ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

42/2013 7 mayo de 2013

Xavier Servitja Roca

CIBERSEGURIDAD, CONTRAINTELIGENCIA Y OPERACIONES ENCUBIERTAS EN EL PROGRAMA NUCLEAR DE IRÁN: DE LA NEUTRALIZACIÓN SELECTIVA DE OBJETIVOS AL "CUERPO CIBER" IRANÍ*

CIBERSEGURIDAD, CONTRAINTELIGENCIA Y OPERACIONES ENCUBIERTAS EN EL PROGRAMA NUCLEAR DE IRÁN: DE LA NEUTRALIZACIÓN SELECTIVA DE OBJETIVOS AL "CUERPO CIBER" IRANÍ*

Resumen:

Este documento se centra en describir las operaciones encubiertas y de contrainteligencia más destacadas en relación al programa nuclear iraní desde que el presidente de la República Islámica de Irán, Mahmud Ahmadineyad, anunciara la reanudación del mismo en el año 2006 hasta nuestros días y que abarcan desde la neutralización selectiva de objetivos al desmantelamiento de redes de espías, pasando por los ciberataques y el uso de Vehículos Aéreos No Tripulados (VANT). En el mismo, se remarca de forma especial el creciente papel que adquiere el ciberespacio en este tipo de operaciones siendo uno de sus resultados directos la creación de la unidad de ciberseguridad iraní una vez detectado en 2010 el ciberataque del *malware* Stuxnet que afectó a su central de enriquecimiento de uranio de Natanz.

Abstract:

This paper is focused on the most relevant covert actions and counterintelligence operations regarding Iran's nuclear program since Iranian president Ahmadineyad announced its resumption in 2006 until today, from the selective neutralization of targets to the dismantling of spy rings, through cyber-attacks and the use of Unmanned Aerial Vehicles (UAV). This paper also pays special attention to the growing role of cyberspace in these operations. One of the direct results has been the creation of the Iranian Cyber security Unit by Iran after detecting in 2010 the malware Stuxnet cyberattack that hits its uranium enrichment plant in Natanz.

CIBERSEGURIDAD, CONTRAINTELIGENCIA Y OPERACIONES ENCUBIERTAS EN EL PROGRAMA NUCLEAR DE IRÁN: DE LA NEUTRALIZACIÓN SELECTIVA DE OBJETIVOS AL "CUERPO CIBER" IRANÍ*

Xavier Servitja Roca

Palabras clave:

R. I. de Irán, Programa nuclear iraní, Servicios de Inteligencia, Contrainteligencia, Operaciones Encubiertas, Ciberseguridad, Ciberataques, Ciberespionaje, el VEWAK, QUDS, Hezbollah, el Mossad, la CIA, VANT.

Keywords:

I. R. of Iran, Iran's Nuclear Program, Intelligence Service, Counter-Intelligence, Cyber security, Cyber-attacks, Cyber espionage, Covert Actions, VEWAK, QUDS, Hezbollah, Mossad, CIA, UAV.

* Desde el principio, es preciso aclarar que no existen pruebas reales ni concluyentes para atribuir la autoría de la mayoría de acciones y hechos descritos en este documento a personas físicas, actores no estatales o a determinados servicios de inteligencia o Estados. Por ello, se hablará casi siempre de presuntos autores materiales.

Xavier Servitja Roca

INTRODUCCIÓN

El pasado 12 de marzo de 2013, el director de la Inteligencia Nacional estadounidense, James R. Clapper, presentó ante la Comisión de Inteligencia del Senado de Estados Unidos el informe sobre la evaluación de las amenazas mundiales que realizan conjuntamente las diecisiete agencias y organizaciones que conforman la comunidad de inteligencia del Estado norteamericano[1]. De dicho documento cabría resaltar dos temas que sobresalen por encima de los demás y que serán conectados en este documento: el programa nuclear iraní y la ciberseguridad.

Respecto a la ciberseguridad, el informe del año 2013 señala a los ciberataques y al ciberespionaje como la mayor amenaza a la que deberá enfrentarse Estados Unidos. Para resaltar la importancia de este asunto, se citan algunos ejemplos como el ciberataque a través de Denegación de Servicio (DDS) que sufrieron algunas webs de bancos y mercados de cambio estadounidenses en el último año, así como el que afectó a la mayor empresa de Arabia Saudí también en 2012, Saudi Aramco. En ambas acciones, oficiales de Estados Unidos y expertos informáticos sospechan que Irán podría ser el presunto instigador y ejecutor de las mismas como represalia al régimen de sanciones que le es impuesto por Estados Unidos y otros actores internacionales por el desarrollo de su programa nuclear[2].

Y es que el régimen de los ayatolás, tras descubrir en 2010 que había sufrido el ciberataque Stuxnet en la instalación de Natanz, perteneciente a su programa nuclear, dentro de una operación encubierta supuestamente ideada por Estados Unidos e Israel y ejecutada por este último Estado con el objetivo de ralentizarlo, ha iniciado en estos dos últimos años un rápido desarrollo de sus capacidades en ciberseguridad tanto para acciones de ciberdefensa, como para llevar a cabo ciberataques.

Precisamente y en relación al ciberataque a la empresa Saudi Aramco, el 20 de marzo de 2013 un portavoz del ministerio del Interior de Arabia Saudí anunció la detención de un iraní, un libanés y dieciséis saudíes, todos chiíes y algunos de ellos trabajadores de la propia compañía Aramco, acusados de formar parte de una presunta red de espionaje al servicio de

[1] CLAPPER James R., "Worldwide Threat Assessment of the US Intelligence Community", *Office of the Director of National Intelligence*, 12 de marzo de 2013, disponible en http://intelligence.senate.gov/130312/clapper.pdf. Fecha de la consulta 13.03.2013.

[2] PERLROTH Nicole, HARDY Quentin, "Bank hacking was the work of Iranians, officials says", The New York Times (08.01.2013), disponible en http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=0&pagewanted=all. Fecha de la consulta 11.04.2013 y PERLROTH Nicole, "In cyberattack on Saudi firm, U.S. sees Iran firing back", The New York Times (23.12.2012), disponible en http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all. Fecha de la consulta 11.04.2013.

Irán[3]. Este hecho, desmentido por el portavoz del ministerio de exteriores iraní, Ramin Mehmanparast, coincide en el tiempo con la presentación por parte del fiscal general de Teherán de cargos contra dieciocho personas acusadas de colaborar y participar entre los años 2007 y 2012 en los asesinatos de 5 científicos nucleares iraníes relacionados con su programa nuclear, asesinatos que Irán atribuye a los servicios de inteligencia británico, estadounidense e israelí[4].

Y es que el programa nuclear iraní, definido como el Santo Grial de la comunidad de inteligencia por el experto en seguridad internacional y diplomacia Julian Borger (The Guardian)[5], sigue siendo un escenario propicio para el desarrollo de operaciones encubiertas y de contrainteligencia tanto para los actores que se opondrían al mismo y quisieran frenarlo, caso de Estados Unidos, Israel, Gran Bretaña o Arabia Saudí, entre otros, como para Irán y su representante en Líbano, Hezbollah, que lo intentan defender, mientras que al mismo tiempo se buscan otras vías de solución al conflicto ya sea a través de políticas de compromiso con el uso de la diplomacia y la negociación como serían los casos del formato del P5+1 con Irán o dentro de las reuniones del Organismo Internacional de la Energía Atómica en su sede en Viena; de políticas de contención con la aplicación de regímenes de sanciones; o de una política de prevención a través de una intervención militar como viene reclamando el reelecto primer ministro israelí, Benjamin Netanyahu.

Sin embargo y paralelamente a estas otras políticas de seguridad, las operaciones encubiertas y de contrainteligencia siguen realizándose y en las mismas, la utilización del ciberespacio y de los "drones" está ganando terreno frente a otro tipo de operativos como la neutralización selectiva de objetivos o el sabotaje por suministro de piezas defectuosas o por colocación de explosivos en determinadas instalaciones claves para el desarrollo del programa.

Por todo este conjunto de factores citados, en este documento se pretende describir las operaciones encubiertas y de contrainteligencia más importantes relacionadas con el programa nuclear iraní desde que este fuera reactivado en 2006 hasta nuestros días, dando especial énfasis al papel que va adquiriendo el ciberespacio y la ciberseguridad en las mismas y sin olvidar el contexto en el cual se desarrollan: la doble rivalidad Irán-Israel e Irán-

[3] AL ARABIYA, "Espionage ring in Saudi Arabia linked to Iran: interior ministry", Al Arabiya (26.03.2013), disponible en http://english.alarabiya.net/en/2013/03/26/Espionage-ring-in-Saudi-Arabia-linked-to-Iran-interior-ministry.html. Fecha de la consulta 26.03.2013.

[4] PRESS TV, "Iran to try 18 over nuclear assassinations", Press TV (17.03.2013), disponible en http://www.presstv.ir/detail/2013/03/17/294041/iran-to-try-18-over-nassassinations/. Fecha de la consulta 24.03.2013.

[5] BORGER Julian, "Iran's nuclear programme: the holy grail of the intelligence world", The Guardian (10.12.2012), disponible en http://www.guardian.co.uk/world/2012/dec/10/iran-nuclear-programme-holy-grail?CMP=twt_gu. Fecha de la consulta 13.03.2013.

Arabia Saudí en la llamada Guerra Fría regional. Al mismo tiempo y a través de esta descripción, también se analizará si dichas operaciones han logrado alcanzar el objetivo propuesto: ralentizar o acabar con el desarrollo del programa nuclear iraní.

Para ello, en primer lugar se realizará una breve definición de lo que se entiende por contrainteligencia, operación encubierta y varios conceptos clave de la ciberseguridad para, a continuación, describir y analizar algunos casos prácticos de los mismos aplicados al conflicto nuclear iraní.

DEFINICIÓN DE LOS CONCEPTOS

En este apartado y de forma breve, se introducen los conceptos de contrainteligencia y operaciones encubiertas, al mismo tiempo que se describen los conceptos básicos referidos a la dimensión del ciberespacio que se tratan en este documento.

En primer lugar, la Contrainteligencia[6] es la necesidad de conocer para proteger y preservar la fuerza militar, económica y otros sectores productivos, incluida la seguridad del gobierno en los asuntos internos y externos, frente al espionaje, sabotaje y otras formas de actividad clandestina designadas para debilitar o destruir un Estado.

Las funciones de la contrainteligencia van desde el ámbito defensivo, con la protección de secretos para la seguridad nacional e impedir que otros servicios de inteligencia los obtengan, entre otros; hasta la dimensión ofensiva o de contraespionaje, que busca identificar al adversario y conocer todo lo que hay que saber tanto de los servicios de inteligencia amigos como enemigos, además de realizar funciones de reclutamiento e infiltración u operaciones de desinformación, entre otras muchas.

En lo referente a las Operaciones Encubiertas[7], son aquellas actividades impulsadas por un Estado para influenciar las condiciones políticas, económicas o militares en el exterior y en las que se pretende que el papel del mismo no sea reconocido públicamente. Es más, ese Estado siempre negará cualquier acusación de estar detrás de la operación. En este sentido, las operaciones encubiertas se realizan porque se cree que son el mejor procedimiento para

---

[6] Información extraída de: EHRMAN John, "What are we talking about when we talk about Counterintelligence?", *Studies in Intelligence*, vol. 53, nº 2, June 2009, 5-20, disponible en https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/pdfs/U-%20UnclassStudies%2053-2.pdf. Fecha de la consulta 14.03.2013 y JOHNSON Loch, WIRTZ James, *Strategic Intelligence: Windows into a secret world*, Los Ángeles, Roxbury, 2004, 287-293 y 304-314.

[7] Información extraída de: JOHNSON Loch, WIRTZ James, *Strategic Intelligence: Windows into a secret world*, Los Ángeles, Roxbury, 2004, 253-285 y JOHNSON Loch, "Sketches for a Theory of Strategic Intelligence", *Intelligence Theory*, cap. 3, 33-53.

lograr un fin deseado o un objetivo político específico. Para ello, se utilizan instrumentos que van desde la propaganda hasta las operaciones paramilitares, pasando por el entrenamiento de equipos o, incluso, acciones de asesinato.

Finalmente y en relación al ciberespacio, entendido como el dominio global y dinámico compuestos por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de información[8], se definen los conceptos de ciberseguridad, ciberataque, ciberdefensa y ciberespionaje sin entrar en los cinco grandes debates que actualmente se producen respecto al ciberespacio en términos de defensa y seguridad[9]. Estos conceptos son concebidos en este documento en su dimensión instrumental para ser empleados en operaciones encubiertas y en contrainteligencia.

Así, la ciberseguridad es el conjunto de actividades centradas en mecanismos defensivos (ciberdefensa) y ofensivos (ciberataques) empleados tanto para proteger el ciberespacio contra el uso indebido del mismo, defender su infraestructura tecnológica, los servicios que prestan y la información que manejan; como para utilizar las capacidades del ciberespacio como arma de ataque por razones de seguridad o actividad militar. En esta dirección, la ciberseguridad se puede utilizar para propósito de espionaje, de sabotaje o de subversión, entre otras actividades[10].

En lo referente a la ciberdefensa y con más detalle, es el conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control del conjunto de actividades que se realizan utilizando el ciberespacio. Para ello, se usan instrumentos como los cortafuegos o *firewalls* para bloquear accesos no autorizados;

---

[8] Algunas definiciones en: Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, *BOD* de 26 de febrero de 2013, disponible en http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf. Fecha de la consulta 15.03.2013.

[9] El primer gran debate se produce entre los "Ciberalarmistas" y los "Ciberescépticos" y gira entorno a si realmente la amenaza ciber es tan importante como se pretende hacer creer o no; un segundo debate se centra en si es correcto emplear el término "Ciberguerra" porque para ello se debería interpretar un ciberataque como "uso de la fuerza" y no todos los expertos están de acuerdo en catalogarlo así, además de no cumplir la definición clásica de acto de Guerra de Clausewitz; el tercero es si a este ciberataque se le puede aplicar la teoría de la Guerra Justa para iniciar una guerra (jus ad bellum) por la dificultad de identificar al atacante y de definirlo como ataque armado intencionado, además de cómo proceder ante una ciberguerra (jus in bello); otro debate tiene como protagonista a la teoría de la disuasión clásica (nuclear) y si ésta es aplicable a la dimensión del ciberespacio o no son comparables; finalmente, el quinto debate se refiere a cómo aplicar la normativa internacional para regular y controlar las actividades del ciberespacio al considerarse un área gris en Derecho Internacional.

[10] RID Thomas, "Cyber War will not take place", *The Journal of Strategic Studies*, vol. 35, nº 1, febrero 2012, 15, disponible en http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939. Fecha de la consulta 20.03.2013 y MEYER Paul, "Cyber-security through arms control", *The RUSI Journal*, vol. 156, nº 2, abril-mayo 2011, 22, disponible en http://www.tandfonline.com/doi/pdf/10.1080/03071847.2011.576471. Fecha de la consulta 20.03.2013.

tecnología de detección; o los llamados *honey pots* u otras trampas que sirvan de distracción y para conseguir información sobre el *modus operandi* del atacante, entre otros muchos[11].

En cuanto a los ciberataques, se pueden definir como las acciones que utilizan el ciberespacio para penetrar, afectar, modificar, causar daños o destruir a los sistemas modernos de información digital en computadoras o sistemas de computadoras, software, hardware u operaciones de los sistemas de información y telecomunicación[12]. Para tal objetivo, los ciberataques utilizan malware o software malicioso, como virus, worm o troyanos, además de la Denegación de Servicio (DDS), entre otros.

Existen tres tipos de ciberataques: el primero de ellos son los ciberataques perturbadores que intentan inutilizar o tomar el control de los sistemas informáticos de infraestructuras críticas como el SCADA (Supervisory Control and Data Acquisition)[13]. Este tipo de ciberataque, a diferencia de las otras dos categorías, busca causar daño físico, funcional o mental a estructuras, sistemas y personas físicas. En segundo lugar, existen los ciberataques no intrusivos que usan instrumentos como la DDS para bloquear accesos o la desfiguración de webs con el propósito de cambiar contenidos. Finalmente, los ciberataques intrusivos son aquellos cuyo objetivo se centra en los datos, ya sea para obtenerlos utilizando *malware* Info-stealer ("ladrón de información"), o para alterar la información[14]. Este último tipo es el utilizado por el ciberespionaje, entendido como el intento de penetrar en un sistema adversario con el propósito de extraer información protegida o sensible que pueda ser utilizada tanto para planificar instrumentos defensivos como ofensivos[15]. Esta es una de las actividades principales de los ciberataques apoyada supuestamente por los Estados.

[11] En: Orden Ministerial 10/2013, op. cit. y FARWELL James, ROHOZINSKI Rafal, "The new reality of Cyber War", *Survival*, vol. 54, nº4, agosto-septiembre 2012, 109, disponible en http://www.tandfonline.com/doi/pdf/10.1080/00396338.2012.709391. Fecha de la consulta 20.03.2013.

[12] En: Orden Ministerial 10/2013, op. cit. y DIPERT Randall, "The ethics of cyberwarfare", *Journal of Military Ethics*, vol.9, nº 4, 2010, 386-388, disponible en http://www.tandfonline.com/doi/pdf/10.1080/15027570.2010.536404. Fecha de la consulta 20.03.2013.

[13] SCADA es el sistema usado para monitorizar y controlar procesos en instalaciones industriales y empresas públicas, como plantas químicas, centrales eléctricas, refinerías, oleoductos de gas y petróleo, entre otros, en: ROSENFIELD Daniel, "Rethinking Cyber War", Critical Review, vol. 21, nº 1, 2009, 77-78, disponible en http://www.tandfonline.com/doi/pdf/10.1080/08913810902812156. Fecha de la consulta 20.03.2013.

[14] DIPERT, op. cit.

[15] RID, op. cit, 20.

CONTRAINTELIGENCIA, OPERACIONES ENCUBIERTAS Y CIBERSEGURIDAD EN EL PROGRAMA NUCLEAR IRANÍ

Principales actores estatales y no estatales implicados

Los principales actores estatales y no estatales supuestamente implicados en operaciones encubiertas y actividades de contrainteligencia en relación al programa nuclear iraní y que, al mismo tiempo, algunos de ellos actuarían dentro del contexto de rivalidad entre las potencias regionales por mantener y ampliar su esfera de influencia y convertirse en el "hegemón" regional, estarían divididos en dos grandes bloques:

El primero de ellos agruparía a aquellos Estados opuestos al programa nuclear iraní y que utilizarían las operaciones encubiertas y la contrainteligencia para frenarlo. Su objetivo a través de estos medios e instrumentos sería ralentizar o parar la ambición nuclear de la república teocrática mientras otras políticas de seguridad más visibles solucionen el conflicto nuclear iraní. Como se detallará más adelante, en este grupo de actores participarían supuestamente y de manera activa Estados Unidos, Gran Bretaña e Israel con sus respectivas agencias de inteligencia competentes para ello, la Central Intelligence Agency (CIA) estadounidense junto a la National Security Agency, entre otras; el Secret Intelligence Service (SIS-MI6) británico; y el Mossad israelí, destacando su unidad Kidon. Además, también se debería incluir en estas operaciones a unidades especiales dentro de las Fuerzas Armadas de cada uno de los Estados como es el caso de la Unidad Militar 8200 de las Fuerzas de Seguridad de Israel (IDF-Tzahal).

Pero tal y como declaraba Ilan Mizrahi, ex director del Consejo Nacional de Seguridad israelí y ex subdirector del Mossad en el gobierno de Ehud Olmert, en esta guerra secreta habría más participantes y nadie actuaría por su cuenta[16], llámese Azerbaiyán, Estado que en más de una ocasión ha recibido acusaciones por parte de Irán de ayudar al Mossad a realizar operaciones encubiertas en suelo iraní[17], o los estados miembros del Consejo de

[16] MOSCOVITCH, Ben, "Interview with Ilan Mizrahi, part 1: Iran", *Foreign Policy Association*, 17 de enero de 2011, disponible en http://foreignpolicyblogs.com/2011/01/17/exclusive-interview-with-ilan-mizrahi-part-1-iran/. Fecha de la consulta 28.03.2013 y GÓNZALEZ Enric, "Un exsubdirector del Mosad sugiere la implicación israelí en el atentado de Irán", El País (11.01.2012), disponible en http://internacional.elpais.com/internacional/2012/01/11/actualidad/1326306296_633894.html. Fecha de la consulta 28.03.2013.

[17] BBC NEWS, "Azerbaijan in row with Iran over 'israeli spies'", BBC News (13.02.2012), disponible en http://www.bbc.co.uk/news/world-europe-17015238. Fecha de la consulta 28.03.2013 y HAARETZ, "Azerbaijan granted Israel access to air bases on Iran border", Haaretz (29.03.2012), disponible en http://www.haaretz.com/news/diplomacy-defense/azerbaijan-granted-israel-access-to-air-bases-on-iran-border-1.421428. Fecha de la consulta 28.03.2013 y REUTERS "Azerbaijan mulls helping Israel with Iran attack", Haaretz (30.09.2012), disponible en http://www.haaretz.com/news/diplomacy-defense/sources-azerbaijan-mulls-helping-israel-with-iran-attack-1.467628. Fecha de la consulta 28.03.2013.

Cooperación del Golfo (CCG) con Arabia Saudí y su servicio de inteligencia exterior del Istakhbarat, también conocido como General Intelligence Directorade (GID), a la cabeza. De hecho, los servicios de inteligencia y las agencias nacionales de seguridad de los miembros del CCG llevan ya años cooperando y coordinando esfuerzos frente a un posible conflicto con Irán. Sobre todo, este trabajo se hace evidente en temas de inteligencia interior y contrainteligencia para detectar redes de espías iraníes e informadores dentro de las comunidades chiitas que hay en sus territorios.

Además, estas operaciones encubiertas, así como los trabajos de contrainteligencia estarían apoyadas por actores no estatales pertenecientes a grupos opositores o minorías étnicas tanto dentro como fuera del territorio iraní. De todos ellos, cabría destacar a los grupos ligados a la minoría kurda; a la minoría árabe, los Ahwazis; a los separatistas azeríes; al bloque opositor de los Muyahidines del Pueblo (MEK), que en septiembre de 2012 fue sacada de la lista de organizaciones terroristas de Estados Unidos[18]; o los separatistas suníes del grupo terrorista Yundallah de la región de Sistán y Baluchistán y con bases también en Pakistán[19]. En el caso de Yundallah, se produjo un conflicto entre los servicios de inteligencia estadounidenses e israelíes al conocerse que agentes del Mossad realizaron una operación de "False Flag" haciéndose pasar por oficiales de la CIA con el propósito de reclutar operativos del grupo terrorista suní para sus operaciones encubiertas dentro de Irán[20]. Incluso se llegaron a realizar reuniones entre miembros de Yundallah y los "falsos" agentes de la CIA en Londres. Cabe mencionar también que Irán ha acusado en algunas ocasiones al servicio de inteligencia pakistaní, el Inter-Service Intelligence (ISI), de dar apoyo y cobertura a dicho grupo terrorista[21].

Respecto al segundo bloque y en el lado opuesto, se situaría a Irán, cuyo objetivo a través de las operaciones encubiertas y la contrainteligencia no sólo es el de salvaguardar el desarrollo de su programa nuclear frente a posibles ataques contra el mismo, incluso tomando represalias contra los actores presuntamente implicados si se llegan a producir, sino también el de afianzar las áreas de influencia del régimen de los ayatolás. En este sentido y como se citará en los siguientes apartados, el Ministerio de Inteligencia y Seguridad Nacional iraní y su servicio de inteligencia del VEVAK (Vezarat-e Ettela'at va Amniat-e Keshvar), así como la

---

[18] SHANE Scott, "Iranian dissidents convince U.S. to drop terror label", The New York Times (21.09.2012), disponible en http://www.nytimes.com/2012/09/22/world/middleeast/iranian-opposition-group-mek-wins-removal-from-us-terrorist-list.html?pagewanted=all&_r=0. Fecha de la consulta 28.03.2013.

[19] HISPAN TV, "Irán desmantela una célula terrorista afiliada a Yundullah", Hispan TV (10.04.2012), disponible en http://www.hispantv.com/detail.aspx?id=178371. Fecha de la consulta 28.03.2013.

[20] PERRY, Mark, "False Flag", *Foreign Policy*, 13 de enero de 2012, disponible en http://www.foreignpolicy.com/articles/2012/01/13/false_flag. Fecha de la consulta 28.03.2013.

[21] Press TV, "New Jundallah ringleader meets ISI agent in Pakistan", Press TV (02.06.2012), disponible en http://www.presstv.ir/detail/244255.html?utm_source=dlvr.it&utm_medium=twitter. Fecha de la consulta 28.03.2013.

Organización de la Ciberseguridad de las Fuerzas Armadas iraníes juegan un importante papel en estos operativos, conjuntamente con la unidad QUDS dirigida por el comandante en jefe Qasem Soleimani y encargada de las operaciones exteriores de los Cuerpos de la Guardia Revolucionaria Islámica (CGRI) a la que pertenecen, además del apoyo que se recibe del representante iraní en Líbano, Hezbollah. Precisamente, se debería remarcar que uno de los grandes éxitos de los servicios de inteligencia iraníes y de los QUDS ha sido la construcción de este tipo de alianzas y de redes de informadores entre las comunidades chiitas exteriores.

Contrainteligencia y operaciones encubiertas más destacadas

En una primera parte se explican algunas operaciones encubiertas tales como la neutralización selectiva de objetivos, sabotajes y desapariciones que serían atribuibles a los actores contrarios al programa nuclear iraní, así como algunos episodios de contrainteligencia a través del reclutamiento o desmantelamiento de redes de espías. Al mismo tiempo, se detallan las actividades iraníes y algunas de sus presuntas respuestas frente a operaciones encubiertas recibidas. Una segunda parte se dedica exclusivamente tanto a la dimensión del ciberespacio de estos operativos, como a la utilización de VANT y la ofensiva electrónica, actividades que progresivamente van ganando terreno y, al mismo tiempo, significan una evolución dentro del campo de las operaciones encubiertas y de contrainteligencia.

De la neutralización selectiva de objetivos a la desarticulación de redes de espías[22]

Dentro de las operaciones encubiertas que han salido a la luz y que habrían sido llevadas a cabo por el bloque contrario al programa nuclear iraní en el periodo de estudio, destacaría la neutralización selectiva de objetivos de especial relevancia, como sería el caso de científicos iraníes relacionados con el desarrollo del programa. Así, un primer caso se daría en el año 2007 cuando Ardeshir Hassanpour, científico empleado en la planta de Esfahan, muere por envenenamiento con material radioactivo. Sin embargo, no es hasta enero de 2010 cuando vuelve a realizarse otra acción de este tipo. En esta ocasión, el físico nuclear Masoud Ali Mohammadi es asesinado con un IED adosado a una moto que fue detonada a su paso. El ataque supuestamente fue perpetrado por el joven iraní, Majid Jamali Fashi, que habría sido captado por el Mossad y habría dado detalles de su entrenamiento durante el interrogatorio al cual fue sometido. Jamil fue sentenciado a muerte y ahorcado en mayo de 2012[23].

[22] Agradecimiento a Ainhoa Amo, periodista, y Fátima Molina, historiadora.

[23] COWELL Alan, "Iran executes man accused as Israeli spy and assassin", The New York Times (15.05.2012), disponible en http://www.nytimes.com/2012/05/16/world/middleeast/iran-executes-alleged-israeli-spy.html. Fecha de la consulta 27.03.2013.

En el mismo año, concretamente el 29 de noviembre de 2010, Majid Shahriari, profesor de física nuclear de la Universidad Shahid Beheshti sufre un atentado con una bomba magnética adosada a su coche por un motociclista que le provoca la muerte. Se da la circunstancia que Shahriari habría sido detectado una semana antes por el Mossad en Damasco (Siria), donde hacía escala de un vuelo procedente de Corea del Norte rumbo a Teherán. También en el mismo día y con el mismo *modus operandi* se intenta acabar con la vida de Fereidoun Abbasi, experto nuclear y actual responsable de la Organización de la Energía Atómica iraní. Estos ataques serían atribuidos a la unidad Kidon del Mossad[24].

Finalmente, los dos últimos hechos tienen lugar el 23 de julio de 2011 y el 11 de enero de 2012 respectivamente en Teherán, cuando varios disparos acaban con la vida del físico iraní Darioush Rezaei y cuando Mustafá Ahmadi Roshan, ingeniero químico y supervisor del programa de enriquecimiento de uranio de la planta de Natanz, muere como consecuencia de un atentado con el método de la bomba magnética, ambas acciones también presuntamente atribuidas a operativos de la unidad Kidon[25].

La neutralización selectiva de objetivos iría acompañada de otro tipo de operaciones encubiertas como el sabotaje de instalaciones por detonación de explosivos. Una primera muestra de ello sucedería el 12 de noviembre de 2011 cuando una fuerte explosión sacude una base de los CGRI cerca de Teherán encargada del desarrollo del programa de misiles balísticos. El presunto atentado provoca 17 muertos, entre ellos Hasan Moghaddam, un alto comandante de los CGRI responsable de dicho programa. Otra explosión similar aunque no confirmada tiene lugar el día 28 del mismo mes en la ciudad de Esfahan, conocida porque en ella hay instalaciones relacionadas con el programa nuclear y donde viven un gran número de militares y científicos iraníes[26].

Dentro de las operaciones encubiertas también se producirían episodios de desapariciones o presuntas deserciones siendo el ejemplo más destacado el del general retirado de los CGRI, Ali Reza Asgari, que también ocupó el cargo de viceministro de Defensa iraní en el gobierno anterior de Mohammad Khatami y que desapareció en el año 2007 en Estambul (Turquía). Sobre este episodio existen versiones contradictorias. Por un lado, Irán siempre ha acusado

[24] GORDON, Thomas, "Mossad: was this the chief's last hit?", The Telegraph, (05.12.2010), disponible en http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8182126/Mossad-was-this-the-chiefs-last-hit.html. Fecha de la consulta 28.03.2013.

[25] VICK Karl, KLEIN Aaron, "Who assassinated an Iranian nuclear scientist? Israel isn't telling", Time (13.01.2012), disponible en http://www.time.com/time/world/article/0,8599,2104372,00.html. Fecha de la consulta 28.03.2013.

[26] PETERSON Scott, "Did Israel assassinate Iran's 'missile king'?", The Christian Science Monitor (14.11.2011), disponible en http://www.csmonitor.com/World/Middle-East/2011/1114/Did-Israel-assassinate-Iran-s-missile-king. Fecha de la consulta 11.04.2013 y KAMALI Saeed, "Iran: explosion in Isfahan reported", The Guardian (28.11.2011), disponible en http://www.guardian.co.uk/world/2011/nov/28/isfahan-explosion-report-iran-nuclear-facilities. Fecha de la consulta 11.04.2013.

al Mossad de haberlo secuestrado y transferido a la prisión israelí de Ayalon, donde supuestamente murió en diciembre de 2010 (por suicidio o ejecución)[27]. Sin embargo, otras fuentes señalan que Asgari habría desertado rumbo a Estados Unidos, donde habría proporcionado información a los servicios de inteligencia estadounidenses sobre el programa nuclear y sobre las conexiones entre Irán y Hezbollah[28].

Por su parte, Irán presuntamente ha respondido a este conjunto de acciones con una serie de operaciones encubiertas llevadas a cabo por sus operativos exteriores y su representante libanés Hezbollah. Así, un primer ejemplo sucedería el 26 de mayo de 2011 en Estambul (Turquía) cuando una bomba es detonada al paso de un coche consular israelí sin causar víctimas mortales. El siguiente episodio tendría lugar en Estados Unidos el 11 de octubre de 2011, cuando el departamento de Justicia estadounidense informa de la detención de dos ciudadanos iraníes en Nueva York acusados presuntamente de preparar el asesinato del embajador de Arabia Saudí, Adel al-Jubeir[29]. Este hecho sí provocó la visita del jefe del ministerio de Inteligencia iraní, Heidar Moslehi, a Riyhadh en diciembre de 2011 para reunirse con el ministro de Interior saudí y el director de la inteligencia saudí de aquel entonces, el príncipe Muqrin bin Abdulaziz, para negar los hechos. Anteriormente a la visita, Arabia Saudí había acusado a Irán de estar detrás del intento de atentado[30]. Precisamente en un Estado vecino, Bahréin, un IED explota el 4 de diciembre de 2011 cerca de la embajada británica de Manama sin provocar daños personales.

Otra cadena de operaciones encubiertas presuntamente dirigidas por elementos de los QUDS tiene lugar en Tiblisi (Georgia), Nueva Deli (India) y Bangkok (Tailandia) entre el 13 y el 14 de febrero de 2012, un mes después del asesinato del científico iraní Ahmadi Roshan[31]. En las dos primeras localidades se atenta contra diplomáticos israelíes con el método de las bombas magnéticas, mientras que en la capital tailandesa, un grupo de iraníes son detenidos tras una explosión ocurrida en su piso alquilado cuando manipulaban explosivos y del cual estaban huyendo con bombas magnéticas que detonaron a la llegada de la policía. A pesar de no causar víctimas mortales en ninguna de las tres acciones y de ser cierta su atribución,

[27] PRESS TV, "Asgari abducted, transferred to Israel by Mossad", Press TV (15.12.2012), disponible en http://www.presstv.ir/detail/2012/12/15/278254/asgari-abducted-by-mossad-iran-cmdr/. Fecha de la consulta 29.03.2013.

[28] KALMAN Aaron, "Iran claims Mossad kidnapped Tehran official with Hezbollah ties", The Times of Israel (16.12.2012), disponible en http://www.timesofisrael.com/iran-claims-mossad-kidnapped-tehran-official-with-hezbollah-ties/. Fecha de la consulta 29.03.2013.

[29] VICK Karl, "The shadow war between Iran and Israel: the Bulgaria front", Time (07.02.2013), disponible en http://world.time.com/2013/02/07/the-shadow-war-between-iran-and-israel-the-bulgaria-front/. Fecha de la consulta 30.03.2013.

[30] KNICKMEYER Ellen, "Iran, Saudi officials hold rare talks", The Wall Street Journal (14.12.2011), disponible en http://online.wsj.com/article/SB10001424052970203518404577096031404782816.html. Fecha de la consulta 30.03.2013.

[31] VICK, "The shadow war…", op. cit.

las mismas vendrían a demostrar la capacidad de respuesta, acción y coordinación de los efectivos iraníes en cualquier punto geográfico.

Mención aparte merece el atentado atribuido a Hezbollah que tuvo lugar en la ciudad búlgara de Burgas, donde el 18 de julio de 2012 un presunto suicida detono un explosivo cerca de un autobús de turistas causando la muerte a ocho personas, entre ellas cinco ciudadanos israelíes. A principios de febrero de 2013, una investigación del atentado llevada a cabo por el actualmente dimitido gobierno de Bulgaria dictaminó la relación de Hezbollah con el mismo, aunque los propios partidos de la oposición búlgara denunciaron tanto la falta de pruebas para tal afirmación, como la presión ejercida por Israel para dictaminar la culpabilidad de Hezbollah con el objetivo de presionar a la Unión Europea para que sea incluida en su lista de organizaciones terroristas[32].

Finalmente, en Chipre el miembro de Hezbollah, Hossam Taleb Yaccoub, es detenido días después del atentado de Burgas y condenado a tres años de prisión por un tribunal chipriota el pasado 28 de marzo de 2013 acusado de preparar ataques contra turistas israelíes en la isla. Estos cargos son negados por el miembro de Hezbollah, aunque sí admite su trabajo como informador para el grupo chiita libanés[33].

En lo referente a contrainteligencia propiamente dicha, *destacarían* las operaciones de reclutamiento, de incentivación de deserciones, desinformación y de desarticulación de presuntas redes de espías entre las filas del bloque enemigo.

Sobre el aspecto de reclutamiento, se acusó a Estados Unidos de poner en marcha un programa secreto llamado "The Brain Drain" en 2005 cuyo objetivo era persuadir a científicos y militares relacionados con el programa nuclear iraní para que desertaran[34]. Aunque este extremo siempre ha sido negado por Estados Unidos, se atribuye a "The Brain Drain" el rocambolesco caso del investigador nuclear Shahram Amirí, supuestamente desaparecido en junio de 2009 durante un peregrinaje a La Meca y que posteriormente, al volver a Irán vía Estados Unidos, acusó a la CIA de haberlo secuestrado[35].

---

[32] HASHEM Ali, "Hezbollah faces pressure after Bulgaria indictment", Al Monitor (06.02.2013), disponible en http://www.al-monitor.com/pulse/originals/2013/02/response-bulgaria-accuses-hezbollah-attack-on-israelis.html. Fecha de la consulta 30.03.2013.

[33] BBC NEWS, "Cyprus jails Hezbollah operative for Israel attacks plot", BBC News (28.03.2013), disponible en http://www.bbc.co.uk/news/world-europe-21970309. Fecha de la consulta 30.03.2013.

[34] MILLER Greg, "CIA has recruited Iranians to defect", Los Angeles Times (09.12.2007), disponible en http://articles.latimes.com/2007/dec/09/world/fg-usiran9. Fecha de la consulta

[35] ESPINOSA Soledad, "Espías, asesinatos y desertores", El País, (15.01.2012), disponible en http://internacional.elpais.com/internacional/2012/01/15/actualidad/1326582407_004748.html. Fecha de la consulta 29.03.2013.

En agosto de 2011, el ministerio de Inteligencia y Seguridad Nacional iraní también acusó a Estados Unidos de llevar a cabo operaciones de reclutamiento de jóvenes iraníes para la CIA, especialmente ingenieros y recién graduados que tuvieran relación con el programa nuclear o la industria de defensa iraní. Para ello, utilizaban centros de empleo tapadera por internet para captarlos como Holbertson Advisers, Technical Hiring, Engineer One, inc., Deon Capital o Marketing Research Association, entre otros. Estas empresas ofrecían trabajo o estudios en Estados Unidos a los jóvenes iraníes seleccionados. Pero cuando se realizaban las entrevistas se les pedía cierta colaboración a cambio de la posición y de la visa[36].

En relación a la desarticulación de redes de espías e informantes, cabría destacar tanto el trabajo de la contrainteligencia de los Estados miembros del CCG, como la del VEVAK iraní y el servicio de contrainteligencia de Hezbollah en el Líbano.

Respecto al primer caso, en marzo de 2011 Kuwait sentencia a muerte a dos iraníes y un kuwaití porque habrían proporcionado inteligencia al QUDS. Otras dos personas, una de ellas siria, son condenadas a cadena perpetua por los mismos hechos. Se da la circunstancia que todos ellos formaban parte del ejército kuwaití[37]. Un mes después, tres diplomáticos iraníes son expulsados por Kuwait acusados de crear una red de espionaje para Irán y de preparar atentados contra posiciones estratégicas kuwaitíes. La respuesta desde Teherán es la expulsión de tres diplomáticos kuwaitíes al mes siguiente[38].

En Yemen, en julio de 2012 las autoridades yemeníes anuncian la desarticulación y detención de los miembros de una supuesta red de espías asentada en Sanaa liderada por un antiguo miembro de los CGRI. Se les acusa de apoyar las revueltas de los Hothy, comunidad chiita del norte, y apoyar a los secesionistas del sur para minar el poder de influencia de Arabia Saudí en Yemen[39]. A ello, hay que sumar el apresamiento el pasado enero de 2013 de un barco cargado con armamento por parte de las fuerzas de seguridad yemeníes en sus aguas territoriales, cuyo presunto destino eran los grupos citados anteriormente. El gobierno de Yemen cree que Irán está detrás del envío y ha solicitado formalmente al Consejo de Seguridad de Naciones Unidas que investigue el caso[40].

---

[36] IRAN TODAY, "VEVAK defeated CIA again, arrested 30 U.S. spies", Press TV, 27 de agosto de 2011, disponible en http://www.youtube.com/watch?v=tCw4LYopMbw. Fecha de la consulta 30.03.2013.

[37] FULTON Will, FARRAR-WELLMAN Ariel, "Kuwait-Iran foreign relations", *AEI Iran Tracker*, 1 de agosto de 2011, disponible en http://www.irantracker.org/foreign-relations/kuwait-iran-foreign-relations. Fecha de la consulta 30.03.2013.

[38] Ibid.

[39] BBC NEWS, "Yemen arrests prompt president's warning to Iran", BBC News (18.07.2012), disponible en http://www.bbc.co.uk/news/world-middle-east-18896321. Fecha de la consulta 30.03.2013.

[40] SHANKER Tom, WORTH Robert, "Yemen seizes sailboat filled with weapons, and U.S. points to Iran", The New York Times (28.01.2013), disponible en http://www.nytimes.com/2013/01/29/world/middleeast/29military.html?_r=0. Fecha de la consulta 30.03.2013).

Otro episodio tiene lugar en febrero de 2013 cuando Bahréin acusa a los CGRI iraní de crear y financiar una célula afín dentro de su Estado para perpetrar asesinatos y atentados. En la operación realizada contra la misma, se detienen a ocho ciudadanos de Bahréin en la propia isla y también en Omán con presuntos vínculos con Irán, Irak y Líbano donde habrían recibido entrenamiento[41]. Ya en noviembre de 2011, las autoridades de Bahréin también acusaron a los QUDS de estar detrás de una operación para perpetrar ataques terroristas contra su gobierno y contra embajadas occidentales, supuestamente llevadas a cabo por al menos cinco ciudadanos chiitas de Bahréin[42].

El ejemplo más reciente tiene lugar en Arabia Saudí el 20 de marzo de 2013 cuando su ministerio del Interior detiene a un ciudadano iraní, un libanés y dieciséis saudíes acusados de formar una red de informantes para Irán. Este hecho es desmentido inmediatamente por el ministerio de Exteriores iraní, aunque Arabia Saudí reitera sus denuncias hacia el régimen de los ayatolás[43].

En la contraparte iraní, el 20 de noviembre de 2011 la CIA confirma la suspensión temporal de sus actividades en el Líbano tras la captura de un número indeterminado de sus agentes y colaboradores en Beirut, se cree que decenas de ellos, por parte de la contrainteligencia de Hezbollah[44]. Tras la desarticulación de esta red de espías e informantes conocida como el ring del Pizza Hut por sus frecuentes reuniones en un establecimiento de esta cadena de comida en la capital libanesa, el VEVAK iraní anuncia la detención de una decena de informadores de la CIA en Irán[45]. Anteriormente, en el mes de mayo, Heidar Moslehi, ministro de Inteligencia iraní, ya había confirmado la detención de otros 30 presuntos colaboradores de la CIA acusados de espionaje y que habrían actuado tanto dentro de Irán, como a través de las embajadas de Estados Unidos en Emiratos Árabes Unidos, Malasia y Turquía. Además, también se identifica a 42 operativos de la inteligencia estadounidense

[41] REUTERS, "Bahrain says Iran's Revolutionaty Guard behind 'terror cell'", Reuters (20.02.2013), disponible en http://www.reuters.com/article/2013/02/20/us-bahrain-violence-cell-idUSBRE91J0CX20130220. Fecha de la consulta 30.03.2013.

[42] CNN, "Bahraini authorities detail terror suspects' ties to Iran", CNN (14.11.2011), disponible en http://edition.cnn.com/2011/11/13/world/meast/bahrain-terror-suspects. Fecha de la consulta 11.04.2013.

[43] AL ARABIYA, "Espionage ring…", op. cit.

[44] DAVID Barak, AP, "Doznes of U.S. spies captured in Lebanon and Iran", Haaretz (21.11.2011), disponible en http://www.haaretz.com/news/middle-east/report-dozens-of-u-s-spies-captured-in-lebanon-and-iran-1.396840. Fecha de la consulta 30.03.2013.

[45] BAER Robert, "Did Hizballah beat the CIA at its own techno-surveillance game?", Time (30.11.2011), disponible en http://www.time.com/time/world/article/0,8599,2100667,00.html. Fecha de la consulta 30.03.2013.

que estarían operando en diferentes Estados. Todo ello después de que agentes del VEVAK se infiltraran en la red[46].

Otra acción de la contrainteligencia iraní se traduce en la condena a muerte dictada el 9 de enero de 2012 contra Amir Mirzaei Hekmati, estadounidense de origen iraní que había servido en la inteligencia militar de Estados Unidos en Irak y Afganistán. El VEVAK lo acusa de ser un espía de la CIA y de intentar infiltrarse en el departamento de inteligencia iraní. Previamente a su visita a Irán, el detenido habría sido localizado por el VEVAK en la base aérea estadounidense de Bagram en Afganistán[47].

Un último ejemplo tiene como protagonista a Yundallah, el grupo terrorista sunita, y la desarticulación de cuatro de sus células entre marzo y junio de 2012 por parte del VEVAK cuando estarían preparando una serie de atentados, según fuentes iraníes[48].

Una peculiaridad de la contrainteligencia iraní es la utilización de la desinformación como instrumento para despistar a las agencias de inteligencia rivales. Este hecho es reconocido por el propio director de la Organización de la Energía Atómica de Irán (OEAI), Fereydoon Abbasi, quien afirma que Irán a veces facilita y filtra información falsa respecto a su programa nuclear tanto al Organismo Internacional de la Energía Atómica (OIEA), a la que Irán acusa de estar infiltrada por el espionaje de los servicios de inteligencia occidentales y de convertir Viena en un nido de espías, como a los medios de comunicación, para protegerlo[49].

A todo este conjunto de operaciones encubiertas y actividades de contrainteligencia descritas, se deberían añadir los nuevos instrumentos que se habrían ido introduciendo progresivamente para desarrollar este tipo de operativos durante el periodo de estudio, destacando, sobre todo, la aplicación de nuevas tecnologías como los Vehículos Aéreos No Tripulados (VANT) o el uso del ciberespacio adaptados a los objetivos de atacar o defender a todo lo relacionado con el programa nuclear iraní.

---

[46] DARAGAHI Borzou, "Iran claims to break CIA spy ring, arrests 30", Los Angeles Times (22.05.2011), disponible en http://articles.latimes.com/2011/may/22/world/la-fg-iran-espionage-20110522. Fecha de la consulta 30.03.2013.

[47] GLADSTONE Rick, MORRIS Harvey, "Iran imposes death sentence on U.S. man accused of spying", The New York Times (09.01.2012), disponible en http://www.nytimes.com/2012/01/10/world/middleeast/iran-imposes-death-sentence-on-alleged-us-spy.html?pagewanted=all&_r=0. Fecha de la consulta 31.03.2013.

[48] PRESS TV, "Iran dismantles four Jundallah-affiliated terrorist groups", Press TV (26.06.2012), disponible en http://www.presstv.ir/detail/2012/06/26/248063/iran-disband-jundallah-terrorist-cell/. Fecha de la consulta 31.03.2013.

[49] GLADSTONE Rick, HAUSER Christine, "Iran's top atomic oficial says nation issued false nuclear data to fool spies", The New York Times (20.09.2012), disponible en http://www.nytimes.com/2012/09/21/world/middleeast/iran-atomic-official-says-it-gave-false-nuclear-information-to-fool-spies.html. Fecha de la consulta 31.03.2013.

Este tipo de instrumentos que implican un menor riesgo físico en las operaciones encubiertas y de contrainteligencia, además de una menor probabilidad de determinar la culpabilidad de un Estado en el caso del ciberespacio, merecen ser tratados de forma especial en el siguiente sub apartado.

Ciberseguridad y Vehículos Aéreos No Tripulados (VANT)

El programa nuclear iraní también destacaría por ser un escenario en el cual se desarrollarían y aplicarían las ciber capacidades ofensivas y defensivas de los actores supuestamente implicados tanto para realizar operaciones encubiertas contra sistemas de infraestructuras críticas, como para conseguir recolectar información para el ciclo de inteligencia (ciberespionaje) y el desarrollo de los propios ciberataques.

Así y en los primeros meses de su mandato, el presidente estadounidense Barack Obama, según cita The New York Times, ordena seguir con el desarrollo del proyecto secreto "Olympic Games" iniciado por su antecesor George W. Bush en 2006[50]. Su objetico sería desarrollar capacidades dentro del ciberespacio que permitieran iniciar una serie de ciberataques contra todas aquellas instalaciones relacionadas con el programa nuclear iraní. Fruto del proyecto y según la misma fuente, la National Security Agency, el Centro de Operaciones de Información de la CIA, conjuntamente con una unidad secreta ligada a la Unidad Militar 8200 de las Fuerzas de Seguridad de Israel (IDF) crean un primer malware llamado "Stuxnet". Dicho malware tendría el objetivo de acceder e inutilizar los sistemas de control (SCADA) de la central nuclear de Bushehr y de la planta de enriquecimiento de uranio de Natanz para destruir, en este último caso, sus centrifugadoras de enriquecimiento de uranio dentro de la "Operación Myrtus".

"Stuxnet", definido en términos de seguridad como una Amenaza Persistente Avanzada (APT en sus siglas en inglés)[51], fue presuntamente introducido al sistema SCADA de Natanz por propio personal de la instalación o de forma involuntaria por el mismo personal a través de sistemas exteriores (Ej. Memoria USB) que habrían sido infectados previamente. Una vez dentro, se produce el ciberataque a sus centrifugadoras. El resultado de dicha operación encubierta fue que se dañaron aproximadamente unas 1.000 centrifugadoras de la planta de Natanz hasta verano de 2010. En mayo del mismo año, la empresa bielorrusa especializada en anti virus Virusblokada descubre el malware "Stuxnet" en un ordenador iraní gracias a un error en un código de una de sus nuevas versiones. Este hecho provoca la liberación del malware hacia ordenadores personales fuera de la planta de Natanz provocando el llamado

[50] SANGER David, "Obama order sped up wave of cyberattacks against Iran", The New York Times (01.06.2012), disponible en http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0. Fecha de la consulta 31.03.2013.
[51] RID, op. cit., 17.

"efecto cascada"[52] en la red global. "Stuxnet" es presuntamente el primer ciberataque atribuido a Estados Unidos contra las infraestructuras críticas de otro Estado[53].

Además, se cree de la existencia de como mínimo otros cuatro malwares más elaborados por la misma plataforma que crea "Stuxnet". Sin embargo y a diferencia de éste, los otros actuarían como "ladrones de información" dentro de operaciones de ciberespionaje para obtener datos y facilitar los ciberataques o la ciberdefensa, entre otros objetivos. De ellos destacaría el malware "Duqu", aunque los dos "ladrones de información" más conocidos utilizados supuestamente por los actores que intentarían sabotear el programa nuclear iraní serían los malware "Flame" y "Gaus"[54].

Así, otro ciberataque destacado contra Irán y que también afecta a Cisjordania, los Emiratos Árabes Unidos y Líbano se realiza a través del malware "Flame" (también conocido como "sKyWIper"), que es un "ladrón de información" descubierto en mayo de 2012 por la empresa especializada en ciberseguridad Kaspersky Lab[55]. Se cree que "Flame" llegó a infectar los sistemas informáticos de infraestructuras clave de Irán, algunas de ellas relacionadas con su programa nuclear, así como ordenadores de oficiales de alto rango iraníes y de algunos ministerios de los cuales podría haber extraído información. De hecho, las autoridades iraníes descubren el malware cuando en abril de 2010 sufren un ciberataque en los ordenadores del ministerio del Petróleo y en sus instalaciones de exportación del crudo, como la situada en la isla de Kharg por donde pasa el 80% del petróleo exportado, y que les obliga a desconectar los terminales de los cuales estarían siendo sustraídos datos de sus discos duros[56].

Según diversos expertos pertenecientes a compañías de seguridad de IT, el malware "Flame" llevaría funcionando aproximadamente cinco años antes de ser detectado y su origen podría estar ligado de nuevo a la colaboración entre Estados Unidos e Israel, aunque es este último quien hubiera iniciado el ciberataque de forma unilateral[57].

---

[52] El problema de los ciberataques es que se realizan contra un objetivo específico pero no se pueden controlar los efectos del malware. Este puede liberarse hacia la red global provocando el "efecto cascada" y el contagio hacia otros sistemas.

[53] RID, op. cit.

[54] FINKLE Jim, "Stuxnet virus, Duqu virus and at least 3 others reportedly built on same platform", The Huffington Post (28.12.2011), disponible en http://www.huffingtonpost.com/2011/12/28/stuxnet-weapon-duqu-virus-kaspersky-lab_n_1173532.html. Fecha de la consulta 31.03.2013.

[55] LABORATORY OF CRYPTOGRAPHY AND SYSTEM SECURITY, *sKyWIper: A complex malware for targeted attacks*, Department of Telecommunications - Budapest University of Technology and Economics, 31 de mayo de 2012, disponible en http://www.crysys.hu/skywiper/skywiper.pdf. Fecha de la consulta 31.03.2013.

[56] BBC NEWS, "Iran 'fends off new Stuxnet cyber-attack'", BBC News (25.12.2013), disponible en http://www.bbc.co.uk/news/world-middle-east-20842113. Fecha de la consulta 11.04.2013.

[57] NAKASHIMA Ellen, MILLER Greg, TATE Julie, "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts", The Washington Post (19.06.2012), disponible en

Paralelamente, en agosto de 2012 el mismo laboratorio de la empresa rusa Kaspersky Lab detecta unos 2500 ordenadores infectados con el malware "Gaus" en el Líbano en otra operación catalogada de ciberespionaje. Este "ladrón de información" se habría dedicado a recopilar información de cuentas bancarias de las principales entidades de este Estado como Bank of Beirut, BlomBank o Credit Libanais. Las mismas son conocidas por sus relaciones clientelares con el régimen sirio de Al Asad, con Hezbollah y con Irán[58].

Por el lado iraní y tras el ciberataque del malware "Stuxnet", el gobierno de Ahmadineyad crea la Organización de la Ciberseguridad. La misma está formada por una vertiente defensiva, la ciberunidad especial dentro de la Organización de Defensa Pasiva de las Fuerzas Armadas de Irán dirigida por el General de Brigada Gholam Reza Jalali y cuya función es contrarrestar y detectar los ciberataques y el ciberespionaje y, por el otro lado, la vertiente ofensiva con el llamado Cuerpo Ciber que los generaría contra sus enemigos[59]. Así, la Organización de la Ciberseguridad se dota de capacidades para desarrollar operaciones encubiertas y de contrainteligencia utilizando el ciberespacio.

Precisamente, oficiales de inteligencia estadounidenses creen que el Cuerpo Ciber iraní estaría detrás de algunos ciberataques como el realizado en agosto de 2012 contra la empresa petrolífera Saudi Aramco de Arabia Saudí con el malware "Shamoon". Este virus podría haber sido introducido por propio personal de la empresa y se estima que destruyó unas tres cuartas partes de la información almacenada en los más de 30.000 ordenadores de la red interna de comunicaciones de la compañía estatal saudí[60]. Es preciso mencionar que Saudi Aramco es una de las grandes beneficiadas por las sanciones internacionales aplicadas al petróleo iraní a causa de su programa nuclear. Dos semanas después, la empresa de gas natural catarí, RasGas, participada también por la estadounidense Exxon Mobil Corp. sufre un ciberataque similar al de Saudi Aramco[61].

Las mismas fuentes también señalarían a Irán como el promotor de otra serie de ciberataques que se vienen produciendo desde septiembre de 2012 contra algunas entidades financieras estadounidenses como Bank of America, Citigroup, Wells Fargo, U.S. Bancorp o Capital One, entre otras muchas. Estos ciberataques utilizarían un malware

---

http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. Fecha de la consulta 31.03.2013.

[58] THE NEW YORK TIMES, "Cyberattacks on Iran: Stuxnet and Falme", The New York Times (09.08.2012), disponible en http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html. Fecha de la consulta 31.03.2013.

[59] IRAN POLITIK, "General Jalali: Iran has begun to operate its first cyber army", Iran Politik (21.02.2012), disponible en http://www.iranpolitik.com/2012/02/21/news/general-jalali-iran-begun-operate-cyber-army/. Fecha de la consulta 31.03.2013.

[60] PERLROTH Nicole, "In cyberattack…", op. cit.

[61] Ibid.

llamado "Itsoknoproblembro" que permitiría alterar, interrumpir o colapsar los sistemas online de dichos bancos con la consiguiente repercusión para sus clientes. Ello podría verse como una represalia por las sanciones impuestas al régimen de los ayatolás. Sin embargo, representantes de Irán como Alireza Miryousefi, secretario de la delegación iraní de Naciones Unidas, niegan su implicación directa o indirecta en dichas acciones[62].

Otro aspecto importante a mencionar sería la utilización de VANT o "drones" y de satélites, tanto estatales como privados, por parte de Estados Unidos y sus aliados como medio para obtener información sobre el programa nuclear iraní (IMINT o Inteligencia de Imágenes), así como para realizar operaciones encubiertas. De hecho, son frecuentes los incidentes reportados sobre VANT estadounidenses acusados de penetrar en territorio iraní para obtener información sobre instalaciones militares o del programa nuclear, así como de maniobras realizadas por las Fuerzas Armadas iraníes y que, en algunas ocasiones, son interceptados o atacados por la aviación del Estado persa[63].

En esta dirección, se cree que Irán dispondría de alta tecnología capaz de interferir en los satélites espías y comerciales, así como de monitorizar y "hackear" los sistemas de navegación de los VANT. Este sofisticado sistema de interceptación de comunicaciones y sistemas guía habría sido proporcionado a Irán por Rusia, en primer lugar, y luego desarrollado por la propia República Islámica añadiendo los datos obtenidos de los "drones" estadounidenses abatidos en Afganistán que habrían llegado a sus manos, por un lado, y por el otro gracias a los VANT capturados en su propio territorio. Esto permitiría a los ingenieros iraníes desarrollar capacidades para realizar ofensivas electrónicas a través de decodificar la información contenida en los "drones" y tener acceso al Sistema de Posición Global (GPS) de algunos modelos VANT fabricados por Estados Unidos. Con ello, la Organización de la Ciberseguridad de las Fuerzas Armadas iraníes, unidad competente para ello, podría haber creado un sistema de intercepción basado en reprogramar el GPS, *hackear* al *drone*, cambiarlo a modo piloto automático haciendo perder el control sobre el mismo al controlador y forzarlo a aterrizar en territorio iraní[64].

Algunos ejemplos de lo anteriormente citado serían el incidente no reportado ocurrido a finales del año 2011 en el que un satélite espía estadounidense fue "cegado" de forma precisa por un láser cuya acción fue atribuida a Irán por los servicios de inteligencia

[62] PERLROTH, op. cit.

[63] SHANKER Tom, GLADSTONE Rick, "Iran fired on military drone in first such attack", The New York Times (08.11.2012), disponible en http://www.nytimes.com/2012/11/09/world/middleeast/pentagon-says-iran-fired-at-surveillance-drone-last-week.html?pagewanted=all. Fecha de la consulta 11.04.2013.

[64] COHEN Dudi, "Iran 'blinded' CIA spy satellite", Ynetnews.com (17.12.2011), disponible en http://www.ynetnews.com/articles/0,7340,L-4162770,00.html. Fecha de la consulta 31.03.2013.

occidentales[65]. En la misma dirección, dos UAV del tipo RQ-11 estadounidenses habrían sido apresados en agosto de 2011 y octubre de 2012 respectivamente. Otro incidente significativo tiene lugar el 5 de diciembre 2011 cuando un UAV RQ-170 "Sentinel" estadounidense cae en manos iraníes cerca de la ciudad de Kashmar, próxima a la frontera con Afganistán. Aproximadamente un año después, otro "drone" de observación del tipo "ScanEagle" es apresado en el espacio aéreo iraní sobre el Golfo Pérsico por la Fuerza Naval de los CGRI[66]. En ambos casos, las autoridades iraníes aseguran haberse hecho con el control de los "drones" una vez aplicado el sistema de interceptación. Sin embargo, fuentes estadounidenses afirman que el primero de ellos se estrelló por un fallo en el sistema de control, mientras que el segundo apresamiento es negado[67].

A pesar de estas versiones contradictorias, Irán podría haber obtenido información muy valiosa acerca de la tecnología VANT estadounidense con estas acciones[68], no sólo para uso propio, sino también para poder vender o compartir dicha tecnología con otros Estados como China, Corea del Norte o Rusia. No se puede obviar que los VANT son una pieza central en la estrategia de seguridad de la administración Obama tanto para realizar ataques selectivos como para la recolección de información.

A todo ello hay que añadir que el 27 de octubre de 2012 y durante una semana, Irán celebra los primeros ejercicios en ciberseguridad de su historia en los que se simulan ciberataques contra infraestructuras críticas como instalaciones nucleares y centrales eléctricas, instituciones públicas, bancos o centros de datos, entre otros. Además, a finales de diciembre de 2012 y durante los seis días de maniobras navales *Velayat 91*, también entra en acción por primera vez la unidad especial en ciberseguridad de la marina iraní en una simulación de ciberataque contra el sistema central de control de las fuerzas de defensa de la Armada[69].

---

[65] Íbid.

[66] PRESS TV, "Iran Navy downs two RQ-11 drones in last two years", Press TV (02.01.2013), disponible en http://www.presstv.ir/detail/2013/01/02/281447/iran-navy-downs-two-rq11-drones/. Fecha de la consulta 31.03.2013.

[67] ERDBRINK Thomas, "U.S. navy denies Iran's claim to have captured drone", The New York Times (04.12.2012), disponible en http://www.nytimes.com/2012/12/05/world/middleeast/iran-says-it-seized-another-american-drone.html. Fecha de la consulta 11.04.2013.

[68] REUTERS, "Iran says extracts data from U.S. spy drone", Reuters (05.11.2012), disponible en http://www.reuters.com/article/2012/12/05/us-iran-usa-drone-idUSBRE8B40E320121205. Fecha de la consulta 11.04.2013.

[69] PRESS TV, "Iran will hold first-ever cyber drills, passive defense chief says", Press TV (24.12.2012), disponible en http://www.presstv.com/detail/2012/10/24/268414/iran-will-hold-firstever-cyber-drills/. Fecha de la consulta 31.03.2013 y PRESS TV "Iran uses cyber defense techniques for first time in naval drills", Press TV (30.12.2012), disponible en http://www.presstv.ir/detail/2012/12/30/280855/cyber-defense-used-in-iran-naval-drills/. Fecha de la consulta 31.03.2013.

Así, el aumento de las capacidades en ciberseguridad de Irán en los últimos dos años, tanto en el desarrollo de instrumentos para ciberataques, como ciberespionaje y ciberseguridad, como en el desarrollo de nuevas tecnologías aplicadas a la defensa de su programa nuclear y a implementar políticas de represalia, sería una de las consecuencias directas de las operaciones encubiertas realizadas contra el régimen de los ayatolás.

¿SE CUMPLEN LOS OBJETIVOS?

El principal objetivo de las operaciones encubiertas y la contrainteligencia presuntamente llevadas a cabo por el bloque contrario al programa nuclear iraní sería ralentizarlo y, a ser posible, acabar con el mismo a través de estas actividades, además de ganar tiempo para que otras políticas de seguridad pudieran ser desarrolladas y aplicadas con más efectividad, como por ejemplo la negociación o el régimen de sanciones impuesto contra Irán, y debilitar así la posición de este Estado.

Sin embargo y tras lo expuesto, sólo se habría conseguido el objetivo de ralentizar el programa con el ciberataque de Stuxnet que afectó a unas 1000 centrifugadoras de la central de enriquecimiento de uranio de Natanz hasta 2010. Pero todas las demás acciones no habrían logrado el propósito de frenarlo, al contrario, el programa nuclear sigue avanzando. Además y en mi opinión, el aumento de las capacidades en ciberseguridad de Irán junto al régimen de sanciones que impide la importación de piezas y componentes para su programa nuclear, hace que sea más difícil que el régimen de los ayatolás vuelva a ser sorprendido por un ciberataque como el sufrido, única vía que habría demostrado ser efectiva hasta el momento para los supuestos objetivos marcados por las operaciones encubiertas.

De hecho y según la revista Time, que cree que el Mossad estaría detrás de muchas de las operaciones encubiertas descritas, el primer ministro israelí, Benjamin Netanyahu, en marzo de 2012 ya habría tomado la decisión de reducir el número de las mismas relacionadas con la neutralización selectiva de objetivos, detonaciones en instalaciones claves iraníes, operativos sobre el terreno o actividades de reclutamiento dentro del programa nuclear iraní, pese a la opinión contraria del Mossad que quería seguir con ellas[70].

Los principales motivos por los que Netanyahu habría adoptado esta decisión serían tres: en primer lugar, la apuesta del primer ministro israelí por una política de seguridad preventiva a través de una intervención militar directa como mejor opción para acabar con el programa

[70] VICK Karl, "Mossad cutting back on covert operations inside Iran", Time (30.03.2012), disponible en http://world.time.com/2012/03/30/mossad-cutting-back-on-covert-operations-inside-iran-officials-say/. Fecha de la consulta 31.03.2013.

nuclear iraní. La posición defendida por Netanyahu y tomada al ver que las operaciones encubiertas no habrían logrado su objetivo de paralizar las ansias nuclearas de Irán, tendría la opinión en contra del Mossad, tanto la de su actual director, Tamir Pardo, como la de su predecesor entre 2002 y 2010, Meir Dagan, y parte de la cúpula militar del Tzahal que la desaconsejarían y apostarían por seguir con las acciones encubiertas hasta que no hubiese pruebas concluyentes referidas a que Irán buscara realmente el arma nuclear. A pesar de ello, Netanyahu sigue firme en su propósito.

Un segundo motivo sería causado por el temor de Netanyahu a que operativos del Mossad fuesen capturados en el marco de una operación encubierta en suelo iraní con las consecuencias que ello podría provocar tanto para el debate sobre la intervención militar, como para la credibilidad de los demás actores internacionales que apuestan por una política de negociación con el régimen de los ayatolás, combinada con una política de contención en forma de duras sanciones internacionales. Dicho temor vendría dado por las repercusiones originadas tras el atentado que acabó con la vida del científico iraní, Mustafá Ahmadi Roshan, en enero de 2012, del que Israel fue directamente acusado y en la que Irán pudo presentarse ante la comunidad internacional como víctima. Y este es el tercer motivo, la impopularidad de algunas operaciones encubiertas, en especial, la neutralización selectiva de objetivos, provoca que aumente el apoyo interno al régimen de los ayatolás y al programa nuclear iraní, y en el exterior, Irán pueda aparecer como la víctima y explotar esta imagen a beneficio propio.

A ello, también se debería añadir la influencia de la doble capacidad de respuesta de la contrainteligencia iraní y sus aliados para desarticular redes de espías en su territorio y para, presuntamente, atentar contra personal e intereses israelíes en puntos divergentes geográficamente.

Así, el bloque liderado por Irán ha logrado que el programa nuclear pueda seguir desarrollándose, a pesar del fallo cometido por su contrainteligencia con el ciberataque Stuxnet y el control del personal con acceso a las instalaciones claves de su apuesta nuclear.

No obstante y de ser ciertas las atribuciones de la autoría de las acciones al bloque iraní, éste habría demostrado capacidad de poder llevar a cabo políticas de represalia, tanto a través de atentados contra objetivos israelíes en diferentes partes del mundo, como a través del ciberespacio contra otros Estados. Estos hechos también permitirían visualizar la amplia extensión de la red de informantes y de equipos móviles que han construido los QUDS no sólo a nivel regional, sino también fuera de ella. A ello hay que añadir el trabajo de contrainteligencia de este bloque que ha permitido, entre otras acciones, desmantelar amplias estructuras de espionaje de la CIA, reconocido por la propia agencia de inteligencia estadounidense como ya se ha citado con anterioridad en el documento.

Sin embargo, también sería preciso resaltar el trabajo realizado por la contrainteligencia de los Estados del CCG a la hora de desarticular supuestas redes de espías y células operativas al servicio del régimen de los ayatolás dentro de las comunidades chiíes que habitan en estos Estados del Golfo Pérsico.

Finalmente, dos de los hechos más destacados del periodo objeto de estudio serían la importancia adquirida por el ciberespacio, las nuevas tecnologías y los "drones" para implementar operaciones encubiertas y actividades de contrainteligencia en detrimento de otras más clásicas, pero que implican más riesgo físico para los operativos; y la creación de la Organización de la Ciberseguridad iraní, con su doble capacidad defensiva y ofensiva, que situarían a Irán como una futura potencia en este apartado tal y como se encarga de señalar el General William Shelton, supervisor de las operaciones en ciberseguridad de las Fuerzas Aéreas estadounidenses, quien reconoce que Irán ha incrementado sus esfuerzos en el ciberespacio tras el ataque sufrido en las instalaciones de Natanz y que será una ciberpotencia a tener en cuenta en el futuro[71].

Así y como conclusión, las operaciones encubiertas podrían ser utilizadas por el bloque contrario al programa nuclear iraní para ralentizarlo y ganar tiempo para las otras opciones que están sobre la mesa en la solución del conflicto nuclear, siendo los ciberataques el instrumento que habría demostrado mayor efectividad para ello.

Sin embargo, este tipo de operaciones no serviría para parar las ansias nucleares iraníes ya que su programa sigue desarrollándose, con el añadido que durante este periodo el régimen de los ayatolás habría perfeccionado sus capacidades defensivas para protegerlo. Además, también habría demostrado tener poder de represalia para responder a aquellos ataques sufridos ya sea a través de operaciones encubiertas realizadas por sus operativos en el exterior, los QUDS, por su representante en Líbano de Hezbollah o por el Cuerpo Ciber iraní.

Xavier Servitja Roca
Licenciado en CCPP y RRII

[71] SHALAL-ESA Andrea, "Iran strengthened cyber capabilities after Stuxnet: U.S. General", Reuters (18.01.2013), disponible en http://uk.reuters.com/article/2013/01/18/us-iran-usa-cyber-idUKBRE90G1C420130118. Fecha de la consulta 31.03.2013.