universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2020/2021

EL CASO STUXNET. ESPECIAL ATENCIÓN A LOS DESAFÍOS Y LAS CONDUCTAS QUE SE PRESENTAN EN LOS CIBERDELITOS

(*THE STUXNET CASE. FOCUS ON THE CHALLENGES AND BEHAVIOURS INVOLVED IN CYBERCRIME*)

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTORA: DÑA. AINHOA NAVA DELGADO

TUTOR: D. MIGUEL DÍAZ Y GARCÍA CONLLEDO

COTUTORA: DÑA. MARÍA ANUNCIACIÓN TRAPERO BARREALES

ÍNDICE

ABREVIATURAS

AEDI	Anuario Español de Derecho Internacional (citado por número y año)
APT	*Advance Persistent Threat*
Art./s.	Artículo/s
CC	Código Civil
CCN	Centro Criptológico Nacional
CD	*Compact Disc*
CDJ	Cuadernos de Derecho Judicial (citada por número y año)
Cdo.	Considerando
CERT	*Computer Emergency Response Team*
CESEDEN	Centro Superior de Estudios de la Defensa Nacional
CIA	*Central Intelligence Agency*
CNRI	Consejo Nacional de Resistencia Iraní
Coord(s).	Coordinador(es)/a(s)
CP	Código Penal
CSNU	Consejo de Seguridad de la Naciones Unidas
CVE	*Common Vulnerabilities and Exposures*
DoS	*Denial of Service*
DPC	Derecho Penal y Criminología (citada por número y año)
DVD	*Digital Versatile Disc*

EE.UU.	Estados Unidos
ENISA	*European Union Agency for Network and Information Security*
GESI	Grupo de Estudios en Seguridad Internacional
I2P	*Invisible Internet Project*
IDP	Revista de Internet, Derecho y Política (citada por número y año)
INCIBE	Instituto Nacional de Ciberseguridad
IP	*Internet Protocol*
JCPOA	*Joint Comprehensive Plan of Action*
KB	*Kilobyte*
LOPJ	Ley Orgánica del Poder Judicial
Malware	*Malicious Software*
n.º	número
NFP	Nuevo Foro Penal (citada por número y año)
NSA	*National Security Agency*
NTI	*Nuclear Threat Initiative*
NVD	*National Vulnerability Database*
OCDE	Organización para la Cooperación y el Desarrollo Económico
OIEA	Organismo Internacional de Energía Atómica
ONU	Organización de las Naciones Unidas
OVAL	*Open Vulnerability and Assessment Language*

p. ej.	por ejemplo
PLC	*Programmable Logic Controller*
RAE	Real Academia Española
RECPC	Revista Electrónica de Ciencia Penal y Criminología (citada por número y año)
REDUR	Revista Electrónica de Derecho de la Universidad de La Rioja (citada por número y año)
REEI	Revista Electrónica de Estudios Internacionales (citada por número y año)
RPC	*Remote Procedure Call*
s(s).	siguiente(s)
SCADA	*Supervisory Control and Data Acquisition*
TIC´s	Tecnologías de la Información y la Comunicación
TNP	Tratado de No Proliferación Nuclear
TNRC	*Teheran Nuclear Research Center*
TOR	*The Onion Router*
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
USB	*Universal Serial Bus*
Vol.	Volumen
VVAA	Varios autores

RESUMEN

El caso de Stuxnet está considerado como el primer caso en el que una ciberarma causa daños en el mundo físico. En 2010 las centrifugadoras para el enriquecimiento de uranio de la central de Natanz, Irán, comienzan a presentar fallos con graves consecuencias. Tras el exhaustivo análisis de expertos en la materia, se llega a la conclusión de que los PLC que dirigían las centrifugadoras fueron *hackeados*.

Atendiendo a la situación geopolítica y, las tensiones que existían (y sigue habiendo) entre Irán y EE.UU. e Israel, se señaló a estos últimos como los supuestos autores y creadores de Stuxnet. Incluso se llegó a publicar un artículo en *The New York Times* que tuvo tal repercusión apoyando esa autoría conjunta, que los tribunales americanos iniciaron una investigación.

A la hora de valorar de forma jurídico-penal este caso, se pone de manifiesto los desafíos que presentan los ciberdelitos; en concreto su calificación jurídica. Es así como Stuxnet puede, *a priori*, encajar en conductas como el *hacking*, *cracking*, o incluso términos como ciberguerra o ciberterrorismo. Para ello, conviene partir de la reciente idea de ciberdelito y su clasificación.

PALABRAS CLAVE

Anonimato, APT, centrifugadora, ciberataque, ciberdelitos, ciberguerra, ciberterrorismo, clasificación, *cracking*, datos, extraterritorialidad, *hacking*, infraestructura crítica, nuclear, PLC, programa, Stuxnet, territorialidad, TNP y vulnerabilidades.

ABSTRACT

The Stuxnet case is the first case in which a cyber-weapon causes damage in the physical world. In 2010, the uranium enrichment centrifuges at the Natanz plant in Iran began to fail, with serious consequences. After exhaustive analysis by experts in the field, it is concluded that the PLCs running the centrifuges were hacked.

Given the geopolitical situation and the tensions that existed (and still exist) between Iran and the US and Israel, the latter were identified as the alleged authors and creators of Stuxnet. An article was even published in The New York Times that had such an impact supporting this joint authorship that the American courts launched an investigation.

A criminal law assessment of this case highlights the challenges presented by cybercrime, in particular its legal qualification. Thus, Stuxnet can, a priori, fit in with behaviours such as hacking, cracking, or even terms such as cyberwar or cyberterrorism. To do so, it is worth starting with the recent idea of cybercrime and its classification.

KEYWORDS

Anonymity, APT, centrifuge, cyberattack, cybercrime, cyberwar, cyberterrorism, classification, cracking, data, extraterritoriality, hacking, critical infrastructure, nuclear, PLC, program, Stuxnet, territoriality, NPT, and vulnerabilities.

OBJETO DEL TRABAJO

El punto central de este trabajo es realizar un análisis jurídico-penal sobre el caso Stuxnet y la dificultad de categorizar los ciberdelitos. Para ello se ha divido en dos partes:

En primer lugar, se ha procedido a una breve contextualización del *malware* conocido como Stuxnet, comenzando por un breve análisis de la situación geopolítica existente en esos momentos, la incertidumbre de por qué fallaban esas centrifugadoras para el enriquecimiento de uranio y la justificación que ofreció *The New York Times* como una posible coautoría de EE.UU e Israel.

En segundo lugar, se analizan los desafíos de los ciberdelitos y se ofrece una posible calificación jurídica penal del caso.

Sobre los desafíos, se parte de que no existe una definición comúnmente aceptada de ciberdelito y mucho menos una clasificación, realmente el término de ciberdelito es algo actual. Se expone como el gran manto del anonimato que proporciona Internet es una ventaja para los ciberdelincuentes. Para llegar a los problemas de territorialidad que supone encontrarnos en un mundo globalizado.

Todo ello para llegar a las posibles conductas típicas que encajarían con Stuxnet, algunas concretas como el *hacking* o el *cracking*, y otras ofreciendo conceptos más amplios como ciberguerra o ciberterrorismo. Para concluir con la posible atribución de competencia a los juzgados españoles.

METODOLOGÍA

El estudio de este trabajo se mueve en un ámbito jurídico-penal. Confluyen en él el análisis dogmático y las consideraciones de política criminal; sigo, por tanto, el método iniciado por el Prof. ROXÍN en Alemania hace ya varias décadas, adoptado por la doctrina española.

La elaboración de este trabajo comenzó con la elección del tutor, D. Miguel Díaz y García Conlledo, Catedrático del Área de Derecho penal de esta Universidad, con quien tras comentar la posibilidad de tratar el caso Stuxnet, accedió a trabajar sobre ello. Al llegar a este punto, mi tutor decidió contar con la colaboración como cotutora de Dña. María Anunciación Trapero Barreales, Catedrática del Área de Derecho penal.

El estudio de la primera parte se ha llevado a cabo a través de la lectura de numerosos artículos de expertos informáticos (explicación fáctica del caso Stuxnet), además de algunos manuales en los que se trataba este tema. Razón por la cual, esta primera parte presenta tantos enlaces *web*. La segunda parte se centra en la lectura de artículos de revistas jurídicas, monografías y manuales que tratan los ciberdelitos.

El sistema de citas utilizado corresponde a las directrices dadas por mis cotutores, siguiendo el resto de las indicaciones y correcciones por ellos efectuadas.

I. PANORÁMICA DEL PROBLEMA

1. POSIBLES SUJETOS ACTIVOS Y SUJETO PASIVO. SITUACIÓN GEOPOLÍTICA

«Para los padres del concepto clásico de geopolítica […], el Estado es un ser vivo que, como tal, necesita alimentarse para sobrevivir y crecer»[1]. Con esta idea se abre paso a un breve análisis de la situación previa que motivó el ciberataque de Stuxnet.

Se sabe que las grandes potencias mundiales[2] han tratado de hacerse con el petróleo de Irán. Un ejemplo es la operación TP-AJAX[3] que culmina, con la ayuda de EEUU, con la proclamación de MOHAMMAD REZA PAHLEVÍ[4] como *sha* de Irán. Durante este régimen (1941-1979) se puede hablar de una fructuosa relación[5] entre EEUU e Irán. Cual títere, este monarca adoptó una serie de medidas, denominadas «revolución blanca»[6], creando claros «sentimientos antioccidentales»[7] en la población. Estas medidas afectaban de forma negativa «al clero y a la disidencia política, pero no a los terratenientes ni al Ejército. […] Junto a [este] macroproyecto […], se encontraba la educación y la igualdad de sexos. Esta modernización, [estaba] alejada de la doctrina restrictiva en la interpretación del islam y herética para los conservadores religiosos, [todo ello con la finalidad de] que la clase media [fuera] la que podía controlar el país»[8].

En el ámbito geográfico se desarrollan una serie de acontecimientos, en concreto guerras, que generan unas fuertes tensiones en Oriente Medio. En particular, se desencadenan tres conflictos[9] que sellarán las relaciones entre Irán e Israel.

---

[1] BAÑOS BAJO, *Así se domina el mundo*, 2017, 18.

[2] Así p. ej., en el momento de producirse los hechos que van a ser explicados en el texto, Reino Unido (con la compañía *Anglo Iranian Oil Company*), EEUU y la antigua Unión Soviética. Siendo las dos primeras las que podían ejercer mayor influencia.

[3] El significado de esta abreviación: «"TP" era el prefijo de país de la CIA para Irán, mientras que "AJAX" parece, de manera bastante prosaica, haber sido una referencia al popular limpiador de hogares, lo que implica que la operación limpiaría Irán de la influencia comunista». Así WILFORD, *The CIA´s secret Arabist and the shaping of the modern middle east*, 2013, 164.

[4] Accesible en: https://www.iranchamber.com/history/coup53/coup53p1.php (visitada el 23/04/2021).

[5] Accesible en: https://www.bbc.com/mundo/noticias-internacional-48759280 (visitada el 14/04/2021).

[6] BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 8.

[7] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 5.

[8] YUSTE GONZÁLEZ, *Historia Rei Militaris: Historia militar, política y social*, n.º 7, 2014, 117.

[9] La crisis del Canal de Suez, la guerra de los seis días y la guerra de Yom Kipur, como señala GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 6.

Durante el régimen de REZA PAHLEVÍ, en 1957, surge el programa nuclear iraní junto con el TNRC, impulsado por el apoyo tecnológico estadounidense, bajo el programa *Atoms for Peace* de EISENHOWER[10]. Como señaló el gobierno iraní públicamente, el desarrollo de esta energía se haría con fines civiles y pacíficos.

Irán firma el Tratado sobre la No Proliferación de las armas nucleares, en el marco de la ONU, en 1968 y lo ratifica en 1970. La ONU señala que «es un tratado internacional clave cuyo objetivo es prevenir la propagación de las armas nucleares y la tecnología armamentística, promover la cooperación en la utilización de la energía nuclear con fines pacíficos e impulsar el objetivo de lograr el desarme nuclear y el desarme general y completo. El TNP es el único tratado multilateral que representa un compromiso vinculante para los Estados poseedores de armas nucleares respecto del objetivo del desarme»[11].

Tras varios años de conflictos y movilizaciones[12] en 1979 se derroca al *sha* PAHLEVÍ y se impone una república islámica bajo el mandato del Ayatolá JOMEINI, quien con ayuda del Hezbollah aumentó desmesuradamente la tensión y los conflictos, especialmente con EEUU e Israel[13].

Se realiza un alto en el programa nuclear iraní, por la ruptura de las (aparentes) relaciones con el gigante americano. Sin embargo, el programa se retoma en 1985, esta vez con el apoyo de Pakistán, China y, por supuesto, Rusia en mayor medida[14]. Por todo ello «el programa nuclear evoluciona significativamente durante esta década [90s] y aumentan las preocupaciones por parte de los estados que estaban en contra»[15]. A fin de paliar esta tensión, se firman los acuerdos de Oslo en 1993 para limitar la cooperación

[10] Accesible en: https://www.nti.org/learn/countries/iran/nuclear/ (visitada 22/04/2021).

[11] Accesible en: https://www.un.org/es/conferences/npt2020/background (visitada el 11/06/2021).

[12] Se ha de tener en cuenta los actos que reivindicaron el odio por el gigante americano, y en definitiva por el sha, que provocaron su derrocamiento en 1979. Entre ellos: el asalto que sufrió la embajada norteamericana en Irán donde secuestraron y retuvieron a ciudadanos estadounidenses, llegando este asunto a la Corte Internacional de Justicia; o el regreso de Jomeini, quien lideró las revoluciones religiosas que azotaron el interior de Irán. BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 9 y ss.

[13] Ante esta tensión, cabe mencionar la doctrina Begin acuñada por Israel, donde declaraba que no permitiría el desarrollo armamentístico nuclear de un país catalogado como enemigo. GARRIDO REBOLLEDO, *REEI*, n.º 12, 2006, 3; BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 7 y ss.

[14] En más detalle: BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 14-16.

[15] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 10.

con Irán[16]. Pese a ello, Irán sigue avanzado, de forma sobresaliente[17], en armamento nuclear[18].

No es hasta el 14 de agosto de 2002 que, desde dentro de Irán, el CNRI[19] da la voz de alarma sobre la construcción de una planta de enriquecimiento de uranio bajo tierra, en Natanz, y una planta de producción de agua pesada[20] en Arak[21], junto con «los nombres de varias personas y compañías que participan en el programa nuclear»[22]. Todos estos datos no habían sido declarados a la OIEA constituyendo una violación de los Acuerdos de los 90s firmados en Oslo; ante esto Irán declaró que realizaba «*new facilities as part of its program to develop a nuclear cycle*»[23].

El periodo de 2003 a 2009 va a verse marcado por las grandes hostilidades entre los países[24]. Con el fin de evitar al CSNU, Irán accede a negociar con el grupo UE-3 (Reino Unido, Alemania y Francia)[25] aceptando «suspender las actividades de enriquecimiento y reprocesado»[26], aunque siguió realizando dichas actividades valiéndose de ambigüedades en ciertos términos.

En 2004 se celebra el Acuerdo de París con la UE-3, a fin de evitar las nuevas sanciones que amenazaban con imponerse a Irán[27]. Sin embargo, durante la presidencia de MAHMUD AHMADINEYAD (2005-2013), quien mantenía una notoria aversión por Israel[28], se retoman estas actividades nucleares[29].

---

[16] Con más detalle en: https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/#geopolitico (visitada el 21/04/2021).

[17] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 77.

[18] Así, p. ej., se observa esta circular informativa disponible en: https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/#geopolitico (visitada el 14/04/2021).

[19] BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 16.

[20] Informe de la NTI sobre la planta de producción de agua pesada: https://www.nti.org/learn/facilities/175/ (visitada el 24/04/2021).

[21] GARRIDO REBOLLEDO, *REEI*, n.º 12, 2006, 6.

[22] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 11.

[23] BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 16.

[24] Recuérdese la invasión de Irak motivada por los atentados de las torres gemelas o la invasión del Líbano debida a la guerra Israel-Hezbollah.

[25] Accesible en: https://www.nti.org/learn/countries/iran/nuclear/ (visitada el 22/04/2021).

[26] JONSSON, *Cuadernos de Estrategia*, n.º137, 2007, 184.

[27] GARRIDO REBOLLEDO, *REEI*, n.º 12, 2006, 8.

[28] Recuérdese la doctrina Begin, expuesta *ut supra.* BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 12.

[29] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 12.

En 2005 el presidente BUSH firma la orden presidencial 13382, «que bloquea los activos financieros de las personas y entidades que apoyan las armas de destrucción masiva»[30].

En junio de 2006, el P5+1[31] negocia la posibilidad de intercambiar tecnología nuclear civil por el cese de la actividad nuclear armamentística; Irán responde enviando una carta a BUSH[32] a modo desafiante, sin pronunciarse apenas sobre la energía nuclear. A raíz de esto, comienza una serie de resoluciones[33] que emite el CSNU que Irán ignora completamente[34].

En 2008, AHMADINEYAD «desafiando abiertamente a occidente, [demostró] al mundo su capacidad de enriquecer uranio»[35].

En 2009 Irán accede a unas inspecciones de la OIEA, donde se revela la potencia nuclear del país[36]. Para más *inri*, AHMADINEJAD incita con sus palabras a crear más instalaciones nucleares; a lo que responde el primer ministro de Israel, BENJAMÍN NETANYAHU[37], declarando tener las armas necesarias para atacar dichas infraestructuras secretas y un posible apoyo de EEUU, mientras que el resto de los Estados firmantes del TNP no se inmiscuyen[38].

[30] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 12.

[31] El P5+1 hace referencia a EEUU, Rusia, China, Reino Unido y Francia, además de Alemania.

[32] Para más detalles de la carta, accesible en: https://www.researchgate.net/publication/253212482_The_Iranian_Letter_to_President_Bush_Analysis_and_Recommendations (visitada 23/04/2021).

[33] Resoluciones accesibles en: https://www.iaea.org/publications/documents/infcircs?field_infcirc_number_value=&field_infcirc_date_value%5Bvalue%5D%5Bdate%5D=&field_infcirc_country_tid%5B%5D=311 (visitada el 15/06/2021).

[34] El propio Ahmadineyad prometió ignorar las resoluciones y continuar con el enriquecimiento. Accesible en: https://www.nytimes.com/2007/01/22/world/middleeast/22iran.html (visitada el 17/08/2021).

[35] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 77.

[36] Accesible en: https://www.nti.org/learn/countries/iran/nuclear/ (visitada el 18/08/2021).

[37] Quien expuso públicamente: «De los informes iniciales ya podemos concluir que este acuerdo es un error histórico para el mundo. […] No se puede evitar un acuerdo cuando los negociadores están dispuestos a hacer cada vez más concesiones a quienes, incluso durante las conversaciones, siguen coreando: "Muerte a América". Sabíamos muy bien que el deseo de firmar un acuerdo era más fuerte que cualquier otra cosa, y por eso no nos comprometimos a impedir un acuerdo. Nos comprometimos a evitar que Irán adquiera armas nucleares, y este compromiso sigue en pie. Les digo a todos los líderes de Israel, es hora de dejar a un lado la política mezquina y unirse detrás de este problema más fatídico para el futuro y la seguridad del Estado de Israel». Accesible en: https://www.iranwatch.org/library/governments/israel/office-prime-minister/israeli-prime-minister-netanyahus-statement-iran-nuclear-deal (visitada el 15/06/2021).

[38] BERMEJO GARCÍA/GUTIÉRREZ ESPADA, *AEDI*, n.º 31, 2015, 61-63.

Claramente EEUU no podía permitir esta actividad que vulnera el TNP, e Israel tampoco, ya que sería uno de los primeros objetivos de dicha tecnología. No sería descabellado pensar que ambos países unieron fuerzas[39] en pos del proverbio árabe «el enemigo de mi enemigo es mi amigo». «En consecuencia, el ciberataque Stuxnet va a ser la alternativa para buscar reducir la amenaza del desarrollo del programa nuclear [iraní]»[40].

En este periodo se desarrolla Stuxnet, como se explicará en adelante. Sin embargo, se ha de tener en cuenta que el programa nuclear iraní sigue siendo una gran amenaza en la actualidad; en 2020 se ha declarado que «Irán ha excedido los límites de enriquecimiento de uranio acordados en el JCPOA[41] [firmado el 14 de julio de 2015]»[42].

Se ha de tener en cuenta, en este contexto previo, que Israel se planteó bombardear la central de Natanz, pero EEUU le persuadió para no hacerlo[43] alegando que esto tendría unos efectos, probablemente, más devastadores que el propio problema[44]; sin contar con las dificultades estratégicas que rodeaban la planta[45]. Es así como se llega a la conclusión de llevar a cabo alguna acción donde el beneficio que se obtenga con el resultado sea superior al despliegue de los medios para llevarlo a cabo[46].

Ninguno de estos Estados ha reconocido de forma oficial su participación en este ciberataque.

2. INFRAESTRUCTURAS CRÍTICAS EN GENERAL, PLC EN PARTICULAR

Durante las tensiones diplomáticas (2002-2009) empiezan a darse fallos en la infraestructura de Natanz. Según detalla el informe del experto en ciberseguridad RALPH LANGNER que se expondrá a lo largo del trabajo, Stuxnet realmente actuó antes de lo que

[39] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 77.

[40] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 14.

[41] Acuerdo firmado en el 2015 por los miembros permanentes del CSNU, Alemania, UE e Irán para que este redujera la producción de material nuclear.

[42] Para el seguimiento actual de los problemas nucleares de Irán: https://www.nti.org/learn/countries/iran/nuclear/ (22/04/2021).

[43] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 78.

[44] Para una exposición detallada de estos motivos, FARWELL/ROHOZINSKI, *Survival*, vol. 53, 2011, 27-32.

[45] La distancia, profundidad bajo tierra, la línea defensiva antiaérea. Mas detalle en RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 77-78.

[46] GÓMEZ LLINÁS, *Stuxnet el virus informático*, 2017, 16.

se piensa. Sin perjuicio de explicar esto más adelante, ahora se expondrán los elementos afectados por Stuxnet.

Lo más conocido públicamente es que este *malware* afectó a las centrifugadoras de gas utilizadas para el enriquecimiento de uranio (ANEXO I). Sin embargo, hay que concretarlo, puesto que estas se encontraban en una infraestructura crítica, y, a lo que realmente atacaba Stuxnet, era a los PLC.

En primer lugar, la Directiva 2008/114/CE define las **infraestructuras críticas** como «el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones»[47]. Aplicado a este caso concreto, las centrales nucleares se entenderían arropadas bajo esta definición, pues se entienden incluidas en el sector de la energía[48].

En segundo lugar, de forma específica ambas versiones de Stuxnet atacaban los **PLC**, perturbando la velocidad y la presión. Por PLC se entiende un autómata programable, es decir, «una máquina industrial susceptible de ser programada al estar basada en un sistema de microprocesador dotado de un hardware estándar independiente del proceso a controlar»[49]. En otras palabras, son máquinas que se colocan en las centrifugadoras para que les dé instrucciones en su forma de trabajo automatizado.

Como señala LANGNER en su informe[50], los dos puntos débiles de estas centrifugadoras, que aprovecharon ambas versiones de Stuxnet, son:

- Las válvulas de presión, controladas por el PLC Siemens S7-417.

[47] Esta definición se formula en el art. 2 a); en el art. 2 b) se ofrece la definición de infraestructura crítica europea: la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructura.

[48] El cdo. 9 de esta directiva señala: «Por lo que se refiere al sector energético […], se sobreentiende que, toda vez que se estime oportuno, podrán incluirse en la generación de energía eléctrica las partes de transmisión eléctrica de las centrales nucleares».

[49] En JIMÉNEZ MACÍAS, *Técnicas de automatización avanzadas en procesos industriales*, 2004, 27.

[50] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada el 05/09/2021).

- Los rotores de las centrifugadoras, el PLC Siemens S7-315 controlaba la velocidad.

Conviene mencionar que el diseño de la central disponía de un sistema de protección en cascada, implementado «con la intención de tener maneras de aislar centrífugas individualmente cuando presentaran inconvenientes e incluso permitir cambiarlas sin detener el proceso productivo»[51].

3. ACCESO A LA RED: APT Y VULNERABILIDADES *ZERO DAYS*. PROPAGACIÓN Y CONSECUENCIAS

En 2008 varias de las centrifugadoras en la planta nuclear presentaron una serie de fallos, dejaron de funcionar. El personal iraní lo achacaba a la baja calidad de los materiales pakistaníes con las que estaban hechas. «Aunque los iraníes en ese momento no lo sabían, eran víctimas de *Stuxnet*»[52]. Sin embargo, este *malware* tiene un precedente, denominado Stuxnet 0.5 por RIVADENEIRA, que inutilizaba completamente las centrifugadoras. Esta versión no fue descubierta.

No es hasta el 24 de junio de 2010 que se descubre el malware en los ordenadores iraníes, en una revisión realizada por la empresa bielorrusa VirusBlokAda, haciéndose público este hecho el 17 de julio de 2010[53].

A raíz de ello, numerosos expertos e investigadores[54] comienzan a analizarlo, p. ej. Symantec[55] tardó algo más de tres meses para descifrar las claves de Stuxnet (lo habitual en ellos era un periodo entre 5-20 minutos). En un primer vistazo, se descubrió que el virus ocupaba 500 KB (cuando lo normal eran 10-15 KB); y, seguidamente, en un análisis más profundo, se reconoció: 1) que afectaba a objetivos concretos, 2) estaba

[51] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 78.
[52] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 76.
[53] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 80.
[54] Entre ellos: la empresa VirusBlokAda, el informe del experto Ralph Langner, la compañía de seguridad Kaspersky Lab. Accesible en: https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/ (visitada el 18/08/2021).
[55] Una empresa líder en ciberseguridad.

configurado de una forma muy particular, y 3) aprovechaba cuatro vulnerabilidades día-cero[56] (entre otras cosas).

Más tarde se fracciona Stuxnet para precisar su objetivo, la infraestructura crítica de Natanz (sin perjuicio de que afectara, de forma colateral o como maniobra de distracción, a otros equipos[57]). «Por primera vez en la historia se había descubierto una ciberarma»[58].

Se parte de la existencia de una o dos acciones (que se analizarán en el punto correspondiente): Stuxnet 0.5 y Stuxnet, dirigidas a los mismos objetivos, pero con resultados diferentes.

Stuxnet, en general, es un gusano informático, un *worn*, que busca reproducirse rápidamente para afectar a un mayor número de equipos. En concreto, se puede hablar de amenaza persistente avanzada, concepto que comenzó a utilizarse tras una publicación del *New York Times* sobre el ataque de una unidad militar china (APT1)[59].

En primer lugar, las **APT** son amenazas dirigidas contra un objetivo concreto y bien delimitado, además de ir acompañadas de una tecnología sofisticada para evitar, principalmente, ser detectada, por ello se dice que están patrocinadas por Estados[60]. Concretamente, la taxonomía de los ciberincidentes cataloga las APT 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»[61].

[56] Accesible en: https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/ (visitada el 24/04/2021).

[57] Según INCIBE: Indonesia, India o el propio EEUU. Accesible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf (visitada el 18/08/2021).

[58] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 80.

[59] Accesible en: https://www.kaspersky.es/blog/que-es-una-apt/966/ (visitada 27/04/2021).

[60] Accesible en: https://www.kaspersky.es/blog/que-es-una-apt/966/ (visitada 27/04/2021).

[61] La taxonomía está recopilada en INCIBE-CERT, *Guía nacional de notificación y gestión de ciberincidentes*, 2020, 17. Accesible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf (visitada el 27/04/2021).

INCIBE señala como métodos de infección de estas APT[62]:

- La ingeniería social, bien a través de *malware* procedente de internet (*phishing*, *software* pirata, entre otros), o bien a través de medios físicos (USB, CD, DVD, entre otros).
- *WebKits/Exploit*, herramientas que intentan aprovecharse de vulnerabilidades.

De acuerdo con los criterios de determinación del nivel de peligrosidad de un ciberincidente, las APT encabezan la lista con el nivel más crítico[63].

En segundo lugar, las **vulnerabilidades** son un «error en un programa o un fallo en la configuración que puede permitir a un atacante obtener acceso no autorizado al sistema»[64]; en concreto, las ***zero days*** «son aquellas vulnerabilidades en sistemas o programas informáticos que son conocidas por determinados atacantes, pero no lo son por los fabricantes o por los usuarios. Son las más peligrosas ya que un atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable»[65]. Lo principal de estas es que son poco comunes y con un desorbitado precio en el mercado negro[66].

[62] Para más detalle de las vías de infección, accesible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf (visitada el 25/04/2021).

[63] INCIBE-CERT, *Guía nacional de notificación y gestión de ciberincidentes*, 2020, 19. Accesible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf (visitada el 27/04/2021).

[64] Accesible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html (visitada el 25/04/2021).

[65] Accesible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html (visitada el 25/04/2021).

[66] Sobre las conductas ilícitas en el mercado negro digital: REZA REYES, en NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 192 y ss.

ENISA señala una serie de bases de datos para catalogar estas vulnerabilidades (CVE, NVD y OVAL)[67].Teniendo en cuenta el catálogo estadounidense NVD, las vulnerabilidades que se aprovecharon[68] para este ciberataque son cuatro[69] (ANEXO II[70]).

Aplicando esta teoría al caso, ¿cómo pudieron acceder?

Stuxnet 0.5 solo podía ejecutar el *malware* «a través de un dispositivo USB, mediante la transferencia del archivo entre computadores o como adjunto por correo electrónico»[71] puesto que la infraestructura estaba desconectada de Internet. Alguien tuvo que abrir el archivo de forma manual, bien con un USB o bien con un portátil[72] dentro de la planta nuclear. Es probable que se aprovecharan de la existencia de trabajadores externos a la central[73].

La siguiente versión, «parece ser que perdieron el acceso directo a los sistemas de la central»[74], por eso utilizaron el mismo método de acceso manual, más probablemente mediante un USB[75].

Una vez infectados los equipos, las fases que sigue una APT son[76]:

- Recopilación de la información del objetivo.
- Inserción en la red inicial.
- Asegurar el envío de la información entre los equipos comprometidos y los que lanzaron la APT.

---

[67] Accesible en: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits#:~:text=Zero%2Dday%20vulnerabilities%20are%20vulnerabilities,to%20information%20regarding%20known%20vulnerabilities (visitada el 25/04/2021).

[68] Una de ellas relacionada con *Conficker*, un *worm* que se propagó en 2008.

[69] Señala RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 79; que «cada una de ellas podría tener en esos años un costo en el "mercado gris", supuestamente para agencias de inteligencia, fuerzas armadas y policías, de entre US $ 50.000 y US $ 150.000, duplicándose dicho costo en el "mercado negro" empleado por cibercriminales».

[70] En el anexo se incluye la gravedad de las vulnerabilidades, así como una breve descripción de ellas. Obtenido de: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Stuxnet&search_type=all (visitada el 25/04/2021).

[71] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 78.

[72] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021).

[73] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021).

[74] Accesible en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

[75] Accesible en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

[76] Accesible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf (visitada el 25/04/2021).

- Búsqueda de los datos más sensibles y necesarios.
- Extracción o alteración de dichos datos.

La primera versión de Stuxnet se servía de una vulnerabilidad *zero days* que le permitía controlar los cambios en los PLC en las centrifugadoras; estas disponían de tres válvulas principales (parar alimentación, descargar el uranio enriquecido o descargar el uranio empobrecido) y auxiliares (para monitorizar los procesos desde la sala de control)[77].

Una vez dentro, bien bajo mandato, bien de forma autónoma, el *malware* buscaba los PLC (Siemens S7-417). Si no encontraba su objetivo el virus no hacía nada, pero cuando lo encontraba se iniciaba el ataque *man in the middle*[78], es decir, podía captar las comunicaciones entre los PLC y la sala de control, de tal forma que alteraba los datos sin hacer saltar las alarmas[79]. Esto se lograba gracias a que Stuxnet grababa los datos del correcto funcionamiento y las reproducía en bucle, así parecía que las centrifugadoras funcionaban correctamente[80]. «De esta forma, cuando el sistema de control SCADA [desde la sala de control] pidiese las lecturas, el controlador devolvería las lecturas reproducidas de Stuxnet y ni los ingenieros ni los sistemas automáticos verían nada anormal»[81].

En el mundo físico, esto se tradujo en el aumento del gas de las centrifugadoras. Durante un correcto funcionamiento, las válvulas se abrirían para dejar salir ese exceso; bajo el dominio del *malware* no se abrían, la presión subía[82] y, en ese momento, el ciberataque **se detenía** en seco[83]. ¿Por qué?[84]. Está claro que, de haber destruido de forma simultánea todas las centrifugadoras de Natanz, solo se habría retrasado el programa

[77] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 78.

[78] INCIBE lo define como «ataque basado en interceptar la comunicación entre 2 o más interlocutores, pudiendo suplantar la identidad de uno u otro según lo requiera para ver la información y modificarla a su antojo, de tal forma que las respuestas recibidas en los extremos pueden estar dadas por el atacante y no por el interlocutor legítimo». Para más detalles: https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo (visitado el 26/04/2021).

[79] RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 78-79.

[80] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 27/04/2021).

[81] Accesible en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

[82] Si la presión pasa cierto límite la instalación explota.

[83] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021); RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 79.

[84] Algunas hipótesis son que carecían de los recursos suficientes para ir más allá, que el ciberataque cambió de mando, querían evitar la destrucción de la central, o que buscaban cierto reconocimiento al crear la primera ciberarma. Mencionadas en RIVADENEIRA, *Revista de Marina,* n.º 951, 2016, 79.

nuclear cerca de unos meses[85] y, teniendo en cuenta la capacidad iraní en ese momento, es probable que existiera una forma más eficaz de retrasar dicho programa: la segunda versión de Stuxnet[86].

No cabe duda de que, para la realización de este daño, «se requería una gran información de inteligencia previa y profundos conocimientos técnicos del funcionamiento del enriquecimiento de uranio iraní y sus sistemas de seguridad»[87].

La segunda versión se servía de cuatro vulnerabilidades *zero days*[88], las cuales atacaban a sistemas Windows, en concreto se dirigía a los sistemas SCADA, los cuales «están diseñados para la recopilación, control y vigilancia de datos en tiempo real de infraestructuras críticas»[89]. Sin embargo, este paquete delictivo no solo contenía estas vulnerabilidades, sino también: «dos certificados digitales robados, pertenecientes a las empresas REALTEK y JMicron, marcas conocidas y hasta ese momento confiables»[90].

Esta versión se propagaba mediante USB igual que la primera, pero se diferencia de aquella en que, además, utilizaba «una vulnerabilidad en el sistema RPC de Windows para infectar a los ordenadores de una misma red privada (conectados por un mismo *router*)»[91]. Esta forma de propagación se externalizó afectando a países como Pakistán, India, Azerbaiyán, o el propio EEUU.

Sin embargo, esta versión atacaba a los PLC (Siemens S7-315) que controlaban la velocidad de los rotores[92] (ANEXO III) en las centrifugadoras. De tal forma que aumentaba la velocidad de los rotores y la detenía, degradando el enriquecimiento de

[85] Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021).

[86] Accesible en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

[87] Opinión que comparto de RIVADENEIRA, *Revista* de Marina, n.º 951, 2016, 79.

[88] Una se usaba para propagarse por los USB, otra para propagarse por las impresoras de redes compartidas y las otras dos se dedicaban a la escala de privilegios (acceder a un equipo con un rol de usuario para poder llegar al rol de administrador). Accesible en: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (visitada el 28/04/2021).

[89] SHAKARIAN, *Air and Space Power Journal*, 2012, 50-51

[90] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 80. Se debe considerar que la obtención de estos certificados es extremadamente complicada, puesto que se encuentran en ordenadores sin conexión a internet y protegidos con altos niveles de seguridad, entre ellos la seguridad biométrica.

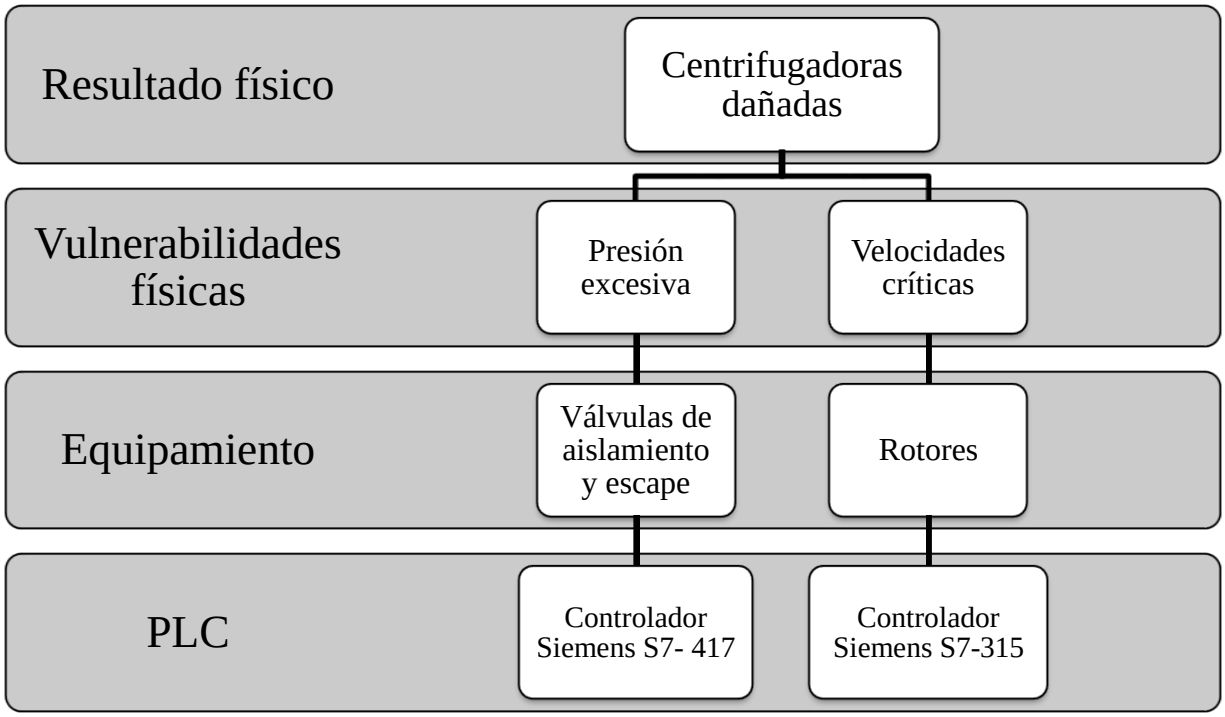
[91] Accesible en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

[92] La pieza que hace girar el uranio con la fuerza del motor.

uranio[93]. Se calcula que este proceso se repitió durante unos 30 días «en junio de 2009, marzo de 2010 y mayo de 2010»[94].

Pero, además, esta versión, de acuerdo con su formación, se dedicaba a «comunicarse con sus servidores de mando y control, enviar información encriptada, abrir puertas traseras y comprometer computadores en forma remota»[95], es decir, robaba información para detallar los progresos del programa nuclear iraní.

A modo de resumen, para el entendimiento visual de este ciberataque se expone el siguiente esquema[96]:



Pero ¿por qué Stuxnet tiene tanta notoriedad? Porque es la primera vez que un ataque desde el ciberespacio causa daños en el mundo físico[97], al menos es del que se tiene conocimiento y se ha publicado numerosa información.

[93] Para más detalles sobre este proceso: Accesible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021)

[94] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 80.

[95] RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 80.

[96] Información extraída en: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021) y en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 26/04/2021).

[97] Así se detalla en: RIVADENEIRA, *Revista de Marina*, n.º 951, 2016, 76; https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/ (visitada el 28/04/2021);

4. ALARMA MEDIÁTICA. PUBLICACIÓN DE LA OPERACIÓN *OLYMPIC GAMES*

Es más que conocido el poder que pueden llegar a ejercer los periódicos americanos en temas políticos, en concreto en su país. Un claro ejemplo es el caso de Stuxnet.

En junio de 2012, el corresponsal de Seguridad Nacional y de la Casa Blanca, DAVID SANGER, publica un artículo titulado: *Obama Order Sped Up Wave of Cyberattacks Against Iran*[98]. En él se expone las personas que, supuestamente, participaron y cómo llevaron a cabo Stuxnet. Todo ello conlleva a que los tribunales americanos inicien una investigación que se vio suspendida por falta de pruebas en 2015[99].

De forma bastante detallada, en este trabajo de investigación se habla sobre diferentes puntos, entre ellos los siguientes.

Desde el mandato de BUSH, agentes de la CIA introdujeron piezas dañadas en las centrales de Irán, pero estas apenas surtieron efecto. Entonces, en 2006, el general CARTWRIGHT diseñó un boceto de un posible ciberataque. Sin embargo, presentaba un gran problema: no conocían el modo de operar de las infraestructuras iranís. Como primer recurso, a regañadientes, el presiente autorizó la utilización de unas balizas para ir describiendo los avances. A continuación, contaron con la ayuda de la Unidad 8200 israelí[100]. Entonces, teniendo un plan más firme, EEUU se sirvió de unas centrifugadoras de gas (iguales a las de Irán) que MUAMAR EL GADAFI había abandonado en Tennessee para probar en ellas el virus.

El siguiente paso era introducirlo en Natanz, algo que se entiende fue de los puntos más difíciles de planear, puesto que tendrían que depender de ingenieros, trabajadores

https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet (visitadas el 28/04/2021).

[98] Accesible en: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (visitada el 28/04/2021).

[99] Accesible en: https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/ (visitada 28/04/2021).

[100] Considerada en aquel momento una de las mejores unidades especiales israelí en temas de inteligencia cibernética.

externos[101], pero uno de los confeccionadores del plan señaló: «*It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand*»[102].

Una vez iniciada Stuxnet, acabó el mandato de BUSH. En la reunión que tuvo con su sucesor OBAMA (antes de su toma de posesión), aquel le pidió que mantuviera dos operaciones: *Olympic Games* y el programa de drones de Pakistán.

Sin embargo, en 2010, el virus escapó de la central de Natanz, exponiendo al riesgo a otros países. En una reunión sobre este asunto, en la que estaban presentes el director de la CIA, PANETTA, OBAMA y BIDEN[103], esté señaló furioso: «*It's got to be the Israelis* […] *They went too far*»[104], es decir, que (supuestamente) las fuerzas israelís introdujeron un error en la programación para ir más allá en el daño. Ante esto el presidente OBAMA decretó que los ataques debían seguir, inutilizando unas 1.000 centrifugadoras desde que se hizo pública la existencia de Stuxnet en 2010.

En conclusión, este artículo establece la autoría de EEUU e Israel. Sin embargo, *The New York Time* no fue el único en afirmarlo, puesto que EDWARD SNOWDEN[105] afirmó: «*The NSA and Israel wrote Stuxnet together*»[106].

Cabe mencionar que, en la actualidad, el portavoz oficial de la OIEA ha expuesto que en 2020 ha tenido lugar una «explosión y un incendio en la nave de ensamblaje de centrifugadoras [de Natanz] que fue resultado de un sabotaje»[107], a la par que recordaba el incidente de Stuxnet de 2010 contra la misma central.

[101] Refiriéndose a los encargados de mantenimiento.

[102] Accesible en: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (visitada el 15/06/2021).

[103] En ese momento, OBAMA era presidente y BIDEN su vicepresidente.

[104] Señala *The New York Times.*

[105] Exsoldado y agente de la CIA, que se encuentra en una situación de asilo político por revelación de secretos de estado.

[106] Accesible en: https://www.scmp.com/news/world/article/1278286/nsa-israel-created-stuxnet-worm-together-attack-iran-says-snowden (visitada el 28/04/2021).

[107] Accesible en: https://escudodigital.com/ciberseguridad/el-ciberataque-de-israel-natanz-volvio-a-recurrir-al-gusano-stuxnet/?utm_source=mailpoet&utm_medium=email&utm_campaign=Newsletter+N%C2%BA81 (visitada el 28/04/2021).

II. MARCO JURÍDICO PENAL

1. DEFINICIÓN Y CLASIFICACIÓN DE LOS CIBERDELITOS

En España «ni el Código Penal de 1995 o sus sucesivas reformas han destinado un Título o rúbrica específica, descartando el establecimiento de un capítulo específico dedicado a los delitos informático[108] o de una norma común que facilite su adecuado tratamiento y sanción. Además, existe una importante dispersión normativa pues las distintas figuras están diseminadas a lo largo del articulado del Código[109].[…] No se considera, pues, que exista ningún vínculo común entre ellos»[110]. Es cierto que no existe una categoría penal, pero para algunos expertos existe un «ámbito de riesgo»[111].

Es cierto que las nuevas tecnologías han supuesto una gran ventaja, en ciertos sectores del día a día (comercial, social, etc). Pero, «junto a estas nuevas posibilidades han aparecido algunas conductas antijurídicas, que constituyen nuevas amenazas, y por ello la necesidad de tipificarlas, lo que ha dado lugar a los llamados delitos informáticos, que comprenden una gran variedad de acciones»[112].

Aquí se presenta el siguiente problema, al no existir acuerdo para establecer una definición de delitos informáticos o ciberdelitos, ni la propia doctrina encuentra un término consensuado[113].

Incluso hay autores que prescinden de la conceptualización, exponiendo únicamente las características[114]. Para SUBIJANA ZUNZUNEGUI son cuatro: «Se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan[115]; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de las lagunas de punibilidad que pueden existir en determinados

[108] ADÁN DEL RÍO, *Eguzkilore* n.º 20, 2006, 152-153.

[109] Entre otros, arts. 186, 197, 211, 238.5, 248.2 y 3, 256, 270, 286 CP.

[110] BARRIO ANDRÉS, *Delincuencia informática*, 2012, 37.

[111] COLÁS TURÉGANO, *Revista Boliviana de Derecho*, n.º 21, 2016, 212-214. También LOREDO GONZÁLEZ/RAMÍREZ GRANADOS, *Celerinet*, año 1-vol.2, 2013, 47.

[112] LUZ CLARA/GABRIEL MURAD, en NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 142.

[113] HERNÁNDEZ DÍAZ, *Eguzkilore* n.º 23, 2009, 228.

[114] Para FERREYROS SOTO, *Informática y derecho: Revista iberoamericana de derecho informático*, n.º 9-11, 1996, 409 y ss; algunas de estas especialidades son: el «rápido dinamismo de creación, desarrollo y evolución de productos y materiales, equipos y programas; […] aumento de la deslocalización de empresas y actividades ejercidos a escala planetaria […] La inmaterialidad del contenido de la información».

[115] Recuérdese el caso Stuxnet, como se consideró esta entre las ventajas de un ciberataque frente a un posible ataque en el mundo físico sobre Natanz.

Estados, algunos de los cuales ha sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas»[116].

A priori se ha de tener en cuenta la evolución que ha sufrido la terminología, desde los delitos informáticos, concepto utilizado entre los 80 y 90 del siglo pasado, hasta los ciberdelitos, utilizado en la actualidad[117].

Los delitos informáticos, en palabras de GONZÁLEZ RUS, se relacionan con una pluralidad de conductas que se dirigen contra el sistema informático y aquellas que se realizan por medio del sistema informático[118]. Sin embargo, esta terminología queda obsoleta puesto que «la pluralidad y diversidad de bienes jurídicos que pueden verse comprometidos, así como de medios comisivos […] apenas aportan en la actualidad una mínima precisión desde el punto de vista criminológico, dogmático, político-criminal y de política legislativa»[119].

Sobre ello ROMEO CASABONA expone que mientras que las conductas de los delitos informáticos se dirigen hacia los sistemas informáticos, los ciberdelitos «girarían en torno a redes telemáticas (abiertas, cerradas o de acceso restringido), siendo en estos casos los sistemas informáticos más instrumentales o secundarios para la comisión del delito»[120].

Sin embargo, en la actualidad hay autores[121] que se plantean la inexistencia de estos ciberdelitos, basando sus argumentos en que «no puede hablarse de un delito informático, sino de una pluralidad de delitos en los que nos encontramos, como única nota común, su vinculación de alguna manera con los ordenadores, pero ni el bien jurídico agredido es siempre de la misma naturaleza ni la forma de la comisión del hecho presenta

[116] SUBIJANA ZUNZUNEGUI, *Eguzkilore*, n.º 22, 2008, 171. En la misma línea: POSADA MAYA, *NFP*, n.º 88, 2017, 82-104; MARTÍNEZ, en VVAA, *Cibercrimen y delitos informáticos*, 2018, 30-32; TEMPERINI, en VVAA, *Cibercrimen y delitos informáticos*, 2018, 61-68; ROIBÓN, en VVAA, *Cibercrimen y delitos informáticos*, 2018, 132-133.

[117] Así lo explica MIRÓ LLINARES, *El cibercrimen*, 2012, 34-39. (Versión *online*).

[118] GONZÁLEZ RUS, RECPC, n.º 1, 1999. (Versión *online*).

[119] ROMEO CASABONA, en PÉREZ ÁLVAREZ/NÚÑEZ PAZ/GARCÍA ALFARAZ (coords.), *Universitas vitae: homenaje a Ruperto Núñez Barbero*, 2007, 655.

[120] ROMEO CASABONA, en PÉREZ ÁLVAREZ/NÚÑEZ PAZ/GARCÍA ALFARAZ (coords.), *Universitas vitae: homenaje a Ruperto Núñez Barbero*, 2007, 657.

[121] Entre ellos: ROMEO CASABONA, en PÉREZ ÁLVAREZ/NÚÑEZ PAZ/GARCÍA ALFARAZ (coords.), *Universitas vitae: homenaje a Ruperto Núñez Barbero*, 2007, 654 y ss; TÉLLEZ VALDÉS, *Derecho informático*, 4.ª, 2008, 188 y ss. (Versión *online*); BARRIO ANDRÉS, *Delincuencia informática*, 2012, 33 y ss.

siempre características semejantes»[122], además estos delitos se van actualizando conforme lo hacen las tecnologías, cambian a la misma velocidad.

En cambio, autores como DAVARA RODRÍGUEZ entienden estos delitos como «la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea *hardware* o *software*»[123]. Sin embargo, está argumentación interpretando en sentido estricto[124] el concepto, no aporta las características de una nueva categoría penal[125].

Teniendo esto en cuenta, algunas de estas definiciones son las siguientes. Para DAVARA RODRÍGUEZ, como se expuso antes, se centra en la comisión de un delito utilizando como medio «un elemento informático, ya sea *hardware* o *software*»[126]. En la misma línea, se define como «fenómeno delictivo de rápida propagación bajo el cual se englobarían todos aquellos delitos que puedan cometerse por medio de un equipo conectado a una red informática»[127]. Otra definición sería la de CAMACHO LOSA, citada por HERNÁNDEZ DÍAZ «toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas»[128]. Para finalizar con esta exposición de definiciones, cabe mencionar la adoptada por un comité de expertos de la OCDE «cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos[129]».

Al no existir un consenso claro en la concepción de los ciberdelitos, tampoco lo habrá en la clasificación. La doctrina ha elaborado numerosas clasificaciones, desde la división «por su carácter económico o lucrativo y afección a la privacidad»[130], a la

[122] ROMEO CASABONA, *Poder informático y seguridad jurídica*, 1988, 41.
[123] DAVARA RODRÍGUEZ, *Derecho informático*, 1993, 302.
[124] En más detalle MIRÓ LLINARES, *El cibercrimen*, 2012, 39 y ss. (Versión *online*).
[125] BARRIO ANDRÉS, *Delincuencia informática*, 2012, 34.
[126] DAVARA RODRÍGUEZ, *Derecho informático*, 1993, 302.
[127] ORTIZ PRADILLO, *Problemas procesales de la ciberdelincuencia*, 2013, 17.
[128] CAMACHO LOSA, *El delito informático*, 1987, 25 y ss; citado por: HERNÁNDEZ DÍAZ, *Eguzkilore*, n.º 23, 2009, 231.
[129] OCDE, citada por VIDAURRI ARÉCHIGA, en NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 204.
[130] SALT, en VVAA, *Delitos no convencionales*, 1994, 227.

división «en función del método informático utilizado para lesionar al bien jurídico en cuestión»[131].

MIRÓ LLINARES plantea una clasificación tripartita, siguiendo el concepto de ciberdelito en sentido amplio[132] y atendiendo a la incidencia de las TIC´s en el comportamiento criminal[133]:

- Ciberataques puros. Conductas ilícitas que son el medio y objetivo para realizar la acción típica. Algunos ejemplos son: el *hacking*, infectar con *malware*, *spam*, ataques DoS.
- Ciberataques réplica. Son aquellas conductas ilícitas que ya se realizaban en el ámbito físico y, ahora, tienen su réplica en el ciberespacio. Algunos ejemplos son: los ciberfraudes o *scam*, el *phishing*, ciberespionaje, *grooming*.
- Ciberataques de contenido. Estos se consideran una parte de los anteriores debido a unas especialidades. Se subdividen en tres grupos:
  - Por la ilicitud del contenido. P. ej. El ciberterrorismo.
  - Por la no autorización en la explotación del contenido. P.ej. La piratería intelectual o industrial.
  - Por la víctima que recibe el contenido. P. ej. La pornografía infantil.

Otra clasificación sería según los criterios de medio o instrumento, u objetivo o fin. En el primer caso, las TIC´s serían el medio para realizar el tipo (*stalking*, clonación de tarjetas, *grooming*); mientras que las segundas tienen como objetivo las TIC´s (robo de datos, dañar los programas)[134].

Incluso podría encontrarse otra clasificación en el Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001[135]. En el que se «sistematiza

[131] Accesible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf (visitada 18/06/2021).

[132] «Cualquier comportamiento delictivo realizado en el ciberespacio». MIRÓ LLINARES, *El cibercrimen*, 2012, 42. (Versión *online*). En cambio, si se entiende los ciberdelitos en sentido estricto, solo ha lugar a los ciberataques puros.

[133] MIRÓ LLINARES, *El cibercrimen*, 2012, 52-102. (Versión *online*).

[134] MIRÓ LLINARES, *El cibercrimen*, 2012, 205-206. (Versión *online*). Clasificación apoyada por TÉLLEZ VALDÉS, *Derecho informático*, 4.ª, 2008, 105. (Versión *online*).

[135] Accesible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221 (visitada el 22/08/2021).

los comportamientos en cuatro grupos: 1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) Delitos informáticos; 3) Delitos relacionados con el contenido; y 4) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines»[136].

2. ALGUNOS DE LOS DESAFÍOS QUE PRESENTAN LOS CIBERDELITOS

Cuando la delincuencia comienza a asomarse por internet, lo hace con escasa entidad, ya que como señala BARRIO ANDRÉS, era «practicada por un conjunto [mínimo] de expertos que fundamentalmente actuaban por una suerte de inquietud intelectual»[137], en otras palabras, eran jóvenes que querían poner a prueba sus conocimientos sobre el ciberespacio, los denominados *hackers*[138].

En la actualidad, las actuaciones de estos ciberdelincuentes[139] han cambiado de forma decisiva. Esos primeros *hackers* mencionados antes «han abandonado unos roles que en muchos casos sólo perseguían el simple reconocimiento, para ponerse a merced de grupos organizados que han sabido ver en sus habilidades un auténtico filón para explotar conjuntamente con sus estructuras criminales [falsificación, estafa, prostitución, entre otras]»[140]. Por lo tanto, el perfil de ciberdelincuente ya no es único, es cierto que «todavía subsisten *hackers* fieles al espíritu original como es el caso de las figuras de Assange, Snowden o el fenómeno de Anonymous[141]. […] Otra parte de ellos se han reconvertido en expertos de ciberseguridad [o] colaboradores de las Fuerzas y Cuerpos de Seguridad»[142], pero es imposible determinar un perfil que caracterice a un ciberdelincuente. Existan varios perfiles, y uno de ellos es el que queda reflejado en este trabajo, el de aquellos que pueden cometer delitos de mayor entidad, esto es que «[hayan

[136] MAYER LUX, *Revista Chilena de Derecho*, vol. 44, n.º 1, 2017, 244.
[137] BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 42.
[138] No confundir este término con *crackers*: «[quienes] utilizan sus grandes conocimientos técnicos para violar sistemas, entrar en ordenadores, robar información o romper la protección y seguridad de los sistemas o programas no para conocer, sino para obtener un provecho material, normalmente económico o provocar un daño», así: ALCOBERRO I PERICAY, *Comunicación: estudios venezolanos de comunicación*, n.º159-160, 2012, 64.
[139] El ciberdelincuente se define como «Todo sujeto que perpetra un hecho delictivo utilizando como parte central el ciberespacio, a través de las nuevas tecnologías informáticas o de telecomunicaciones» Así: CÁMARA ARROYO, *Derecho y Cambio Social*, n.º 60, 2020, 492.
[140] LÓPEZ LÓPEZ, *IDP* n.º5, 2007, 65.
[141] Sobre ello COLEMAN, *Las mil caras de Anonymous*, 2016, *passim.*
[142] BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 43.

sido] contratados por un Estado para atacar infraestructuras críticas de otro Estado, [o] los que forman parte de organizaciones y grupos criminales y lo hacen por razones puramente económicas»[143].

ABOSO establece entre otros los siguientes desafíos que presentan las TIC´s en el ámbito penal: «a) el anonimato, b) el bajo costo, c) vulnerabilidad de los sistemas y redes telemáticas, d) la vulnerabilidad tiene como efecto o consecuencia que se ve afectada la integridad, funcionalidad y confidencialidad de los sistemas informáticos […] y e) delitos a distancia y conflictos jurisdiccionales»[144].

A continuación, se hará referencia a algunos de estos desafíos, los que más incidencia tienen en el caso Stuxnet.

2.1. Sobre el anonimato y bajo coste de Internet, y sus consecuencias

La popularidad que tiene internet, entre otras cosas, se debe al anonimato que ofrece, a un bajo coste[145]. Como expone FERNÁNDEZ TERUELO «el derecho penal y el procesal (penal) vigentes, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de criminalidad física, marginal e individual. Frente a ello, con la aparición de Internet, los distintos organismos encargados de su represión se han debido enfrentar a un cauce de ejecución delictiva que cuestiona plenamente muchos de los axiomas vigentes. Así, el medio Internet determina, en primer lugar, una notable y especial dificultad para la detección y persecución del delito debido, entre otros factores, a las posibilidades de anonimato que ofrece el mismo, a la escasa conciencia de los usuarios respecto a la necesidad de mantener una serie de medidas de seguridad, o al carácter transnacional de algunas conductas delictivas»[146].

Pero ¿en qué se traduce este anonimato? Desde una perspectiva penal, los ciberdelitos presentan un gran problema a la hora de determinar a los responsables

[143] BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 43.

[144] ABOSO, *Derecho penal cibernético*, 2017, 31. En la misma línea, entre otros, VIDAURRI ARÉCHIGA, en NAVA GARCÉS, *Ciberdelitos*, 2019, 202.

[145] LÓPEZ ORTEGA, *CDJ*, n.º 10, 2001, 119.

[146] FERNÁNDEZ TERUELO, *Cibercrimen, los delitos cometidos a través de Internet*, 2007, 13. En la misma línea FLORES PRADA, *RECPC*, n.º 17, 2015, 9.

jurídico-penales[147]. Si bien es cierto que es posible identificar la dirección IP del ordenador desde el que se ha llevado a cabo la acción o se ha utilizado como medio, ello no garantiza la identificación de la persona[148].

Los métodos para acceder a internet de forma anónima, como señala la UIT, son «los terminales públicos de Internet, las redes abiertas (inalámbricas), las redes pirateadas y los servicios de prepago que no requiere registro»[149]. Un ejemplo claro sería el sistema TOR[150] para acceder a la *Deep web*, aunque no es la única forma[151].

Como se señaló *ut supra*, de la mano del anonimato va el bajo coste de los elementos que se utilizan para llevar a cabo ciberdelitos. Como señala VIDAURRI ARÉCHIGA «la desproporción entre los beneficios ilícitos que puede alcanzarse mediante el uso abusivo de las computadoras y la baja probabilidad de ser descubiertos y juzgados adicionan escollo a la intervención jurídicopenal»[152].

2.2. Sobre los delitos a distancia y competencia territorial

La globalización que va a aparejada de internet «dificulta extraordinariamente determinar el lugar de comisión del delito y, en consecuencia, la competencia para juzgar unos determinados hechos, así como esclarecer la autoría»[153].

La premisa de la que se parte es que la acción típica se desarrolla en el ciberespacio[154]. Donde el sujeto activo puede actuar en un país, utilizar los recursos de

[147] MATA Y MARTÍN, *Actualidad penal*, n.º 37, 2003, 935 y ss. En el mismo sentido CORCOY BIDASOLO, *Eguzkilore*, n.º 21, 2007, 23.

[148] VIDAURRI ARÉCHIGA, en NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 202.

[149] Accesible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf (visitada el 19/06/2021).

[150] BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 44.

[151] Existen otros sistemas como *ZeroNet*, *Freenet* o I2P.

[152] VIDAURRI ARÉCHIGA, en NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 202.

[153] FERNÁNDEZ TERUELO, *Cibercrimen, los delitos cometidos a través de Internet*, 2007, 14-26. En el mismo sentido BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 50.

[154] BARRIO ANDRÉS, *Delitos 2.0: aspectos penales*, 2018, 50

otro y producir el resultado en otro[155]. Aquí entra en juego los problemas para determinar la competencia judicial[156].

A todo esto, se debe sumar la rapidez y facilidad con la que se mueven los datos, en este caso el material ilícito, sirviéndose estos autores de los denominados paraísos informáticos[157] o «espacios de impunidad, en los que el control normativo, por intereses superiores o por nivel de desarrollo de la sociedad, no existe o es muy permisivo»[158].

En conclusión, todas estas circunstancias navegan hacia la famosa sociedad de la información, pero el precio a pagar es la inseguridad en el ciberespacio, «donde no existen los mismos patrones sociales del mundo real, un mundo al que nos asomamos oculto tras la pantalla […]. Donde la protección que ofrece la facilidad de crear identidades ficticias supone un acicate o desinhibidor de nuestros temores frente a las barreras sociales, impulsándonos a veces a superar la legalidad establecida»[159].

3. ANÁLISIS DE LAS CONDUCTAS TÍPICAS QUE RODEAN AL CASO STUXNET.

Se expondrá la posibilidad de aplicar una serie de delitos al ya explicado caso Stuxnet. Se va a plantear la posible calificación jurídico-penal tomando como referencia el actual CP, es decir, no se va a tomar en consideración la fecha de comisión de los hechos (cometidos en 2010); además en 2015 se han reformado la mayoría de los delitos que se mencionarán en este epígrafe 3.

Como establece SUBIJANA ZUNZUNEGUI las conductas delictivas se establecen en un marco cuadrangular[160]:

- Sujeto Activo. Quien realiza la acción de insertar Stuxnet en la central de Natanz. Tiene lugar la figura de autoría mediata (EE.UU. e Israel) en

[155] Accesible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf (visitada el 19/06/2021).

[156] Más adelante se explicarán los principios, territoriales y extraterritoriales, que determinan la competencia judicial regulados en el art. 23 LOPJ.

[157] Sobre ello CLIMENT BARBERÁ, *CDJ*, n.º 10, 2001, 660 y ss; ADÁN DEL RÍO, *Eguzkilore*, n.º 20, 2006, 158 y ss.; FLORES PRADA, *RECPC*, n.º 17, 2015, 20 y ss.

[158] SALOM CLOTET, *Cuadernos de Estrategia*, n.º 149, 2011, 134-135.

[159] SALOM CLOTET, *Cuadernos de Estrategia*, n.º 149, 2011, 135.

[160] SUBIJANA ZUNZUNEGUI, *Eguzkilore* n.º 22, 2008, 171.

cuanto a que los países crean un grupo multidisciplinar (autores directos o inmediatos) para llevar a cabo Stuxnet.

- Coadyuvantes (no intencionados). Los que proveen el servicio de internet. En este caso no ha lugar, porque no se accedió a los terminales desde internet.
- Ciberdelito. Sera objeto de estudio a continuación.
- Sujeto pasivo. Quien sufre los daños de la acción, en el caso fue Irán. Lo que he señalado antes sobre el lugar que va a ocupar el apartado dedicado a la competencia judicial, donde se planteará como hipótesis que los hechos sucedidos en el caso Stuxnet se hubieran cometido en España.

3.1. Ciberterrorismo

Al igual que no existe un acuerdo sobre la definición de los delitos cibernéticos, tampoco existe sobre el ciberterrorismo. Este concepto ha ido evolucionando a lo largo de los años, como se expone brevemente a continuación.

El concepto de ciberterrorismo fue acuñado en los 80 por BARRY COLLIN, quien de una forma simplificada lo definía «como la convergencia del ciberespacio del terrorismo»[161]. Después, en los 90 MARK POLLIT, un agente del FBI que concretó más la definición: «es 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»[162].

Sin embargo, previamente a obtener ninguna definición hay que analizar una serie de cuestiones.

En primer lugar, el terrorismo se estructura conforme a un elemento medial (ejecución de los actos de extrema violencia o intimidación), un elemento estructural

[161] COLLIN, *The Future of CyberTerrorism: Where the Physical and virtual Worlds Converge*, citado por NIETO FERNÁNDEZ, *Revista General de Marina*, vol. 275, mes 1 (julio), 2018, 134.

[162] POLLIT, *Computer Fraud &* Security, citado por NIETO FERNÁNDEZ, *Revista General de Marina*, vol. 275, mes 1 (julio), 2018, 134.

(vinculación a un grupo u organización criminal[163]), y un elemento teleológico (la destrucción del Estado de Derecho)[164].

Como modalidad específica existe el ciberterrorismo, que puede analizarse desde una perspectiva medial o final. La primera significa que el terrorismo utiliza las TIC´s como forma de intimidar, coaccionar; mientras que la perspectiva final constituye la destrucción de los datos sensibles que se encuentran en los sistemas informáticos[165], siendo esta última la que englobaría mejor el caso Stuxnet.

En la misma línea, GONZÁLEZ AMADO establece unas premisas para saber qué conductas pueden considerarse como una amenaza[166]. Entre ellas: 1) las máquinas dependen del hombre, por lo que solo alguien con los conocimientos suficientes será capaz de sembrar el terror; 2) no existe un sistema informático infranqueable, todo puede ser *hackeado*; 3) la sociedad en la que vivimos depende en gran parte de la tecnología, al no guardarse las correctas medidas de seguridad, esto puede servir a los delincuentes; 4) la seguridad es un punto muy importante, por lo que una forma de limitar o minimizar los riesgos sería restringir el uso de los servidores oficiales, tanto a nivel público como privado, el problema radica en que estas actuaciones causarían un colapso en los servicios que prestan; y 5) señala el autor que «según los reportes consultados, la seguridad informática es violada, primordialmente, por personas que se encuentran en el entorno en donde ella misma ha sido desarrollada»[167], entre ellos hace referencia a exempleados, sin embargo, se está viendo que ya no es necesario tener esos conocimientos previos de los sistemas a atacar.

De manera más actual la definición que puede resultar más objetiva sería la de VERTON[168], quien define el ciberterrorismo como «es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, con objetivo político, utilizando tecnología

[163] Definido en el art. 570 ter1 CP: « A los efectos de este Código se entiende por grupo criminal la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos». Y en el art. 570 bis 1 CP: «A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos».

[164] SUBIJANA ZUNZUNEGUI, *Eguzkilore*, n.º 22, 2008, 172.

[165] SUBIJANA ZUNZUNEGUI, *Eguzkilore*, n.º 22, 2008, 172-173.

[166] GONZÁLEZ AMADO, *DPC*, vol. 28, n.º 84, 2007, 25-27.

[167] GONZÁLEZ AMADO, *DPC*, vol. 28, n.º 84, 2007, 26.

[168] Periodista especializado en seguridad informática y antiguo oficial de la inteligencia Naval de EE.UU.

informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos servicios esenciales[169]. El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general. El ciberterrorismo existe porque es el reino cibernético donde son más débiles la mayoría de las naciones industrializadas»[170].

Es importante el marco legal que engloba este delito. Puesto que a raíz de los atentados del 11-M o el 11-S, la UE ha reforzado su actuación frente a estos ciberdelitos.

Un primer paso fue la Decisión Marco 2002/475/JAI[171] del Consejo, de 13 de junio, relativa a la lucha contra el terrorismo, la cual ha sido modificada por la Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre[172]. El último, de momento, es la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo[173]: esta se traspuso mediante la LO 1/2019, de 20 de febrero, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, para trasponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, y abordar cuestiones de índole internacional[174].

También cabe mencionar, de forma más general, porque afecta a todos los ciberdelitos, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto, relativa a los ataques contra los sistemas de información y por la que se sustituye

[169] Conforme a la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas, define en su art. 2 como servicio esencial «el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas». El daño que afecte a una infraestructura crítica aparece tipificado en el art. 264.2.4.ª CP.

[170] VERTON, *Black Ice. La amenaza invisible del ciberterrorismo*, 2004, 32.

[171] Es un primer paso para unificar legislaciones, estableciendo unos mínimos sobre los delitos de terrorismo. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002F0475&from=ES (visitada el 20/06/2021).

[172] Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008F0919&from=ES (visitada el 20/06/2021).

[173] Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-80558 (visitada el 21/08/2021).

[174] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2019-2363&p=20190221&tn=1 (visitada el 21/08/2021).

la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero[175]. Finalmente, el Convenio del Cibercrimen de Budapest, de 23 de noviembre de 2001[176], que, aunque no regula el ciberterrorismo, tiene una gran importancia puesto que se centra en la protección de: la seguridad, integridad y libertad informática.

En el ámbito nacional, el art. 573.2 CP establece que: «Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior». Las finalidades se establecen en el 573.1 CP y son:

«1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.ª Alterar gravemente la paz pública.

3.ª Desestabilizar gravemente el funcionamiento de una organización internacional.

4.ª Provocar un estado de terror en la población o en una parte de ella».

Es momento de preguntarse si la conducta expuesta en el apartado I de este trabajo puede englobarse en este art. 573 CP. Para ello, en primer lugar, el hecho ha de poder subsumirse en uno de los ciberdelitos específicamente mencionados, en particular, en el delito de daños del art. 264 CP; para el caso de que se cumpla este requisito (y más adelante se hará una mención específica a esta posible calificación), en segundo lugar, se necesita, además, que se cumpla alguna de las finalidades[177] expuestas *ut supra*:

- Subvertir el orden constitucional. La RAE define subvertir como «trastornar o alterar algo, especialmente en el orden establecido»[178], es decir, que se persigue la modificación del régimen constitucional

[175] Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648 (visitada el 21/08/2021).

[176] Este Convenio ha sido ratificado por España. Accesible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221 (visitada el 20/06/2021).

[177] Explicado en más detalle en: ASUA BATARRITA, en ECHANO BASALDUA (coord.), *Estudios jurídicos en memoria de José María Lidón*, 2002, 78 y ss.

[178] Accesible en: https://dle.rae.es/subvertir (visitada el 21/08/2021).

existente. Claramente la conducta de Stuxnet no se podría englobar en este apartado.

- Alterar la paz pública. Se entiende una «situación de alarma o inseguridad social, como consecuencia del carácter sistemático, reiterado y muy frecuentemente indiscriminado de esta actividad delictiva»[179]. Como se ha explicado, ni siquiera Irán fue consciente de Stuxnet 0,5, tampoco ha lugar aquí.
- Desestabilizar una organización internacional[180]. No se atacó ninguna organización internacional.
- Causar el pánico en la población. Al igual que se expuso en la alteración de la paz pública, si ni siquiera se encajaba ahí, mucho menos en la finalidad de causar el pánico a la población.

Por todo ello, analizando este precepto no se cumple ninguna de las finalidades establecidas en el tipo; se puede suponer que Stuxnet perseguía la finalidad de detener el programa nuclear de Irán, por lo que no encajaría en ninguna de las cuatro finalidades.

Cabría la posibilidad de sugerir, como mucho, un delito de colaboración con organización, grupo o elemento terrorista del art. 577 CP. Sin embargo, si entendemos que EE.UU e Israel colaboraron (sobre todo económicamente, pero también suministrando los equipos necesarios) con un grupo de expertos informáticos, quienes lanzaron Stuxnet a la central de Natanz, no podrían estos técnicos, desde mi punto de vista ser tachados de terroristas, puesto que no cumplen con la definición ni de grupo ni de organización criminal.

Hay que tener en cuenta, como explica NIETO FERNÁNDEZ, que el hecho de que un grupo terrorista desarrolle una ciberarma de estas magnitudes es difícil (salvo que cuente con ayuda de algún Estado), por dos motivos fundamentales: 1) Stuxnet necesitaba un «equipo multidisciplinar que englobe físicos, ingenieros, informáticos y otros muchos y largos años de trabajo que han de ser sufragados [a ello sumándole la capacidad de] desarrollar una ciberarma con capacidad de atacar con efectividad una infraestructura

[179] ASUA BATARRITA, en ECHANO BASALDUA (coord.), *Estudios jurídicos en memoria de José María Lidón*, 2002, 79.

[180] Término expuesto en más detalle en la Decisión Marco 2002/475/JAI del Consejo, en su art. 1. Accesible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002F0475:20081209:ES:PDF (visitada el 21/08/2021).

crítica»[181]; y 2) el éxito que tuvo este *malware* se debió a la colaboración o posible chantaje de una persona que trabajara dentro de la central.

Todo ello, ha lugar a la necesidad de que debiera existir una información previa del interior de la central de Natanz, por lo que se abre paso al siguiente delito, el espionaje.

3.2. Ciberespionaje: hacking

Se parte de la premisa donde «el ciberespionaje no es comparable al espionaje tradicional»[182]. En las relaciones internacionales, siempre han existido conflictos de intereses por distintos motivos (económicos, geopolíticos, militares, etc.), donde las agencias de inteligencia de los países desarrollan, a la par que avanza la tecnología, una nueva forma de controlar la información, el ciberespionaje, que se ha convertido «en un arma poderosa, silenciosa y efectiva»[183]. Se ha pasado de pinchar teléfonos a una serie concreta y específica de acciones en el ciberespacio[184].

Las fases para realizar un ataque contra un ordenador o red de ordenadores son las siguientes[185]:

- Reconocimiento. Consiste en recabar toda la información posible sobre el futuro sujeto pasivo de la acción.
- Escaneo. Con la información pertinente anterior, se estudia las posibles vulnerabilidades del sistema, centrándose en los puertos[186].
- Ganar acceso. Una vez detectadas las vulnerabilidades, con sus conocimientos técnicos podrá penetrar o no en el terminal.
- Mantener el acceso. Cuando ya está dentro del ordenador, debe permanecer invisible para la víctima, puesto que entre más tiempo permanezca más acceso a la información tendrá.

[181] NIETO FERNÁNDEZ, *Revista General de Marina*, vol. 275, mes 1 (julio), 2018, 139-140. Como señala el autor, el presupuesto de Stuxnet fue de unos 300 millones de dólares.

[182] SÁNCHEZ MEDERO, *Derecom*, n.º 13 (marzo-mayo), 2013, 116.

[183] ALBA USECHE, *Ciencia y Poder Aéreo*, vol. 9, n.º 1, 2014, 98.

[184] SÁNCHEZ MEDERO, *Derecom*, n.º 13 (marzo-mayo), 2013, 116. Para más información sobre la evolución del espionaje al ciberespionaje: ALBA USECHE, *Ciencia y Poder Aéreo*, vol. 9, n.º 1, 2014, 99 y ss.

[185] MAMANI QUISBERT, *Revista de Información, Tecnología y Sociedad*, n.º 8, 2013, 70.

[186] Los puertos son puntos de conexión con el ordenador.

- Cubrir las huellas. Esta es una de las fases más importantes, pues se centra en borrar todo tipo de pruebas que le puedan incriminar.

Estas conductas están teniendo cada vez más eco en la sociedad actual, dando lugar a casos mediáticos[187].

Como señala MUÑOZ CONDE: «el tipo comprende tanto el acceso al sistema, como el mantenimiento dentro del mismo. La segunda modalidad es alternativa a la primera y supone que ha habido un acceso legítimo, pero que después, por las razones que sean, el titular del sistema cancela el permiso para ese acceso, lo que convierte la permanencia en ilegítima. No obstante, si la denegación del permiso va paralela a la adopción de medidas que impidan la continuación en el acceso (modificando por ejemplo la clave de acceso)la nueva entrada se debe incluir en el supuesto primero»[188].

Se ha de tener en cuenta que el bien jurídico protegido en este precepto está en discusión. Se plantea que el legislador al ubicarlos dentro de los delitos contra la intimidad pretendió «dar *ex novo* una protección de la seguridad de los sistemas informáticos»[189]; de ahí que el bien jurídico protegido en este caso sean los sistemas informáticos de la central.

En primer lugar, podrían ser imputados los informáticos como autores directos (ya que los autores mediatos serían los responsables estadounidenses e israelís) por el delito tipificado en el art. 197 bis 1 CP, que reza así «el que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años».

El art. 197 bis exige que el hecho se cometa, primero, vulnerando medidas de seguridad para impedir el acceso, y segundo, que el sujeto no esté debidamente autorizado. No se sabe quién ha podido cometer el hecho narrado en el apartado I, parece que ha podido ser algún empleado de la central (supuestamente personal de limpieza); si es así, es importante saber exactamente qué empleado ha podido ser, porque tiene

[187] Véase p. ej.: https://as.com/meristation/2021/04/23/betech/1619175232_192867.html (visitada el 05/09/2021).
[188] MUÑOZ CONDE, *Derecho penal. Parte especial*, 23ª ed., 2021, 282.
[189] COLÁS TURÉGANO, *Revista Boliviana de Derecho*, n.º 21, 2016, 215.

implicaciones en estos dos elementos del 197 bis; ya que esa persona introdujo los USB en los servidores con el fin de dar acceso a los programas que controlaban las centrifugadoras de uranio.

3.3. Cracking o sabotaje informático

Existe en nuestro CP la figura de sabotaje informático o *cracking*, la cual no puede confundirse con el *hacking* (explicado en el apartado anterior): mientras que este hace referencia al acceso sin autorización; el sabotaje se refiere a haber causado daños informáticos.

Como señala la doctrina, este concepto implica la «conducta consistente en la destrucción o en la producción generalizada de daños en su sistema, datos, programas informáticos o telemáticos»[190]. Este delito se encuentra tipificado en el art. 264 CP, que reza así:

«1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la

[190] Véase, por todos, MARCHENA GÓMEZ, *Actualidad Jurídica Aranzadi*, n.º 40, 2001, 7.

protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.»

Tomando en consideración los hechos narrados en el apartado I, se procede a explicar brevemente los elementos del tipo.

Es difícil señalar claramente el bien jurídico protegido. Si bien es cierto que este delito se engloba en el Título XIII delitos contra el patrimonio y orden socioeconómico, así que, en un principio podría entenderse este como el bien jurídico protegido. Pero la ubicación sistemática no es un elemento decisivo para deducir el objeto de protección; de hecho, se ha entendido que en el delito de daños o sabotaje informático se protege «un bien jurídico específico, propiamente informático»[191]. Sin embargo, al haber tenido Stuxnet repercusión en el mundo real, creo conveniente fijar como bien jurídico el patrimonio, entendido este como «un conjunto de derechos y obligaciones, referibles a cosas u otras entidades, que tienen un valor económico y que deben ser valorables en dinero»[192].

Siguiendo con el tipo objetivo, este precepto regula un delito de resultado[193], por lo que se exige una relación de causalidad entre la acción y el resultado. La teoría de la equivalencia de las condiciones[194] dispone que si, al suprimir mentalmente la acción que provoca el resultado, este no se produce, entonces si será causa de ese resultado. Esto es, que si Stuxnet no hubiera accedido a los servidores de Natanz no hubiera provocado los

[191] MAYER LUX, *Revista Chilena de Derecho*, vol. 44, n.º 1, 2017, 246.

[192] MUÑOZ CONDE, *Derecho Penal. Parte especial*, 23ª ed., 2021, 366-367. (Versión *online*).

[193] No solo se sanciona la mera conducta (delitos de simple actividad), sino que se castiga la producción del resultado.

[194] En más detalle GARCÍA ARÁN/MUÑOZ CONDE, *Derecho penal. Parte general*, 9ª ed., 2015, 219 y ss. (Versión *online*).

daños en las centrifugadoras de uranio en la central nuclear iraní; ello concluye que existe relación de causalidad.

Se cumple la conducta-objeto señalada en el apartado 1, ya que se ha actuado sin autorización, y de manera grave se han alterado los datos de las centrifugadoras de uranio, es decir, la gravedad podría radicar en la alteración de los mecanismos que controlaban material nuclear.

Finalmente hay que analizar la imputación objetiva, de la cual hay que cumplir tres requisitos:

- Crear un riesgo penalmente relevante. Esto es que la creación del *malware* (el riesgo) específicamente para la destrucción de centrifugadoras
- Relación del riesgo. Ese *malware* fue el causante de que las centrifugadoras fallaran y dejaran de enriquecer uranio.
- Ámbito de protección de la norma. Claramente se puede enmarcar en el art. 264 CP, conducta que dicho precepto pretendía evitar.

Tras analizar brevemente estos elementos del tipo, a mi juicio, cabría englobar la conducta de una forma más correcta, en el tipo del art. 264. 2. 4.ª CP.

Se aplicaría la pena agravada del apartado 2 (prisión de dos a cinco años y multa del tanto al décuplo del perjuicio), puesto que concuerda con la circunstancia del subapartado 4.ª «Los hechos hayan afectado al sistema informático de una **infraestructura crítica** o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones». Incluso, cabría la aplicación del 264.3 CP si se probara la utilización de las tarjetas identificativas del personal para acceder a la central de Natanz.

En conclusión, las conductas encajan en dos preceptos penales: 1º) delito de *hacking* del art. 197 bis I CP y 2º) delito de *cracking* o sabotaje informático del art. 264.2.4ª CP. Ambos, a mi juicio, deben aplicarse el concurso ideal impropio o medial, esto es que un delito sirve de medio para cometer otro, «la jurisprudencia y la doctrina

exigen, con razón, que este precepto sólo sea aplicable cuando exista una *relación de necesidad*, que debe ser entendida en un sentido real, concreto y restrictivo; de tal forma que no bastará el plan subjetivo del autor, sino que será preciso que en el caso concreto un delito no pueda producirse objetivamente sin otro delito, que esté tipificado como tal de forma independiente»[195]. Esto cuenta su apoyo en el caso práctico, puesto que de no haber accedido a los servidores de Natanz (delito de *hacking* art. 197 bis I CP), no habría sido posible hacerse con el control y manipular los controladores de las centrifugadoras (sabotaje informático art 264.2.4ª. CP).

3.4. Ciberguerra

El hecho de que los países afirmen utilizar el ciberespionaje como un medio para reforzar su seguridad, conlleva a la reacción de que los países afectados reaccionen mediante algún conflicto, incluso la ciberguerra.

Son muchos los autores[196] los que hablan sobre la guerra del s. XXI como aquella que se librará en el ciberespacio, aunque esto no conlleva la desaparición de la guerra tradicional (como se ha visto recientemente, en las noticias sobre Irán e Israel). Como señala JOHN ARQUILLA, la ciberguerra es «una guerra mejor, más barata y menos sangrienta»[197].

Autores como NAVA GARCÉS señalan el ciberterrorismo como el paso previo a la ciberguerra[198]. Por lo expuesto *ut supra* no es de aplicación el delito de ciberterrorismo, por lo que *a priori* tampoco parece serlo el de ciberguerra.

[195] GARCÍA ARÁN/MUÑOZ CONDE, *Derecho penal. Parte general*, 9ª, 2015, 469. (Versión *online*).

[196] Entre ellos: SÁNCHEZ MEDERO, *Boletín de Información*, n.º 317, 2010, 63 y ss; *Derecom*, n.º 11 (septiembre-noviemnre), 2012, 124 y ss; LEJARZA ILLARO, *Pre-bie3*, n.º 1, 2014, 1 y ss; AZNAR LAHOZ, *Pre-bie3*, n.º 1, 2015, 1 y ss.

[197] ARQUILLA, *Swarming and the future of conflicto*, 2000; citado por SÁNCHEZ MEDERO, *El viejo topo*, n.º 275, 2010, 9.

[198] NAVA GARCÉS, en: NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 178.

Los cuatro Convenios de Ginebra de 1949[199] y sus dos Protocolos adicionales de 1977[200] establecen los límites sobre la guerra[201]. La guerra podría definirse como «agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático»[202]. Además, señala el Ministerio de Defensa que el concepto de ciberguerra incluye, entre otros, «la intrusión en infraestructuras críticas»[203].

A nivel nacional, el CP militar trata más en profundidad la defensa nacional, pero no tipifica los actos de guerra contra España. Sin embargo, el Título XXIII CP, donde se tipifican los descubrimientos y revelación de secretos e informaciones relativas a la Defensa Nacional (arts. 598 y ss.); más concretamente el art. 602 CP establece: «El que descubriere, violare, revelare, sustrajere o utilizare información legalmente calificada como reservada o secreta relacionada con la energía nuclear, será castigado con la pena de prisión de seis meses a tres años, salvo que el hecho tenga señalada pena más grave en otra Ley», tipo penal en el que perfectamente se puede subsumir la conducta de Stuxnet. Puesto que en los hechos se señaló haber sustraído información de la central de Natanz. Este delito no especifica medios concretos para la comisión de las conductas típicas, por esto no es un impedimento para que las mismas puedan ser cometidas a través de medios tecnológicos. No se está ante un ciberdelito puro; sí se puede calificar como ciberdelito si se opta por un concepto amplio de este término.

[199] I Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña; II Convenio de Ginebra para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar; III Convenio de Ginebra relativo al trato debido a los prisioneros de guerra en el mar; y IV Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempo de guerra.

[200] Protocolo Adicional I relativo a la protección de las víctimas de los conflictos armados internacionales; y Protocolo Adicional II relativo a la protección de las víctimas de los conflictos sin carácter internacional.

[201] Accesible en: https://www.icrc.org/es/document/los-convenios-de-ginebra-de-1949-y-sus-protocolos-adicionales (visitada el 05/09/2021).

[202] SÁNCHEZ MEDERO, *Boletín de Información,* n.º 317, 2010, 64. En la misma línea GIL, *Análisis GESI*, n.º 35, 2017, 6.

[203] Monografías del CESEDEN, n.º 126, 2012, 32.

4. ATRIBUCIÓN DE LA COMPETENCIA JUDICIAL A LOS TRIBUNALES ESPAÑOLES. PRINCIPIO DE EXTRATERRITORIALIDAD

Como se ha expuesto *ut supra*, los Estados involucrados son EEUU, Israel e Irán.

Para analizar los principios que atribuyen competencia a los tribunales para el conocimiento de hechos delictivos ha de acudirse a normas extrapenales. En concreto, al art. 8.1 CC y a los arts. 4, 9.1º y 3º, 21 y 23 LOPJ.

El art. 8.1 CC establece que «las leyes penales, las de policía y las de seguridad pública obligan a todos los que se hallen en territorio español», es decir, que, tratándose de hechos sucedidos en territorio nacional, se aplicarán siempre las normas del Estado de carácter penal. En este caso concreto no es posible aplicar este precepto, puesto que nada ha ocurrido en España.

Siguiendo con la LOPJ, el art. 21.1 establece, de forma similar al anterior, «Los Tribunales civiles españoles conocerán de las pretensiones que se susciten en territorio español con arreglo a lo establecido en los tratados y convenios internacionales en los que España sea parte, en las normas de la Unión Europea y en las leyes españolas». Este precepto, como refleja su tenor literal, está referido al ámbito civil.

Para la asignación de competencia judicial en materia penal se ha de estar a lo dispuesto en el art. 23 LOPJ.

En primer lugar, se ha tomar en consideración el principio de territorialidad, expuesto en el art. 23.1 LOPJ, donde se señala: «En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte».

Dado que los hechos que han sido descritos en el apartado I han sido cometidos indudablemente fuera del territorio español, de momento no ha lugar a la atribución de la competencia a los tribunales españoles.

Por lo tanto, queda claro que, utilizando la regla general del principio de territorialidad, los jueces españoles no tienen competencia para conocer del caso Stuxnet. Ahora bien, el siguiente paso sería analizar los criterios de extraterritorialidad.

Prosiguiendo con el art. 23 LOPJ, este establece las excepciones al citado principio en los apartados 2, 3 y 4 de dicho precepto[204].

En primer lugar, el art. 23.2 LOPJ utiliza el principio de la nacionalidad, cuando «los criminalmente responsables fueren españoles o extranjeros que hubieran adquirido la nacionalidad española con posterioridad a la comisión del hecho» y cumplan una serie de requisitos. Claramente este apartado no resulta de aplicación, pues no consta que los hechos narrados en el apartado I hayan sido cometidos por un ciudadano español, o extranjero que haya adquirido la nacionalidad española con posterioridad a su comisión.

En segundo lugar, el art. 23.3 LOPJ regla el principio real o de protección, en el que ofrece una lista cerrada de los delitos que serán perseguibles cuando sean «cometidos por españoles o extranjeros fuera del territorio nacional». Los delitos son:

«a) De traición y contra la paz o la independencia del Estado.
b) Contra el titular de la Corona, su Consorte, su Sucesor o el Regente.
c) Rebelión y sedición.
d) Falsificación de la firma o estampilla reales, del sello del Estado, de las firmas de los Ministros y de los sellos públicos u oficiales.
e) Falsificación de moneda española y su expedición.
f) Cualquier otra falsificación que perjudique directamente al crédito o intereses del Estado, e introducción o expedición de lo falsificado.
g) Atentado contra autoridades o funcionarios públicos españoles.
h) Los perpetrados en el ejercicio de sus funciones por funcionarios públicos españoles residentes en el extranjero y los delitos contra la Administración Pública española.
i) Los relativos al control de cambios.»

La conducta de Stuxnet no encaja en ninguno de estos delitos, así que este principio tampoco puede ser utilizado para atribuir competencia a los tribunales españoles.

En tercer lugar, el art. 23.4 LOPJ[205] establece el principio de justicia universal, por el cual los tribunales españoles podrán conocer hechos que hayan tenido lugar fuera

[204] Explicados en más detalle en GUINOT MARTÍNEZ, *La reforma del principio de justicia universal*, 2018, 69 y ss. (Versión *online*).

[205] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666 (visitada el 22/08/2021).

del territorio nacional, hayan sido cometidos por español o extranjero y pertenezca a uno de los delitos que recoge este precepto.

Visto el art. 23.4 CP, la única posibilidad de que los jueces españoles sean competentes es que el caso Stuxnet sea calificado como delito terrorista, y claro, que se cumplan las condiciones que requiere el art. 23.4, en letras d) o e).

Por lo expuesto *ut supra*, *a priori* no cabría imputar la competencia a los tribunales españoles. Por lo que, este trabajo se ha planteado desde la hipótesis de cómo actuarían los juzgados españoles ante un ciberataque de esta magnitud.

CONCLUSIONES

I

Es indiscutible la existencia de un virus informático o *malware* que en un primer momento afectaba a la presión de las centrifugadoras para enriquecer uranio de Natanz y seguidamente, una evolución de ese mismo *malware* aumentaba y disminuía la velocidad en los rotores de las centrifugadoras. Lo que conllevó a la detención del armamento nuclear iraní. Además, es casualmente llamativo que la propagación de estos *malware* coincide con los puntos de tensión máxima entre EE.UU e Israel contra Irán.

Sin embargo, pese a todos los indicios que se han expuesto en el punto de la exposición fáctica, pese al impactante artículo de prensa que hizo saltar las alarmas del *New York Times*, es imposible, y así ocurrió, demostrar la autoría de EE.UU ni de Israel. Se pone en evidencia así el primer problema que gira en torno a los ciberdelitos, el anonimato que ofrece Internet.

II

Desde un punto de vista más jurídico, hay que partir de la idea de que los ciberdelitos o delitos informáticos no tienen una definición consensuada, la doctrina está dividida. En mi opinión, creo que el concepto de ciberdelito debe entenderse en sentido amplio, es decir, cualquier conducta que tenga lugar en el ciberespacio. Puesto que en todos ellos se plantean los mismos problemas que sirven para identificar a los ciberdelitos denominados puros.

Además, se regulan una serie de delitos a lo largo del CP actual, que, a pesar de poderse calificar como ciberdelitos, están dispersos en los diferentes capítulos de la ley. En otras palabras, no son una categoría autónoma, y en mi opinión, debería crearse un título aparte dentro del propio CP. Puesto que atendiendo a la relevancia que estos delitos están tomando, tienen la suficiente entidad para que sean tipificados de forma separada. Se está viendo como cada vez más, estos tienen un impacto mayor en nuestra sociedad y con ejemplos como Stuxnet queda constancia de que en nuestro ordenamiento (y más, en general) la respuesta que ofrecen antes estos problemas es incompleta, y en caso como el presente, insatisfactoria.

III

El avance exponencial de las TIC´s que acompaña a nuestra sociedad tiene numerosas ventajas y por supuesto, sus desventajas. Desde una perspectiva jurídico-penal, estas desventajas se ven en los ciberdelitos; puesto que, *a priori* parece favorecer no solo la comisión de los delitos, sino que anonimiza al sujeto activo, posible autor de los hechos delictivos.

IV

Al mencionar internet es inevitable hablar de la globalización. En la vertiente negativa de esta globalización, en los ciberdelitos, se traduce en los problemas que generan sobre la aplicación de los criterios de territorialidad. En la práctica, implica que una conducta ilícita cometida a través de internet pueda no encontrase tipificada en el Estado que conozca del asunto, es decir que quedaría impune. La solución, en mi opinión, más factible pero improbable es el establecimiento de una autoridad global que controle este tipo de ciberdelitos.

V

En lo referente a las posibles conductas en las que podría encuadrarse Stuxnet, tras analizar los delitos de: ciberterrorismo, *hacking* o *cracking* y ciberguerra, considero que, atendiendo al CP, el art. 197 bis I sería sin duda la primera conducta que abarca Stuxnet, al introducirse en los servidores de la central nuclear; ofreciendo así el control que da lugar al art. 264. 2. 4.ª CP para modificar los controladores que enriquecían el uranio de Natanz; para finalmente aplicar el art. 602 CP en cuanto a la sustracción de la información clasificada sobre el material nuclear de Irán. Sin embargo, se vuelve al problema principal de averiguar, con pruebas reales y no meros indicios, quien es el autor o los autores reales del delito, pues de la prueba de este elemento se podrá constatar el cumplimiento de alguno de los requisitos típicos exigidos en particular en el delito de *hacking*.

BIBLIOGRAFÍA[206]

ABOSO, Gustavo Eduardo: ***Derecho penal cibernético****: la cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, Editorial B de F, Madrid, 2017.

ADÁN DEL RÍO, Carmen: *La persecución y sanción de los delitos informáticos*, en: Eguzkilore, n.º 20, 2006, 151-161.

ALBA USECHE, Daniela Alejandra: *El espionaje y agencia de seguridad: los Estados Unidos y la Federación Rusa*, en: Ciencia y Poder Aéreo, vol. 9, n.º 1, 2014, 97-105.

ALCOBERRO I PERICAY, Ramon: *Ética aplicada en Internet, estudio de la ética hacker*, en: Comunicación: estudios venezolanos de comunicación, n.º 159-160, 2012, 60-67.

ASUA BATARRITA, Adela: *Concepto jurídico de terrorismo y elementos subjetivos de finalidad. Fines políticos últimos y fines de terror instrumental*, en ECHANO BASALDUA, Juan Ignacio (coord.): ***Estudios jurídicos en memoria de José María Lidón***, Universidad de Deusto, Bilbao, 2002, 41-85.

AZNAR LAHOZ, José Luis: *Evolución de los modelos de confrontación en el ciberespacio*, en: Pre-bie3, n.º 1, 2015, 1-25.

BAÑOS BAJO, Pedro: ***Así se domina el mundo***, Ariel, Barcelona, 2017.

BARRIO ANDRÉS, Moisés: ***Delitos 2.0: aspectos penales****, procesales y de seguridad de los ciberdelitos*, Wolters Kluwer, Madrid, 2018.

— ***Delincuencia informática***. *Tiempos de Cautela y Amparo*, Thomson Reuters Aranzadi, Navarra, 2012.

BERMEJO GARCÍA, Bermejo/GUTIÉRREZ ESPADA, Cesáreo: *Del programa nuclear de la República Islámica de Irán y de su evolución (política y derecho)*, AEDI, n.º 31, 2015, 7-63. (Versión *online*).

[206] Las palabras en negrita corresponden a las utilizadas para la cita abreviada (salvo en el caso de los nombres de revistas, cuya abreviación aparece en el índice de abreviaciones).

CAMACHO LOSA, Luis: ***El delito informático***. *Un análisis en profundidad del mayor riesgo con que se enfrenta la moderna sociedad informatizada*, L. Camacho, Madrid, 1987.

CÁMARA ARROYO, Sergio: *La cibercriminología y el perfil del ciberdelincuente*, en: Derecho y Cambio Social, n.º 60, 2020, 470-512.

CLIMENT BARBERÁ, Juan: *La justicia penal en internet. Territorialidad y competencias penales*, en: CDJ, n.º 10, 2001, 645-663.

COLÁS TURÉGANO, María Asunción: *El delito de intrusismo informático tras la reforma del CP español de 2015*, en: Revista Boliviana de Derecho, n.º 21, 2016, 210-229.

COLEMAN, Gabriella: ***Las mil caras de Anonymous****: Hackers, activistas, espías y bromistas*, Arpa Editores, Barcelona, 2016.

CORCOY BIDASOLO, Mirentxu*: Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos*, en: Eguzkilore, n.º 21, 2007, 7-32.

DAVARA RODRÍGUEZ, Miguel Ángel: ***Derecho informático***, Aranzadi Thomson Reuters, Madrid, 1993.

FARWELL, James/ROHOZINSKI, Rafal: *Stuxnet and the Future of Cyber War*, en: Survival, vol. 53, 2011, 23-40.

FERNÁNDEZ TERUELO, Javier Gustavo: ***Cibercrimen, los delitos cometidos a través de Internet****: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red*, Constitutio Criminalis Carolina, Oviedo, 2007.

FERREYROS SOTO, Carlos: *Aspectos metodológicos del delito informático*, en: Informática y derecho: Revista iberoamericana de derecho informático, n.º 9-11, 1996, 407-412.

FLORES PRADA, Ignacio: *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia*, en: RECPC, n.º 17, 2015, 1-40.

GARCÍA ARÁN, Mercedes/MUÑOZ CONDE, Manuel: ***Derecho penal. Parte general***, 9ª, Tirant lo Blanch, Valencia ,2015. (Versión *online*).

GARRIDO REBOLLEDO, Vicente: *El programa nuclear iraní y las dificultades para visitar a los amigos*, en: REEI, n.º 12, 2006, 1-13. (Versión *online*).

GIL, Javier Miguel: *La integración del ciberespacio en el ámbito militar*, en: Análisis GESI, n.º 35, 2017, 1-16.

GÓMEZ LLINÁS, Daniel Alejandro: *Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo:* ***Stuxnet el virus informático***, tesis doctoral, Universidad de Bogotá, 2017.

GONZÁLEZ AMADO, Iván: *Ciberterrorismo: una aproximación a su tipificación como conducta delictiva*, en: DPC, vol. 28, n.º 84, 2007, 13-46.

GONZÁLEZ RUS, Juan José: *Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos*, en: RECPC, n.º 1, 1999. (Versión *online*).

GUINOT MARTÍNEZ, Marta: ***La reforma del principio de justicia universal*** *y el delito de tráfico de drogas*, Tirant lo Blanch, Valencia, 2018. (Versión *online*).

HERNÁNDEZ DÍAZ, Leyre: *El delito informático*, en: Eguzkilore, n.º 23, 2009, 227-243.

JIMÉNEZ MACÍAS, Emilio: ***Técnicas de automatización avanzadas en procesos industriales***, tesis doctoral, Universidad de La Rioja, 2004.

JONSSON, Jonas: *Irán y la UE ¿una relación estratégica?*, en: Cuadernos de Estrategia, n.º 137, 2007, 165-194.

LEJARZA ILLARO, Eguskiñe: *Ciberguerra, los escenarios de confrontación*, en: Pre-bie3, n.º 1, 2014, 1-20.

LÓPEZ LÓPEZ, Antonio: *La investigación policial en Internet: estructuras de cooperación internacional*, en: IDP, n.º 5, 2007, 63-74.

LÓPEZ ORTEGA, Juan José: *Libertad de expresión y responsabilidad por los contenidos en Internet*, en: CDJ, n.º 10, 2001, 83-126.

LOREDO GONZÁLEZ, Jesús Alberto/RAMÍREZ GRANADOS, Aurelio: *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo*, en: Celerinet, año 1-vol. 2, 2013, 44-51.

LUZ CLARA, Bibiana/GABRIEL MURAD, Andrés: *Delitos y tecnologías de la información*, en NAVA GARCÉS, Alberto Enrique (coord.): ***Ciberdelitos***, Tirant lo Blanch, Ciudad de México, 2019, 141-155.

MAMANI QUISBERT, David Joel: *Fases de un ataque hacker*, en: Revista de Información, Tecnología y Sociedad, n.º 8, 2013, 70-71.

MARCHENA GÓMEZ, Manuel: *El sabotaje informático: entre los delitos de daños y desórdenes públicos*, en: Actualidad Informática Aranzadi, nº. 40, 2001, 1-8.

MARTÍNEZ, Matilde: *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*, en: VVAA: ***Cibercrimen y delitos informáticos***. *Los nuevos tipos penales en la era de internet*, Erreius, Buenos Aires, 2018, 33-47.

MATA Y MARTÍN, Ricardo: *Criminalidad informática: una introducción al cibercrimen*, en: Actualidad Penal, n.º 37, 2003, 935-961.

MAYER LUX, Laura: *El bien jurídico protegido en los delitos informáticos*, en: Revista Chilena de Derecho, vol. 44, n.º 1, 2017, 235-260.

MIRÓ LLINARES, Fernando: ***El cibercrimen****: fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons Ediciones Jurídicas y Sociales, Madrid, 2012. (Versión *online*).

MUÑOZ CONDE, Manuel: ***Derecho penal. Parte especial***, 23ª, Tirant lo Blanch, Valencia, 2021. (Versión *online*).

NAVA GARCÉS, Alberto Enrique: *Ciberterrorismo: La nueva cara de la delincuencia en el siglo XXI. La participación y fomento al delito por órganos de gobierno y empresas*, en: NAVA GARCÉS, Alberto Enrique (coord.): ***Ciberdelitos***, Tirant lo Blanch, Ciudad de México, 2019, 157-196.

NIETO FERNÁNDEZ, Ignacio: *La letalidad del ciberterrorismo*, en: Revista General de Marina, vol. 275, mes 1 (Julio), 2018, 133-142.

ORTIZ PRADILLO, Juan Carlos: ***Problemas procesales de la Ciberdelincuencia***, Coléx, Madrid, 2013.

POSADA MAYA, Ricardo: *El cibercrimen y sus efectos en la teoría de la tipicidad. De una realidad física a una realidad virtual*, en: NFP, n.º 88, 2017, 72-112.

REZA REYES, Sandra: *Uso ilícito de la red: "El caso de la DEEP WEB"*, en: NAVA GARCÉS, Alberto Enrique (coord.): ***Ciberdelitos***, Tirant lo Blanch, Ciudad de México, 2019, 181-196.

RIVADENEIRA, Erwin Frederick: *Stuxnet, la primera ciberarma*, en: Revista de Marina, n.º 951, 2016, 76-80.

ROIBÓN, María: *Reflexiones sobre el acceso ilegítimo a un sistema o dato informático*, en VVAA: ***Cibercrimen y delitos informáticos***. *Los nuevos tipos penales en la era de internet*, Erreius, Buenos Aires, 2018, 131-141.

ROMEO CASABONA, Carlos María: ***Poder informático y seguridad jurídica***. *La función tutelar del derecho penal ante las nuevas tecnologías de la información*, Fundesco, Madrid, 1988.

— *De los delitos informáticos al cibercrimen*, en: PÉREZ ÁLVAREZ, Fernando/NÚÑEZ PAZ, Miguel Ángel/GARCÍA ALFARAZ, Isabel (coords.): ***Universitas vitae: homenaje a Ruperto Núñez Barbero***¸ Ediciones Universidad de Salamanca, 2007, 649-670. (Versión *online*).

SALOM CLOTET, Juan: *El ciberespacio y el crimen organizado*, en: Cuadernos de Estrategia, n.º 149, 2011, 131-164.

SALT, Marcos: *Delitos informáticos de carácter económico*, en VVAA: ***Delitos no tradicionales***, Editores el puerto, Buenos Aires, 1994, 224-242.

SÁNCHEZ MEDERO, Gema: *Los Estados y la Ciberguerra*, en: Boletín de Información, n.º 317, 2010, 63-76.

— *¿El ataque a Irán es el inicio de la ciberguerra?*, en: El viejo topo, n.º 275, 2010, 8-17.

— *La ciberguerra: los casos de Stuxnet y Anonymous*, en: Derecom, n.º 11 (septiembre-noviembre), 2012, 124-133.

— *El ciberespionaje*, en: Derecom, n.º 13 (marzo-mayo), 2013, 115-124.

SHAKARIAN, Paulo: Stuxnet: *Revolución de Ciberguerra en los Asuntos Militares*, en: Air and Space Power Journal, 2012, 50-59.

SUBIJANA ZUNZUNEGUI, Ignacio José: *El ciberterrorismo: una perspectiva legal y judicial*, en: Eguzkilore, n.º 22, 2008, 169-187.

TÉLLEZ VALDÉS, Julio: ***Derecho informático***, 4ª, McGraw Hill, México, 2008. (Versión *online*).

TEMPERINI, Marcelo: *Delitos informáticos y cibercrimen: alcance, conceptos y características*, en: VVAA: ***Cibercrimen y delitos informáticos***. *Los nuevos tipos penales en la era de internet*, Erreius, Buenos Aires, 2018, 49-68.

VERTON, Dan: ***Black Ice. La amenaza invisible del ciberterrorismo***, McGraw Hill, Madrid, 2004.

VIDAURRI ARÉCHIGA, Manuel: *Delitos informáticos. Los retos del Derecho Penal*, en: NAVA GARCÉS, Alberto Enrique (coord.): ***Ciberdelitos***, Tirant lo Blanch, Ciudad de México, 2019, 197-220.

WILFORD, Hugh: *America´s Great Game:* ***The CIA´s secret Arabist and the shaping of the modern middle east***, Basic Book, New York, 2013.

YUSTE GONZÁLEZ, Javier: *Irán 1966-1969*, en: Historia Rei Militaris: Historia militar, política y social, n.º 7, 2014, 114-117.

PÁGINAS *WEB*

https://escudodigital.com/ciberseguridad/el-ciberataque-de-israel-natanz-volvio-a-recurrir-al-gusano-stuxnet/?utm_source=mailpoet&utm_medium=email&utm_campaign=Newsletter+N%C2%BA81 (visitada el 20/04/2021).

https://www.researchgate.net/publication/253212482_The_Iranian_Letter_to_President_Bush_Analysis_and_Recommendations (visitada 23/04/2021).

https://www.iranchamber.com/history/coup53/coup53p1.php (visitada el 23/04/2021).

https://www.nti.org/learn/facilities/175/ (visitada el 24/04/2021).

https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits#:~:text=Zero%2Dday%20vulnerabilities%20are%20vulnerabilities,to%20information%20regarding%20known%20vulnerabilities. (visitada el 25/04/2021).

https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html (visitada el 25/04/2021).

https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra (visitada el 26/04/2021).

https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo (visitado el 26/04/2021).

https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf (visitada el 27/04/2021).

https://www.kaspersky.es/blog/que-es-una-apt/966/ (visitada el 27/04/2021).

https://www.bbc.com/mundo/noticias-internacional-48759280 (visitada el 28/04/2021).

https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/ (visitada el 28/04/2021).

https://www.scmp.com/news/world/article/1278286/nsa-israel-created-stuxnet-worm-together-attack-iran-says-snowden (visitada el 28/04/2021).

https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (visitada el 28/04/2021).

https://www.un.org/es/conferences/npt2020/background (visitada el 11/06/2021).

https://www.iaea.org/publications/documents/infcircs?field_infcirc_number_value=&field_infcirc_date_value%5Bvalue%5D%5Bdate%5D=&field_infcirc_country_tid%5B%5D=311 (visitada el 15/06/2021).

https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (visitada el 15/06/2021).

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf (visitada el 19/06/2021).

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008F0919&from=ES (visitada el 20/06/2021).

https://www.nytimes.com/2007/01/22/world/middleeast/22iran.html (visitada el 17/08/2021).

https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf (visitada el 18/08/2021).

https://www.nti.org/learn/countries/iran/nuclear/ (visitada 18/08/2021).

https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-80558 (visitada el 21/08/2021).

https://www.boe.es/buscar/act.php?id=BOE-A-2019-2363&p=20190221&tn=1 (visitada el 21/08/2021).

https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648 (visitada el 21/08/2021).

https://dle.rae.es/subvertir (visitada el 21/08/2021).

https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002F0475:20081209:ES:PDF (visitada el 21/08/2021).

https://www.un.org/spanish/law/icc/statute/spanish/rome_statute(s).pdf (visitada el 22/08/2021).

https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666 (visitada el 22/08/2021).

https://www.boe.es/buscar/doc.php?id=BOE-A-1991-25882 (visitada el 22/08/2021).

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221 (visitada el 22/08/2021).

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (visitada 05/09/2021).

https://as.com/meristation/2021/04/23/betech/1619175232_192867.html (visitada el 05/09/2021).

https://www.icrc.org/es/document/los-convenios-de-ginebra-de-1949-y-sus-protocolos-adicionales (visitada el 05/09/2021).

ANEXOS

ANEXO I

Fuente: https://www.elmundo.es/elmundo/2013/02/21/internacional/1361465446.html (visitada 27/04/2021). En esta imagen podemos ver al presidente de Irán paseando por entre las centrifugadoras a gas de la central de Natanz.

ANEXO II

Accesible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Stuxnet&search_type=all (visitada el 25/04/2021).

CVE-2011-3402	Vulnerabilidad no especificada en el motor de análisis de fuentes TrueType en win32k.sys en los controladores en modo kernel en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2 y R2 SP1 y Windows 7 Gold y SP1 permite a los atacantes remotos ejecutar código arbitrario a través de datos de fuentes elaborados en un documento de Word o página web, como lo explotó en la naturaleza en noviembre de 2011 por Duqu, también conocido como "Vulnerabilidad de análisis de fuentes TrueType". **Publicado:** 04 de noviembre de 2011; 5:55:05 PM -0400	*V3.x:* (no disponible) *V2.0:* 9.3 ALTA
CVE-2010-2743	Los controladores en modo kernel en Microsoft Windows XP SP3 no realizan correctamente la indexación de una tabla de puntero de función durante la carga de diseños de teclado desde el disco, lo que permite a los usuarios locales obtener privilegios a través de una aplicación diseñada, como se demostró en la naturaleza en julio de 2010 por el gusano Stuxnet, también conocido como "Win32k Keyboard Layout Vulnerability". NOTA: esto puede ser un duplicado de CVE-2010-3888 o CVE-2010-3889. **Publicado:** 20 de enero de 2011; 4:00:01 PM -0500	*V3.x:* (no disponible) *V2.0:* 7.2 ALTA
CVE-2010-3889	La vulnerabilidad no especificada en Microsoft Windows en plataformas de 32 bits permite a los usuarios locales obtener privilegios a través de vectores desconocidos, como los explotó en estado salvaje en julio de 2010 el gusano Stuxnet e identificados por investigadores de Microsoft y otros investigadores. **Publicado:** 08 de octubre de 2010; 6:00:37 PM -0400	*V3.x:* (no disponible) *V2.0:* 7.2 ALTA
CVE-2010-3888	La vulnerabilidad no especificada en Microsoft Windows en plataformas de 32 bits permite que los usuarios locales obtengan privilegios a través de vectores desconocidos, como los explotó en estado salvaje en julio de 2010 el gusano Stuxnet e identificados por los investigadores de Kaspersky Lab y otros investigadores. **Publicado:** 08 de octubre de 2010; 6:00:37 PM -0400	*V3.x:* (no disponible) *V2.0:* 7.2 ALTA
CVE-2010-2772	El sistema Siemens Simatic WinCC y PCS 7 SCADA utiliza una contraseña codificada, que permite a los usuarios locales acceder a una base de datos back-end y obtener privilegios, como lo demostró en la naturaleza en julio de 2010 el gusano Stuxnet, una vulnerabilidad diferente a CVE-2010 -2568. **Publicado:** 22 de julio de 2010; 1:43:58 AM -0400	*V3.x:* (no disponible) *V2.0:* 6.9 MEDIO
CVE-2010-2568	Windows Shell en Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 y SP2, Server 2008 SP2 y R2, y Windows 7 permite a los usuarios locales o atacantes remotos ejecutar código arbitrario a través de un (1) .LNK o (2) .PIF diseñado archivo de acceso directo, que no se maneja correctamente durante la visualización de iconos en el Explorador de Windows, como se demostró en la naturaleza en julio de 2010, y originalmente reportado para malware que aprovecha CVE-2010-2772 en sistemas Siemens WinCC SCADA. **Publicado:** 22 de julio de 2010; 1:43:49 AM -0400	*V3.x:* (no disponible) *V2.0:* 9.3 ALTA

ANEXO III

Fuente: https://www.bbc.com/mundo/noticias-47308687 (visitada 26/04/2021).