT" El futuro es Apasionante. 14 de marzo de 2016. https://www.youtube.com/watch?v=ijjBiSu57SE (Consulta 1 de mayo de 2019).

[135] El Mundo "España, tercer país del mundo con más ciberataque". Jorge Benítez. 15 de mayo de 2017 https://www.elmundo.es/espana/2017/05/15/5918ae9222601d51718b46d7.html

[136] Cinco días "Un ataque *hacker* bloquea la web del Banco de España"27 de agosto de 2018. https://cincodias.elpais.com/cincodias/2018/08/27/midinero/1535368940_689955.html (Consulta el 6 de junio de 2019).

El Gobierno español ha aprobado recientemente un decreto-ley para transponer a nuestro el directivo NIS (Network and Information Security: Seguridad de las Redes y Sistemas de Información), de la Unión Europea.

Este decreto Ley 7 de septiembre de 2018 aprobado en el Consejo de Ministros transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.

Este Real decreto presenta medidas garantistas, como bien describe en su articulado donde, *"se requiere a los operadores de servicios esenciales y los proveedores de servicios digitales que notifiquen los incidentes significativos que sufran en las redes y servicios de información que emplean para la prestación de los servicios esenciales y digitales así como La norma protege a la entidad notificante y al personal que informe sobre incidentes ocurridos; se reserva la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permite la notificación de incidentes cuando no sea obligada su comunicación".*

Esto es una herramienta de gran ayuda a las fuerzas y cuerpos de Seguridad del Estado en el caso de que alguna persona tuviera reticencias por denunciar estas unidades receptoras de la información son:

GC https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

PN https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

Las FCSE, entre sus labores se encuentra:

- La vigilancia del ciberespacio y las redes en donde se comunican los ciberterroristas.
- Colaboración con los proveedores de Internet
- Colaboración con otros países en el ámbito Internacional.
- Preparación de Ciberataques para vulnerar las defensas de los ciberterroristas.
- Soporte de ayuda a infraestructuras críticas y detección ante posibles ataques cibernéticos.

El CNI dispone igualmente amparo Jurídico que se rige por el principio de sometimiento al orden Jurídico, con competencias y s actividades específicas reguladas en la Ley 11/2002 de 6 de mayo reguladora del CNI y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

El proyecto J-CAT.

En el año 2014 se impulsó la creación de otra unidad a nivel europeo, en la que el Gobierno Español, a través del Ministerio del Interior, se centra en el Organismo *Europol* para luchar contra el ciberdelito e invertir más recursos y mecanismos para impulsar la cooperación internacional.

Nace así El proyecto J-CAT, presentando como característica más representativa su carácter extraeuropeo, permitiendo la ayuda mutua entre país como Estados Unidos, Canadá, Australia o Colombia.

El proyecto J-CAT, corresponde a las siglas *Joint Cybercrime Action Task Force*, o Grupo de Trabajo Conjunto de Acción contra el Cibercrimen, perteneciente a *Europol* en la Unidad contra el Cibercrimen, conocida por las siglas EC3.

Esta Unidad[137] con sede en la Haya (Holanda), se inauguró el 11 de enero de 2014, y tal como indica la Comisión Europea, supone un cambio en el modelo integral de la UE, en la lucha contra el ciberdelito, lo que supone un impulso a las investigaciones criminales y fomentara las soluciones a nivel europeo. La Comisión Europea Manifiesta:

> *"El Centro también facilitará la investigación y el desarrollo y garantizará el refuerzo de las capacidades de las autoridades responsables de la aplicación de la ley, los jueces y los fiscales; asimismo, llevará a cabo evaluaciones de las posibles amenazas, que incluirán análisis, previsiones de tendencias y alertas tempranas. Con el fin de desmantelar un mayor número de redes de delitos informáticos y de perseguir a un mayor número de sospechosos, el EC3 recopilará y tratará los datos relacionados con la ciberdelincuencia y ofrecerá un servicio de asistencia en materia de ciberdelincuencia a las fuerzas de seguridad de los países de la UE. Además, prestará apoyo operativo a los países de la UE (por ejemplo, contra la intrusión, el fraude, el abuso sexual de menores en Internet, etc.) y aportará conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas".*

[137] La Comisión Europea." El Centro Europeo de Ciberdelincuencia (EC3)".http://europa.eu/rapid/press-release_IP-13-13_es.htm (Consulta el 7 de junio de 2019).

En este proyecto están presentes unidades de investigación del delito de diferentes países Estados Unidos (FBI y Servicio Secreto), Reino Unido, Australia, Colombia, Canadá, Alemania, Holanda, Austria, Italia y Francia., contando estos países con especialistas en:

- Malware y hacking.
- Fraudes en medios de pago.
- Explotación sexual de menores.

La mayor colaboración Internacional como ya hemos explicado hace de este proyecto una estrecha colaboración con otros países fuera de Europa, y así lo hace constar en el Ministerio de Interior[138] que ya incorporó en el 2014 a agentes de la Guardia Civil y La Policía Nacional para este Proyecto.

Ghost Security

Existe otros equipos de trabajo de Carácter No Oficial, ni dependientes de Organismo Públicos, este grupo de *hackers* activistas ocasionalmente colabora con las agencias de Inteligencia en la lucha contra el Estado Islámico, *hackeando* cuentas en favor de este Grupo en Twitter, algunos de los miembros de este Grupo, provienen de Anonymous.

En los informes de la lucha contra el ciberterrorismo se sabe que los ciberterroristas se reúnen en torno a plataformas como Facebook, Twitter e Instagram entre otras, haciendo uso de conversaciones privadas[139] con carácter "cifrado", para encriptar sus mensajes. Esto produce una barrera de difícil investigación para los cuerpos policiales al no poder adelantarse a las conspiraciones para atentar desde la red. Así lo manifiesta el director del Centro Nacional de Contraterrorismo de EE.UU, en la entrevista dada a Jim de Special Report de la CCN donde manifestó "está claro que nuestros adversarios terroristas descubrieron y

[138] Gobierno de España. Ministerio del Interior. "El Ministerio del Interior apuesta por Europol para reforzar la cooperación internacional en la lucha contra el cibercrimen" (06 de septiembre de 2014). http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2459641 (Consulta el 06 junio de 2019).

[139] Expansión. "La tecnología y la lucha contra el terrorismo" 24 de noviembre de 2015. https://expansion.mx/tecnologia/2015/11/24/la-tecnologia-y-la-lucha-contra-el-terrorismo (Consulta el 17 de mayo de 2019).

aprendieron cuáles son las formas de comunicación que hemos podido interceptar anteriormente. Ahora entienden que, si encuentran otras formas de comunicarse, pueden proteger sus comunicaciones".

Los ciberterroristas del ISIS, disponen de medios tecnológicos sofisticados así lo refleja el artículo de la CNN[140], donde pone de manifiesto la capacidad de los miembros de este grupo y su alta preparación disponiendo de 5 miembros que ofrecen servicio asesoramiento en la red las 24 horas del día. Este asesoramiento se da a través de un canal de la Aplicación de Telegram, al tener esta unas características propias que hacen las conversaciones más seguras y privadas.

Este grupo de asesoramiento dispone también de manuales de capacitación, así como ofrecer consejos para evitar las agencias de investigación estatales. Mostramos aquí algunas de las preguntas/ dudas que han sido captadas a este servicio del ISIS:

- ¿Cómo ocultar su número de teléfono al registrarse para aplicaciones como Telegram?: En una guía de la website CNNMoney[141] ya mostraba una guía demostrando como se podía el número de teléfono para crear cuentas tanto en Telegram como en Twitter.

- Otro tipo de Preguntas que realizan a este equipo es si deben comunicarse mediante Skype y la seguridad de esta aplicación para asegurar sus conversaciones.

- Otro tipo de consejos que dan son a la hora de publicar y difundir la propaganda de los ciber terroristas es evitar dejar constancia de su ubicación, así como informar de numerosos consejos para evitar la tecnología de reconocimiento facial.

Como se puede observar este tipo de asesoramiento dificulta el seguimiento y control de los ciberterroristas con pequeños consejos que dificultan enormemente la posible captura de los

[140] CNN. "*Top preguntas hechas en el 'Help Desk' de ISIS"*. Erica Fink y Laurie Segal, 18 de noviembre de 2015. https://money.cnn.com/2015/11/18/technology/isis-jihad-help-desk/index.html?iid=EL (Consulta el 13 de abril de 2019).

[141] Wikipedia. "CNNMONEY.COM" https://es.wikipedia.org/wiki/CNNMoney.com (Consulta el 14 de abril de 2019).

ciberterroristas. El experto en ciberseguridad el Dr. Aaron Brantly [142], expone en su página https://www.afterwestphalia.org/, que "el ciberespacio es complejo y requiere un enfoque multidisciplinario", por lo que requiere abarcar todos los campos posibles desde la inteligencias artificial, el tratamiento del Big data, la encriptación y los conflictos cibernéticos entre otros, para proporcionar a los Estados un arma tanto de persuasión como de contravigilancia y lucha contra los ataques ciberterroristas, numerosos ataques tan complejos y sofisticados entre países de primer nivel como China o Estados Unidos nos presentan casos relevantes muy de actualidad como indica el Informe[143] de amenazas cibernéticas de Estados Unidos, poniendo de manifiesto la cantidad de ramificaciones delictivas presentes en la red, entre ellas destapa la ubicación de más de 70 grupos de delitos informáticos alojados en Facebook, que publicitan actividad Ilícita[144], como se ha visto la inteligencia artificial combate este tipo de acciones comparando fotos y videos para cribar los que no cumplan unos requisitos de publicación y seguridad.

En la Web[145], señala a DigitaShadow como el grupo, *Ghost Security* que "*ha desmantelado 149 sitios de propaganda del Estado Islámico, 110,000 cuentas en redes sociales y más de 6,000 videos de propaganda.*". Este grupo no ha podido aportar datos verificados sobre las cuentas oficiales descubiertas en redes sociales.

Ghost Security confirmo que creó a través de un software automatizado, la identificación de cuentas del ISIS en redes sociales, consiguiendo interceptar las conversaciones privadas de los terroristas y poniendo al descubierto la IP, pudiendo llegar a logar la identificación y localización de los miembros de ISIS, aunque *Ghost*, se dedica en particular a perseguir a ciber terroristas del Estado Islámico, también persigue a otros grupos extremistas.

---

[142] Virginia Tech. Aaron F. Brantly. https://liberalarts.vt.edu/departments-and-schools/department-of-political-science/faculty/aaron-brantly.html (Consulta el 4 de abril de 2019).

[143] United State Military Academy." *Cyber Threat Report May*" 6 de mayo. https://digitalcommons.usmalibrary.org/aci_rp/40/ (Consulta el 7 de junio de 2019).

[144] Cyberscoop. "*Facebook albergó a más de 70 grupos de delitos informáticos que publicitaban todo tipo de actividad ilícita*". Jeff Stone. 5 Abril de 2019.https://www.cyberscoop.com/facebook-cybercrime-groups-cisco-talos/ (Consulta el 9 de junio de 2019).

[145] Expansión. "*La tecnología y la lucha contra el terrorismo*" .https://expansion.mx/tecnologia/2015/11/24/la-tecnologia-y-la-lucha-contra-el-terrorismo (Consulta el 22 de mayo de 2019).

GNUWATCH

Este programa *GNUWATCH*, utiliza el *HASH* de archivo como localizador remoto de contenidos, siendo el *Hash* de archivo un dato que sirve para identificar archivos, no mostrando el contenido, siendo necesario descargase el archivo para posteriormente se pueda certificar que el contenido genere sea el mismo *Hash*.

El error de este tipo de programa, según se ha visto en foros especializados[146] alojados en Emule, afirman que este programa no detecta a nadie por error, sino que cuando se da con un usuario es porque éste tiene la clara intención de descargar y tratar este tipo de contenidos.

En estos casos no podía faltar la cautela, y aunque hasta la fecha no se conoce que haya virus o malware que tengan que ver con este tipo de contenidos, que puedan llevar una imputación hacia ciertos delitos es necesario ver esta herramienta de trabajo como manifiesta este individuo con los procedimientos de investigación de la Policía, si bien en este caso es investigado por un delito de Pedofilia, nos valdrá para poner analizar el modus operandi de la investigación policial en otros caso como el ciberterrorismo:

El usuario del foro[147] reseñado anteriormente, de nombre Indignado7777, ofrece otra perspectiva contraria y critica a esta praxis policial investigativa, manifestando la siguiente visión del perjudicado por este tipo de técnica policial de investigación ,que debemos plasmar en este trabajo para contrastar las dos caras, este usuario del Foro de Internet ha sido detenido por una Operación anti-pornografía infantil ,cuestiona las técnicas de investigación de la Policía limitándola a tres pasos que desarrolla siendo estos:

1) El Rastreo P2P remoto (recopilación de IP).

2) Justificación judicial para identificar a los titulares de las IP (retirada amparo artículo 18.1CE).

[146] Foro. Emule. 15 de septiembre de 2013. https://forum.emule-project.net/index.php?showtopic=157143&st=20 (Consulta el 12 de mayo de 2019).

[147] Emule. Foro sobre detenidos PSP. 13 de septiembre de 2013. https://forum.emule-project.net/index.php?showtopic=157143&st=20 (Consulta el 12 de mayo de 2019).

3) Una vez recibida las identidades por parte de las operadoras, se justifica judicialmente los registros domiciliarios simultáneos en todo el territorio nacional (retirada del amparo constitucional al 18.2). Manifiesta lo siguiente:

"Que Efectivamente esos rastreos P2P podrían y deberían servir para poner en alerta a los agentes". Pero la labor policial se limita a tres pasos:

Este detenido critica la fase de investigación en el ámbito tecnológico reprochando que "nunca *se interceptan las comunicaciones de los sospechosos*" (artículo 18.3CE), así como de no existir una línea de investigación adicional sobre los titulares de esa IP o las personas que habitan en su casa.

No se hace un seguimiento de sus vidas o de su entorno, sobre otras posibilidades de usurpación o robo de la IP, ya que no se revisa si la Wifi está abierta, tal como indica la noticia[148] del periódico digital Cincodias donde narra que el 8,7% de los internautas españoles le roba la WIFI a su vecino.

Este usuario del foro de Internet manifestó sus dudas sobre la praxis policial en la forma de llevar a cabo las investigaciones cibernéticas, y dejando ciertas dudas sobre la imparcialidad de las FCSE en el proceso Judicial.,

Las FCSE junto al CNI, tiene la capacidad y los conocimientos necesarios para verificar y comprobar operativamente diversas técnicas de ataque y vigilancia en las labores investigativas el acceso a la red Wifi, es una fuente inagotable de información y control sobre el objetivo que se persiga, ya que los ciberterrorista utilizan como medida de seguridad utilizan las redes Wifi de terceros para realizar su acciones, con las siguientes técnicas de ataque y control se puede llegar a controlar a estos:

Es muy importante destacar los tipos de ataque y control en las redes Wifi, que serían de modo pasivo, es decir no se modifica la información, solo se escucha y se monitoriza la información, este modus operandi es difícil de detectar y será de gran ayuda a las agencias de Inteligencia para adelantarse a un posible ataque.

[148] Cinco dias. "*El 8,7% de los internautas roba el wifi del vecino*". 14 de julio de 2011. https://cincodias.elpais.com/cincodias/2011/07/14/tecnologia/1310881605_850215.html (Consulta el 26 de abril de 2019).

De otro lado se encuentra el modo activo, donde los agentes se introducen en los equipos y sin estar autorizado modifica o deniega el acceso a la información, por lo que esta operatividad haría de cortafuegos ante una posible llamada a realizar atentados terroristas.

Algunas de estas modalidades son:

- *Sniffing*. Se explica como un ataque pasivo que monitoriza toda la información que va por la red, debido a las debilidades de las redes inalámbricas, es más factible llega a acceder desde un tercer equipo al contenido de los paquetes de información.

- Análisis de datos. Este equipo de ataque pasivo analiza de manera detallada el uso del equipo, es decir, su encendido y apagado, duración del uso, equipos con los que interactúa, etc., por lo que aporta una información valiosa a la investigación llevaba a cabo.

- Suplementación o enmascaramiento. En este modus, se trata de apoderarse de la autentificación real del usuario para poder acceder a la información dentro de la red.

- *Access Point Spoofing*. Es una suplantación por la que se hace pasar por otra red *WLAN*, logrando que las victimas crean que están conectada a una red de su confianza.

- *Rogue Access Point*. Se enfocaría como acceder a un dispositivo conectado a una red segura sin la autorización del responsable de la red Wifi.

- *Denegación de Servicios* (DoS). Este método consiste en generar interferencias hasta que produzcan errores de la velocidad y hacer caer la red, provocando el cese de actividad de la web.

Las FCSE, junto a las agencias de inteligencia deben dominar tanto la defensa como el ataque, por el bien de la detección e intrusión del ciberterrorista, por ello es necesario conocer la disciplina de la Esteganografia que se desarrolla en el siguiente punto.

La esteganografía

Esta es otra disciplina que deben conocer nuestros servicios de Inteligencia es la disciplina que trata del estudio y la aplicación de técnicas para ocultar información, dentro de otros, de

manera que no se perciba su existencia, a grandes rasgos es ocultar mensajes dentro de otros objetos, y poder tener un canal de comunicación oculto, que puede no estar encriptado como se pudiera creer, pero que pasa inadvertido para los investigadores.

En el ámbito cibernético tanto el mensaje como el portador puede ser un software creado para tal fin, dándose generalmente medios sencillos como una simple fotografía, audio o video que insertan los ciberterroristas para trasmitir mensajes ocultos, a estos se añade la problemática de que estos mensajes son previamente encriptados, lo que dificulta aún más a los investigadores el avance en la investigación.

Estas técnicas, aunque desconocidas están muy presentes en nuestros días, en el sistema Android se encuentra la aplicación llamada Steganography Máster, que oculta texto en el interior de imágenes, y que solo se puede descifrar desde esta aplicación. Para iOS se encuentra "Steganographia", que realiza similares características donde utilizan fotografías para ocultar los textos que se pretenden encriptar.

De igual manera las fuerzas de Seguridad deben velar por la actualización permanente con software que detectan este tipo de contenido oculto en archivos es lo que se llama el estegoanálisis[149], definiéndola Wikipedia como ":

> "*la disciplina dedicada al estudio de la detección de mensajes ocultos usando esteganografía. Dichos mensajes pueden estar ocultos en diferentes tipos de medio, como pueden ser por ejemplo las imágenes digitales, los ficheros de vídeo, los ficheros de audio o incluso un simple texto plano".*

Han sido muchas las aplicaciones criptográficas que se han sugerido como complemento para proteger la información y el contenido., la gravedad de la información que se pueda trasmitir y el modus que se utiliza está prohibido en muchos países del mundo, como Francia o China, en EE. UU está fuertemente controlado al catalogarse como amenaza para la seguridad nacional [150]

[149] Wikipedia. Estegoanalisis. 2019. https://es.wikipedia.org/wiki/Estegoan%C3%A1lisis (Consulta el 1 de junio de 2019).

[150] http://laredargen.www6.50megs.com/criptografia.htm (Consulta el 4 de mayo de 2019).

En este modus operandi, se está trabajando para tener comunicaciones secretas y ocultas a través de programas como WhatsApp, Line o Spotbros, que son la referencia actual en el ámbito de la mensajería instantánea.

En la siguiente Ilustración se muestra el proceso estenográfico básico:

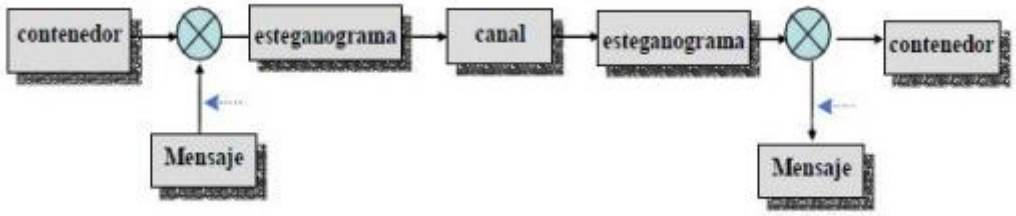

Ilustración 8. Proceso estenográfico.

Esta disciplina ayuda, en gran medida, a mantener comunicaciones ocultas entre los servicios de inteligencia de los Estados, así como a policías infiltrados en redes criminales, mantener el anonimato en el voto electrónico, algunas de las aplicaciones más conocidos según Arturo Ribagorda, Juan M. Estévez-Tapiador y Julio César Hernández, Esteganografía, estegoanálisis e Internet (2007) son: F5, Jsteg, OutGuess, EzStego y Steganos.

Las Fuerzas y Cuerpos de Seguridad utilizan en Internet herramientas de búsqueda en redes P2P, conocidas como rastreadores. Un rastreador es una herramienta que como su nombre indica, rastrea la redes, generalmente P2P, en busca de imágenes similares a las almacenadas en una base de datos de imágenes pedófilas incautadas, pero la búsqueda y comparación no la hace con las imágenes tal cual, sino mediante su *hash*.

Un hash es un identificador inequívoco de un archivo informático, el cual se genera aplicando unos algoritmos matemáticos a un fichero de entrada y obteniendo una cadena alfanumérica única para ese archivo, el *hash*. El rastreador compara el *hash* de los ficheros compartidos por los usuarios en la red P2P investigada, con una base de datos.

Si los *hashes* coinciden es que el archivo es el mismo, y por lo tanto el fichero analizado del usuario es un resultado positivo. La averiguación del valor *hash* es una tarea investigadora que no afecta a derecho fundamental alguno, es un dato público, por lo tanto, no requiere de autorización judicial.

La identificación de los ficheros por su *hash* es de gran importancia en las investigaciones policiales ya que, aunque se cambie el nombre del fichero, el código *hash* sigue igual, por lo

que las simples medidas de seguridad que puedan tomar los ciberterroristas como renombrar los ficheros para esconder su material a la hora de compartirlo no serán efectivas.

La BCIT actualmente emplea los rastreadores SpyMule, NordicMule y GnuWatch.

El Cuerpo Nacional de Policía colabora en proyectos para el desarrollo de otras herramientas para la lucha contra los delitos cometidos en el Ciberespacio, junto con el INCIBE (Instituto Nacional De Ciberseguridad), avanzan en el proyecto ASASEC18 (Advisory System Against Sexual Explotation of Children).

El objetivo de ASASEC es facilitar la identificación de evidencias a los investigadores en los dispositivos incautados en el ámbito de una operación policial. ASASEC es capaz de procesar grandes volúmenes de datos de cada uno de los dispositivos de almacenamiento analizados, ofreciendo como resultado un listado priorizado de todos los archivos, clasificándolos, y distinguiendo los posibles positivos de en especial del tipo pena de posesión de pornografía infantil, pudiendo ser utilizado para otros fines como la lucha contra el ciberterrorismo., siendo necesario dar respuesta ágil y eficaz del Derecho Internacional para que ciberespacio no sea escondite ni lugar de encuentro de los ciberterrorista.

Este tipo de delitos que no conocen de fronteras, la leal colaboración internacional debe ser una máxima en la lucha de estos delitos, a pesar del desconocimiento y falta de formación por parte del ámbito judicial de la mayor parte de los aspectos relacionados con las nuevas tecnologías de la información y la comunicación, por lo que resulta de vital importancia dotal de cursos de formación a estos profesionales que permitan, dada que la complejidad técnica de los procesos, conocer el alcance de las medidas que puedan solicitarse. En este punto podemos encuadrar la figura del Agente encubierto, en la lucha contra el ciberterrorismo el cual se define como "*empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red"* mediante "*la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los ciberdelincuentes"*, actúan con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales (Villanueva, 2016).

Los agentes estarán habilitados para crear un pseudoperfil en cualquier red social, e intercambiar con otro usuario material que pudiera ser sea constitutivo de delito, para lograr recabar las pruebas y poner a Disposición judicial al autor.

Los agentes podrán grabar imágenes y conversaciones cuando ello sea necesario, con medios y conocimientos técnicos analizar los algoritmos asociados a estos archivos ilícitos con la finalidad de localizar a los supuestos autores de determinados hechos delictivos.

La reforma procesal de la Ley Orgánica 13/2015[151], por la que se modifica de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, esta reforma actualiza el uso de tales recursos por el agente encubierto pueda obtener imágenes y grabar conversaciones bajo la Autoridad Judicial.

El Agente encubierto actualmente se infiltra en canales cerrados de comunicación bajo tutela judicial, para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación" regulados ciertos requisitos en la ley Apartado IV de la Exposición de Motivos de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. BOE núm. 239. El Fiscal Juan Ignacio Zaragoza Tejeda, en su ponencia[152], la importancia de dotar de respaldo legal y seguro a los agentes encubiertos, señalando como "*Según la Directiva 2014/41/CE del Parlamento Europeo y del consejo 158, relativa a la orden europea de investigación en materia penal, en su artículo 29, titulado "Investigaciones encubiertas", se centra en las características que ha de tener las investigaciones encubiertas, las cuales define como "realización de investigaciones de actividades delictivas por parte de agentes que actúen infiltrados o con una identidad falsa.".*

Es necesaria dar respuesta ágil y eficaz del Derecho Internacional para que ciber espacio no sea escondite ni lugar de encuentro de los ciberterrorista.

---

[151] Gobierno de España. Ministerio de la Presidencia relaciones con las Cortes e igualdad." Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica." BOE. Publicada 6 de Octubre de 2015.https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725. (Consulta el 07 de junio de 2019).

[152] Zaragoza Tejeda, J. (2019). "L*a modificación operada por la ley 13/2015 el agente encubierto informático".* https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Zaragoza%20Tejada,%20Javier%20Ignacio.pdf?idFile=d16b7d76-2654-4b4e-abdf-b00f2540d57b (Consulta el 07 de junio de 2019).

Este tipo de delitos que no conocen de fronteras, la leal colaboración internacional debe ser una máxima en la lucha de estos delitos, a pesar del desconocimiento y falta de formación por parte del ámbito judicial de la mayor parte de los aspectos relacionados con las nuevas tecnologías de la información y la comunicación, por lo que resulta de vital importancia dotal de cursos de formación a estos profesionales que permitan, dada que la complejidad técnica de los procesos, conocer el alcance de las medidas que puedan solicitarse.

Israel dispone de los más avanzados equipos de ciberespionaje,creando la Agencia Aman, donde se agrega la Unidad 8200, cuya definición en Wikipedia la define como "*la unidad perteneciente a los Cuerpos de Inteligencia de las Fuerzas de Defensa de Israel cuya misión es la captación de señales de inteligencia y descifrado de códigos*." con funciones similares a la NSA, esta unidad se sospecha que está detrás del fallo de la red siria de radares que se produjo antes del ataque efectuado por las Fuerzas Aéreas de Israel a un reactor nuclear encubierto de este país, tal como se comentó anteriormente, así como el responsable del desarrollo del gusano informático Stuxnet.

En el Documental[153] de HISPANTV, alojado en Facebook, los *Hacker* de *Anonymous* ARAB, amenazan con causar el mayor daño posible tanto a objetivos civiles como a militares el 7 de abril.

[153] Facebook. *"Guerras Frías del Mundo",* abril de 2014. https://www.facebook.com/Dj.Sky.Starboy.warrior/videos/2230464673870418/ (Consulta el 11 de abril de 2019).

5 UNIDADES CONTRA EL CIBERTERRORISMO EN ESPAÑA Y EUROPA

5.1 Agencia de la Unión Europea para la Formación Policial (Cepol).

Es necesario la Unificación de criterios, la coordinación Internacional y una formación especializada de los diferentes cuerpos de Seguridad del Estado de los Estados miembros, por ello en el año 2001 se creó CEPOL[154], siendo este Organismo una "Agencia que forma parte de una red de cooperación policial integrada por los centros nacionales de formación de los servicios de Policía de los Estados miembros de la Unión Europea.".

Presenta un objetivo principal que es la cooperación transfronteriza para prevenir y luchar contra la delincuencia a todos los niveles dentro de la Unión Europea.

Esta escuela imparte a los Policías numerosos cursos para especializar a los agentes en las materias más sensibles y complementar la formación y especialización en beneficio de una mayor seguridad dentro de la Comunidad Europea.

Su sede se encuentra en Budapest, (Hungría), donde entre sus actividades principales son:

- La Formación de Mandos Policiales en leyes y normas europeas.
- La Formación especializada para policías y formadores policiales.
- Ofrece el intercambio de Personal policial entre Estados.

Como se observa la Prioridad de esta Escuela es la formación dando un valor primordial al respeto a los derechos humanos y de las libertades fundamentales en el contexto policial, tal como indica el reglamento 2015/2219 del Parlamento Europeo y del Consejo.

En el Art 3. del Reglamento de CEPOL, hace hincapié en la lucha contra la delincuencia grave y organizada que afecte a dos o más Estados miembros, y el terrorismo, el mantenimiento del Orden Público, en particular el control policial internacional de grandes acontecimientos.

[154] Wikipedia. CEPOL. https://es.wikipedia.org/wiki/Escuela_Europea_de_Polic%C3%ADa (Consulta el 8 de junio de 2019).

5.2 Unión de Cooperación Judicial (EUROJUST).

Este Organismo no es nuevo y su creación se remonta al año 2002, en la Decisión 202/187/JHA[155] del consejo que posteriormente fue modificada en el año 2009 en la Decisión 2009/426/JHA[156], la sede se encuentra en la Haya, los Estados nombre representantes de jueces, fiscales o funcionarios policiales.

Como ya hemos visto es fundamental la colaboración entre Estados para la lucha contra el ciberterrorismo. Eurojust es una herramienta básica para perseguir de manera a los delincuentes y terroristas sirviéndose de una rápida y eficaz comunicación, coordinación entre los Estados Miembros, por lo que es considerado como un elemento fundamental en la lucha contra las formas Graves de Delincuencia y como Centro de experiencia en la lucha contra la Criminalidad Organizada, reduciendo la problemática transfronteriza.

En la propia página de Eurojust, informa que tramitan más de 200 casos anuales que van desde las cuestiones sobre la tramitación de asuntos hasta la planificación operativa que puedan surgir entre Policías de varios Estados, como puedan ser registros simultáneos en diferentes países.

Las funciones principales son "*las reuniones de coordinación se centran en casos concretos, en relación con los delitos considerados como prioritarios por el Consejo de la Unión Europea: terrorismo, narcotráfico, tráfico de seres humanos, fraude, corrupción, delito informático, blanqueo de capitales y otras actividades ilegales relacionadas con la presencia de grupos delictivos organizados en la economía*." Eurojust 2019.

Otro de los accesos a este Organismo más común son los conflictos de Jurisdicción donde se marcará que Autoridad Nacional es la competente para llevar la investigación o una diligencia Judicial en cuestión, marcando quien debe ser el responsable de dicho acto.

[155] Diario Oficial de la Comunidad Europea. Decisión del consejo de 28 de febrero de 2002. http://eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Eurojust%20Decision%20(Council%20Decision%202002-187-JHA)/Eurojust-Council-Decision-2002-187-JHA-ES.pdf

Eurojust, facilita la ejecución de los instrumentos jurídicos como la conocida como Orden Europea de Detención[157], esta Orden ha dado lugar a numerosas quejas sobre su funcionalidad por la forma de proceder de varios Estados a raíz de la OED, del presidente de la Comunidad Autonómica Catalana Carles PUIGDEMONT.

5.3 Agencia Europea de Seguridad de las redes y de la información. ENISA.

Esta agencia de Ciberseguridad de la UE apuesta por dar mayor protección de los sistemas, por lo que crea Enisa, siendo este, un centro de conocimiento especializado para la Seguridad Cibernética tiene su sede en Heraklion (Grecia), esta agencia ayuda a prevenir, detectar y dar soluciones a los problemas de seguridad de la información.

Esta agencia ofrece soluciones a empresas públicas y privadas de la UE, en los ámbitos de la Ciberseguridad, para ello organiza ejercicios[158] de una posible gestión de crisis cibernética., de igual manera fomenta la cooperación entre los equipos de Emergencias informáticas y la creación de Capacidades.

La estructura de Enisa, se regula por los Reglamentos CE. N. 460/2004[159] y (UE) núm. 526/13.[160]. Este Organismo ayuda a dar estabilidad económica al mercado interior europeo, la forma de proceder de este Organismo según marca en su propia web es:

---

[157] Gobierno de España. " Cooperación Jurídica Internacional Orden Europea de Detención y entrega."https://www.mjusticia.gob.es/cs/Satellite/es/1215197995954/Tematica_C/1215198003700/Detalle.html (Consulta el 12 de abril de 2019).

[158] Enisa. "European Unión Agency for Network and Information Security".2019 https://www.enisa.europa.eu/topics/cyber-exercises (consulta el 15 de abril de 2019).

[159] Parlamento Europeo. "Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información. 13 de marzo de 2004. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:ES:HTML (Consulta el 1 de junio de 2019).

[160] Parlamento Europeo. " REGLAMENTO (UE) No 526/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 21 de mayo de 2013 sobre la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004" https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN (Consulta el 16 abril de 2019).

- Experiencia: anticipar la aparición de problemas de seguridad de la información y de las redes y ayudar a Europa a hacerles frente teniendo en cuenta la evolución de lo digital.

- Política: asistir a los Estados miembros y a las instituciones de la UE en la elaboración y aplicación de las políticas necesarias para cumplir los requisitos legales y reglamentarios de la Seguridad de la Información Nacional.

- Capacidad: ayudar a Europa a dotarse de los medios más avanzados de seguridad de las redes y la información.

- Comunidad: potenciar la cooperación tanto entre Estados miembros como entre las comunidades de Seguridad de la Información Nacional.

ENISA trabaja desde todas las ramas desde la Ciberseguridad hasta temas tan actuales como el ciber *Bullyin*g tal como muestra el reportaje sobre este asunto y los consejos y recomendaciones para el tratamiento de este delito, en la siguiente imagen se observan los consejos prácticos para combatir el **acoso escolar** en la red:

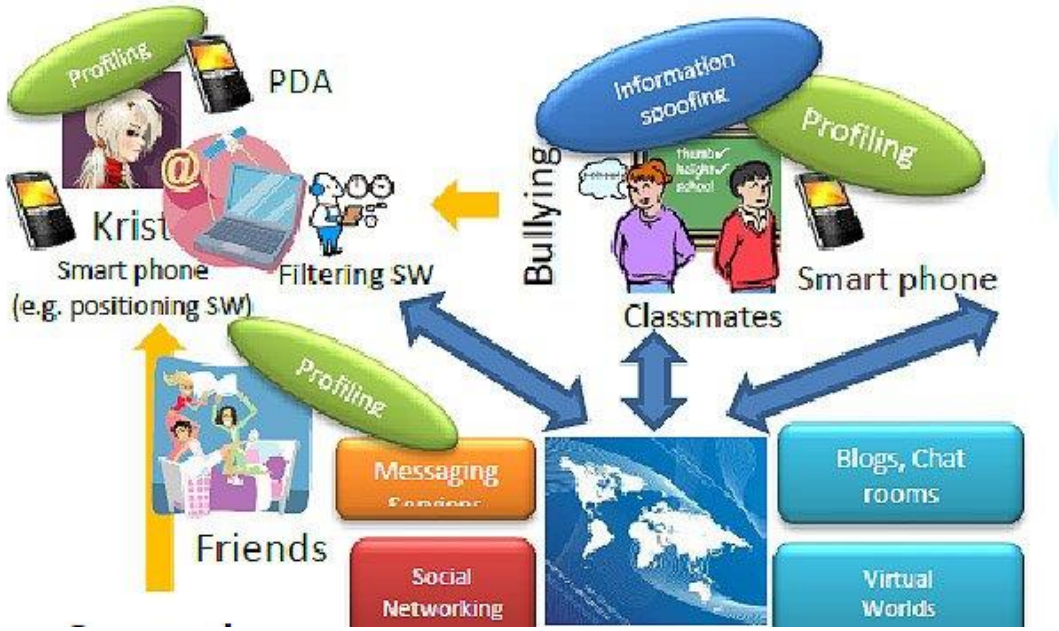

Ilustración 9. Agencia Europe. ENISA. Campaña contra el cyber- bullying.

5.4 Instituto de Ciberseguridad (INCIBE).

El Instituto Nacional de Ciberseguridad, está orientada a trabajar para elevar el nivel de confianza digital, elevar la seguridad en la Red, y contribuir al impulso del uso seguro del ciberespacio de España, desde el 28 de octubre de 2014, el Instituto Nacional de Tecnologías de la Comunicación paso a llamarse como hoy lo conocemos como INCIBE.

Este Organismo depende directamente del Ministerio de Economía y Empresa, siendo la mayor referencia en el campo de la ciberseguridad. El Estado Español a través de INCIBE, impulsa la investigación para preservar la ciberseguridad tanto a nivel nacional e internacional a través de los que llamamos INCIBE-CERT, que son tal como define el Organismo[161]:

> "*INCIBE-CERT es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública.*"

INCIBE, fomenta los conocimientos y la trasparencia en el ámbito de la ciberseguridad, a través de los agentes unificando criterios de apoyo y coordinación en la red, fortaleciendo la seguridad Nacional. En la siguiente Imagen se muestra la estructura de Incibe:

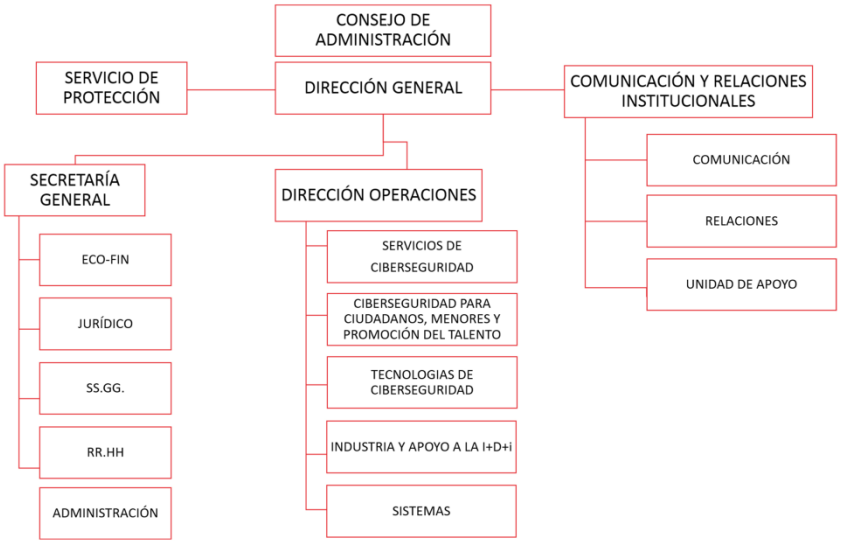

Ilustración 10. Estructura INCIBE.

[161] Instituto Nacional de Ciberseguridad. https://www.incibe.es/que-es-incibe (Consulta el 7 de abril de 2019).

Otro acierto de INCIBE, es la Oficina de Seguridad del Internauta[162], que se presta de manera gratuita a los usuarios para resolver problemas que pueden ocurrir en la red, guiando en aspectos básicos de los usuarios noveles de las nuevas tecnologías.

Entre algunos consejos que se encuentran alojados en la web de esta Oficina, orientando en tareas muy útiles como la instalación de Antivirus, el análisis de nuestro equipo para observar si tenemos instalados herramientas espías o la eliminación de archivos temporales a través de herramientas de limpieza.

5.5 Centro Nacional para la Protección de Infraestructuras críticas.

Este centro fue creado en el 2007, consiguiendo sus competencias reguladas en la ley 8/2011[163], estableciendo medias para la protección de Infraestructuras críticas en el Real Decreto 704/2011[164], donde se refleja el reglamento vigente para la protección de Infraestructuras críticas, de especial interés es el apartado h, donde especifica:

> "*Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados*".

Analizando esta Ley el apartado K, hace hincapié en la colaboración y coordinación con el Centro Nacional de Coordinación Antiterrorista, tal como señala en dicho apartado:

> "*Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación Antiterrorista, los informes sobre evaluación de amenazas y tipos de*

---

[162] Oficina de Seguridad del Internauta. https://www.osi.es/es (Consulta el 18 de mayo de 2019).

[163] B.O.E. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf (Consulta el 11 de mayo de 2019).

[164] MINISTERIO DEL INTERIOR. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf (Consulta el 18 de mayo de 2019).

vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva".

En la web del Cnpic, nos muestra en el siguiente grafico el nivel de alerta en el que nos encontramos, estando en la actualidad en nivel 4, Alto, considerado de Alto riesgo.

Ilustración 11. CNPIC. Nivel de alerta de Infraestructuras Críticas.

5.6 Cuerpo Nacional de Policía. Brigada de Investigación tecnológica.

La Policía Nacional presenta una de las unidades más especializadas e importantes de este Cuerpo Policial, conocida bajo las siglas BIT.

La Brigada Central de Investigación Tecnológica da respuesta a las nuevas formas de delincuencia graves en todas las ramas delictivas desde Organizaciones Criminales hasta pequeñas estafas y fraudes por Internet.

Esta unidad está encuadrada en la Unidad de Investigación Tecnológica, dependiente de la Dirección General de la Policía. Tiene como misión: perseguir a los delincuentes y poner a unas y otros a disposición judicial, la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación en los foros internacionales de cooperación policial y la colaboración ciudadana.

Actualmente cuenta con más de 90 agentes que van desde Ingenieros informáticos, técnicos informáticos dedicados a la lucha cibernética., como se ha dicho anteriormente asumen las Funciones recogidas en el art 7.6 de la Orden INT/28/2013[165] de 18 de enero.

Fundamentalmente esta unidad obtiene pruebas para perseguir delitos y detener a delincuentes solicitando muchas en muchas ocasiones la colaboración de los ciudadanos difundiendo ciertos fotogramas para su difusión y que sirven de gran ayuda para esclarecer crimines o criminales. En la siguiente imagen veremos la estructura de la BIT:

Ilustración 12. Estructura de la BIT[166]

[165] Gobierno de España, Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. B.O.E. https://www.boe.es/buscar/doc.php?id=BOE-A-2013-662 (Consulta el 12 de junio de 2019).

[166] Fuente: Gobierno de España. Ministerio de Interior. Conferencia Navaja Negra.

6 FORMAS DE FINANCIACIÓN DEL CIBERTERRORISMO

6.1 El Bitcoin

El Bitcoin, es una moneda virtual, una moneda Criptográfica, usada como dinero electrónico que escapa de los controles tradicionales de la banca monetaria mundial.

Este dinero nació con la idea de descentralizar los pagos, puenteando las instituciones financieras en las transacciones y trasferencias financieras, su uso está creciendo en todos los ámbitos y popularizándose su uso.

A pesar de lo que se pueda pensar el uso de esta moneda virtual es bastante seguro, tal como señala INTECO-CERT[167], resumiendo sus fortalezas:

- La implementación de recompensas en forma de monedas virtuales incentiva la participación de los usuarios en la red., actuando como nodos que realizan los cálculos complejos que se requieren.
- La seguridad que ofrece Bitcoin por medio de criptográficas de seguridad da como resultado un alto nivel de seguridad.
- La escalabilidad del sistema garantiza a largo y medio plazo.
- La trasparencia es otra característica ya que las transacciones pueden ser comprobadas por cada usuario de donde proviene y a dónde va cualquier bitcoin.

Actualmente el Bitcoin es utilizado por los ciberterroristas para realizar tratos ilegales, tanto para la venta de armas o drogas como para cometer actos ilícitos y pagar en esta moneda virtual para dificultar la investigación. Este dinero puede convertirse en moneda de curso legal, hoy en día ya existen cajeros automáticos que autorizan a pagar con divisa digital, en España existen unos 7000 puntos para realizar esta función. La mayoría de las acciones

[167] Instituto Nacional de Tecnología de la Comunicación INTECO. BITCOIN. "Una moneda Criptográfica". https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf (Consulta el 11 de junio de 2019).

realizas ilícitamente tienen su origen en TOR, estos portales permiten ocultar la IP, la agencia Europol estima que el 30%[168] de los servicios que se alojan en este servidor son ilegales.

Los bitcoins facilitan la comisión de delitos al presentar unas características ventajosas para no ser alcanzado como es el anonimato, la privacidad en las transacciones y la clara falta de regulación en cuanto a los límites de dinero, siendo el único impedimento la cadena de bloques de la que hablamos anteriormente que permite saber de dónde proviene y a donde va dirigido las monedas virtuales conocidas como Criptomonedas.

La tecnología de cadena de bloques, también conocida como Blockchain, es la encargada de llevar la contabilidad de las cuentas y el uso de las claves para realizar las trasferencias. El modus operandi la siguiente, las criptomonedas deben registrarse en a nombre de las "claves electrónicos", Diego Rodríguez Roldan, experto y asesor de la Empresa Deloitte señala como característica de este sistema:

> «*es anotarla en cualquier nodo de la red blockchain, firmada por la 'clave electrónica' origen*», por lo que, con la clave electrónica facilitada, la red aceptaría este movimiento y verificaría la criptomoneda junto a la firma ya validada.

Estos nodos no presentan escalones o niveles careciendo de autoridad administrativa, por lo que los servidores una vez verificados guardan la cadena de bloques. Bitnodes señala que existen más de 7200 nodos operando. En el siguiente grafico se muestra el número de nodos accesibles en el mundo:

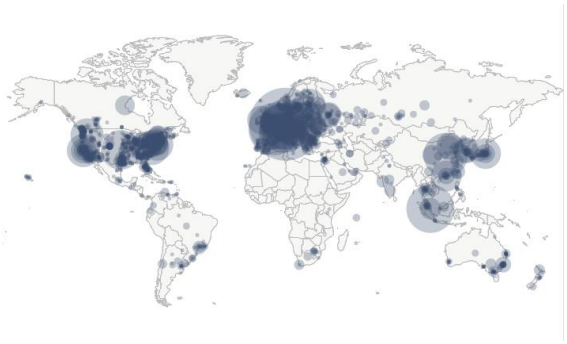

Ilustración 13. Nodos accesibles en el mundo[169]

[168] ABC "*Nacen los «criptomercados», tiendas online de drogas en internet*" Agencia EFE. 25 de septiembre de 2019. https://www.abc.es/tecnologia/redes/abci-nacen-criptomercados-tiendas-online-drogas-internet-201602111745_noticia.html (Consulta el 2 de junio de 2019).

[169] Mapa de Nodos de BITCOIN. https://bitnodes.earn.com/te (Consulta el 3 de junio de 2019).

El miedo al uso de esta moneda y pérdida de control hace que numerosos países prohíban las criptomonedas entre ellos China[170], dando como argumento un posible fraude financieros y estafas piramidales.

6.2 Grupo DD4BC y consecuencias

Este grupo es considerado un grupo de ciberdelincuentes que exigen a través de chantajes pagos a terceros por medio de Bitcoins, evitando los ataques DDoS, por lo que los pagos deben realizarlo en moneda virtual dificultando como hemos visto su investigación.

Este grupo autodenomina DD4BC, por las siglas (DDos for Bitcoin), ha sofisticado sus ataques y su frecuencia llegando a todas las esferas tanto en el ámbito privado como a Organismos Oficiales. El modus operandi de este grupo es lanzar ataques DDoS, que irán creciendo hasta lograr que el ataque lanzado resulte efectivo. Con un ataque inicial de entre 10 y 20 GBps, de magnitud masiva pero capaz de agrandar si cabe esta densidad de ataque. Para los usuarios afectados se recomienda no pagar a este grupo, según el blog.elhacker.net [171]

En el año 2014 intensifico sus ataques llegando incluso a expandir sus acciones a países como Suiza, al tener los usuarios residentes en dicho país un alto nivel económico, siendo estas víctimas de chantajes[172], con nuevos ataques DDoS.

---

[170] Xataka. "Pánico en el mundo de las criptomonedas: China prohíbe las ICOs" Javier Pastor. 4 de septiembre de 2017. https://www.xataka.com/empresas-y-economia/panico-en-el-mundo-de-las-criptomonedas-china-prohibe-las-icos (Consulta en 11 de junio de 2019).

[171] El blog. El hacker. "*DD4BC extorsiona pidiendo dinero en Bitcoins a cambio de parar sus ataques DDoS* " 19 de junio de 2015 https://blog.elhacker.net/2015/06/dd4bc-extorsiona-pidiendo-dinero-en-bitcoins-a-cambio-de-parar-sus-ataques-DDoS.html (Consulta el 11 de junio de 2019).

[172] Concellodemelon. "*El Grupo de Extorsión Bitcoin DD4BC solicita una advertencia del gobierno suizo*" https://www.concellodemelon.org/news/el-grupo-de-extorsion-bitcoin-dd4bc-solicita-una-advertencia-del-gobierno-suizo/ (Consulta el 12 de abril de 2019).

7 CONCLUSIONES

El imparable avance de las tecnologías de la información y la comunicación, su incursión en los aspectos cotidianos ha hecho que todas las facetas diarias de nuestra vida estén condicionadas por el uso del acceso a la red, su penetración en los múltiples y variados aspectos de la vida, su utilización generalizada por parte de todos los ciudadanos y por los organismos e instituciones tanto del sector público como privado está revolucionando nuestra sociedad.

Tras todo el análisis realizado, se ha podido observar la realidad serena pero amenazante entre los conceptos del cibercrimen y del ciberterrorismo, siendo ambos una amenaza para nuestra sociedad, donde los gobiernos están actualizando el marco normativo con leyes cada vez más específicas para la protección de nuestros Derechos fundamentales.

Las nuevas tecnologías y modus operativos de los servicios de Inteligencia para defender la Seguridad mundial, ha creado equipos de incidentes ante ciberataques, un paso muy importante que marca la línea de trabajo conjunto, con equipos multidisciplinares, tanto en el ámbito privado como en los cuerpos policiales donde se ha observado la ayuda mutua que se prestan las agencias descritas en el punto 5 de este trabajo.

A la par se viene dotando de tecnología digital e informática cada vez más sofisticada para la rápida actualización de las medidas de investigación tradicionales dotándolas de la ayuda necesaria para combatir y detener a los ciberterroristas, ya que detrás de cada IP. se encuentra un individuo ,que tras ser identificado como amenaza ciberterrorista por sus actos, debe ser una máxima no solo su localización sino su detención y puesto a disposición judicial, de nada sirve poner medidas de detección si no llegamos a la raíz del problema, este alumno ha podido observar la dispersión en materia legislativa , alejado de un criterio único, en algo tan esencial como la definición de ciberterrorismo, provocando en este primer paso una brecha que es aprovechada por estos sujetos y grupos Terrorista para evadir ciertas acciones sobre ellos , protegiéndose en países de laxa legislación penal y en algunas ocasiones en connivencia con ciertos Estados, difuminando así la responsabilidad de Gobiernos en ataques de ciberespionaje, por lo que a Juicio de este alumno un Tribunal Internacional especializado en esta materia, de carácter independiente, debería juzgar ciertas acciones consideradas como ciberterroristas.

La globalización de la tecnología ha producido como ya sabemos las barreras físicas, por lo que en el mundo actual las acciones ciberterroristas extienden sus actos en el campo virtual

que complementa con acciones terroristas físicas, la dependencia a las nuevas tecnologías, fomenta como cualquiera de nosotros podemos ser víctima de una acción cibernética, a pesar del gran problema que representa esta sensación de seguridad subjetiva , sin ser alarmistas, las Agencias Oficiales como la Policía, la Gc o el CNI, realizando una labor encomiable al carácter de todo el respaldo tanto material como burocrático para combatir de manera más rápida a los ciberterroristas, por lo que a criterio de este alumno sería necesario una Unidad específica que englobe a todos los Organismos con competencia en ciberterrorismo para la unificación de criterios y con unos niveles de acceso más rápido y solventes que los agentes encargados de combatir la ciberdelincuencia, si bien es cierto que algunos Jueces ya trabajan de manera rápida en la concesión de medidas restrictivas de derechos en forma de Autos, es necesario una resolución mucho más ágil y rápida, al depender el resultado de estas medidas de la captura o no del ciberterrorista.

Queda mucho margen de mejora para poder combatirlo, siendo necesario mejoras para concienciación de todos los usuarios de la red por ser cualquier equipo, teléfono móvil o sistema electrónico la vía de entrada a nuestro espacio por lo que todo parece llevarnos a pensar que todos somos corresponsables de nuestra propia Seguridad como de la seguridad cibernética mundial.

8 REFERENCIAS BIBLIOGRÁFICAS

Beltrán, J. I. (15 de 09 de 2015). *Universidad Politécnica de Valencia*. Obtenido de https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

Centeno, U. (Septiembre de 2015). *WWW.IEEE.ES*. Recuperado el 15 de abril de 2019, de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Centro Criptológico Nacional. (2019). *https://www.ccn.cni.es*. Recuperado el 5 de mayo de 2019, de https://www.ccn.cni.es/index.php/es/menu-ccn-es/funciones-del-ccn

CCN. (Noviembre de 2017). *https://www.ccn-cert.cni.es*. Recuperado el 5 de abril de 2019, de https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5362-el-2017-acabara-con-mas-de-26-500-ciberincidentes-en-el-sector-publico-y-empresas-estrategicas-espanolas-un-26-mas-que-el-ano-pasado.html

DSN. (Diciembre de 2017). *Estrategia de Seguridad Nacional*. Recuperado el 20 de Mayo de 2019, de https://www.dsn.gob.e: https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

Future Trends Forum. (s.f.). *http://www.ticpymes.es*. Recuperado el 2019 de Mayo de 16, de /tecnologia/noticias/1089353049504/diez-propuestas-future-trends-forum.1.html

https://www.ccn.cni.es. (03 de mayo de 2019). *https://www.ccn.cni.es*. Obtenido de https://www.ccn.cni.es/index.php/es/menu-ccn-es/funciones-del-ccn

https://www.kaspersky.es/resource-center/threats/botnet-attacks. (2019). Recuperado el 1 de junio de 2019

kaspersky. (2019). *https://www.kaspersky*. Recuperado el 20 de abril de 2019, de https://www.kaspersky.es/resource-center/threats/spyware

Navarro Bonilla, D. (2009). *Tres mil años de informacion y secreto*. Plaza y Valdés.

Organizacion de Naciones Unidas. (24 de septiembre de 2014). Resolucion 2178 (Aprobado por el Consejo de Seguridad en sesion 7272). Obtenido de https://www.un.org/sc/ctc/wp-content/uploads/2015/06/N1454802_ES.pdf

Urueña Centeno, F. (Septiembre de 2015). *www.ieee.es*. Recuperado el 20 de mayo de 2019, de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

9 GLOSARIO DE TÉRMINOS

APT (*Advanced Persitent Threat* o Amenaza Persistente Avanzada) / AVT (*Advanced Volatility Threat*): Este concepto se define como ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Ataque por diccionario: Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres alfanuméricos, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

BOT dañino: Una *botnet* es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un BOT es una pieza de software maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los *bots* y que ejecuten las órdenes dictadas remotamente.

Ciberamenaza: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. ν Taxonomía: Clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

Ciberespacio: Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

Ciberincidente: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

Ciberseguridad: Parte de la seguridad que se ocupa de los delitos cometidos en el ciberespacio y la prevención de estos.

Descifrado de contraseña: Proceso de transformar una contraseña protegida por contraseña, en una contraseña en texto claro y legible.

Dominios DGA: Procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y control, técnica usada en redes *Botnet* para dificultar su detención. ν Criptografía: Técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

DoS (*Denial of Service*) o ataque de denegación de servicio: Consiste en una serie de técnicas que provocan la inoperatividad de un servicio o un recurso. El procedimiento consiste en la implementación masiva de peticiones a un servidor, lo que genera una sobrecarga del servicio y el posterior colapso del mismo al no poder éste atender la gran cantidad de solicitudes que le llegan.

Gestión de ciberincidentes: todos los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

Gusano: *Malware* similar a un virus, y en ocasiones se considera una subclasificación de este. Exactamente igual que un virus, un gusano se difunde de ordenador a ordenador. La principal característica que distingue a un gusano de un virus es el hecho de que el gusano tiene la capacidad de diseminarse sin la necesidad de una acción humana. Un gusano normalmente explota vulnerabilidades del Sistema Operativo o de contraseñas débiles para diseminarse a otros ordenadores.

***Malware* (código dañino)**: La palabra malware deriva de los términos *malicious y software*. Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como programa maligno. Es un término que engloba varios tipos de programas dañinos.

PROXY: Ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera trasparente para el usuario.

Ransomware: *Malware* que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

Robo de credenciales de acceso: Acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.

Rootkit: Es un conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por máquina se entiende todo el espectro de sistemas IT, desde *smartphones* hasta ICS. El propósito por tanto de un *rootkit* es enmascarar eficazmente *payloads* y permitir su existencia en el sistema.

***Scanning* (escaneo de puertos)**: Análisis local o remoto mediante software, del estado de los puertos de una máquina conectada a una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

***Scanning* (escaneo de red):** Análisis local o remoto mediante software, del estado de una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

***Sniffing* (análisis de paquetes):** Análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y usado para detectar y analizar posibles vulnerabilidades.: Consiste en la suplantación de la identidad mediante la que el atacante, de forma masiva, trata de obtener información relevante de usuarios para uso dañino. Para ello se emplean métodos de ingeniería social.

Spam: Correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

***Spyware* (programa espía):** *Malware* que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir *keyloggers*, monitorizaciones, recolección de datos, así como robo de datos. Los *spyware* se pueden difundir como un troyano o mediante explotación de software.

Telnet: Protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

Troyano: *Malware* que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el software dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la capacidad de replicarse, no obstante, puede tener gran

capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de software.

Virus: *Malware* cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro.