Anuario en Relaciones Internacionales
2022
Editado anualmente desde 1994
(Publicación digital) ISSN: 1668-639X

Departamento del Seguridad Internacional y Defensa

Artículos

Ciberguerra entre Israel e Irán: desde Stuxnet hasta los ciberataques actuales

Gustavo Wajsman[521]

Resumen.

El presente trabajo tiene como fin dar cuenta del primer Ciber ataque estatal con una Ciber arma presuntamente llevado a cabo por Israel y Estados Unidos aunque ejecutado por una unidad especial del Mossad, el Kidon, contra la central nuclear iraní en la ciudad de Natanz. Dicho ataque cibernético tuvo la intención de retrasar los planes nucleares de Irán que incidirían en el poder y status quo de la región detentado por Israel como potencia regional y principal aliado de los Estados Unidos de Norteamérica. Si bien hay varios actores externos involucrados, nosotros solo abordaremos la postura israelí fundamentada en una visión neorrealista de las relaciones internacionales contempla el uso de ataques preventivos desde 1981 para salvaguardar la seguridad del estado. En este caso debuto el uso del quinto dominio a través de la ciber arma STUXNET y ello ocasiono su consecuente repercusión en la doctrina de defensa iraní.

Según nuestra visión esta guerra librada en el Ciberespacio, la cual fue complementada con operaciones de información, operaciones especiales y actividades especiales de inteligencia en las que participo el Mossad Israelí y la unidad 8200 de AMAN, la inteligencia militar de dicho país, fue pergeñada estratégicamente para usarse en conjunto con operaciones convencionales y no convencionales. En el caso tratado ello ocurrió como consecuencia de la lección aprendida en la guerra de Iom Kipur en 1973 y lo que ellos llaman “El concepto”. . Así se dio el primer punta pie que dio origen a una nueva era ampliando la guerra al ciberespacio.

521Maestrando en Relaciones Internacionales (USAL) y candidato al Doctorado de Estudios Internacionales (Universidad Di Tella); egresado de la EDENA y Diplomado en Seguridad Internacional y Defensa (Universidad de Belgrano); Maestrando en Derecho, LLM (Universidad de Londres); experto en Cibercrimen y Ciberseguridad (Universidad Siglo XXI) y Diplomado Universitario en Gestión de la Ciberdefensa (Escuela Superior de las Fuerzas Armadas).

Pero como toda fuerza de acción tiene otra fuerza de reacción, igual y opuesta, el exitoso uso de STUXNET a pesar de su negación al principio y posterior reconocimiento por parte de altos funcionarios Iraníes que retraso varios meses su programa nuclear, logro ganar algo de tiempo para usar otros medios alternativos como ser los diplomáticos internacionales para detener el desarrollo nuclear del país persa pero como contrapartida , provoco que Irán desarrollara una poderosa unidad de ciberdefensa y comience usar el Ciberespacio como un dominio más de la guerra.

Justificacion

Desde un abordaje desde el realismo estructural trataremos el tema de STUXNET como la primer ciber arma dando comienzo a la ciberguerra, como un dominio más de la guerra, teniendo en cuenta la historia militar israelí, las relaciones internacionales, la seguridad internacional como campo especifico de las relaciones internacionales y la estrategia. Lo novedoso del presente trabajo es que no solo identifica a STUXNET como primer ciber arma sino que fue el producto final de una revisión en su doctrina militar luego del error estratégico militar cometido por Israel en 1973, durante la guerra de IOM KIPUR, el cual casi le cuesta una derrota militar y política sin precedente desde la creación del estado de Israel el 14 de mayo de 1948 que podría haber acabado con el estado judío.

Nuestra visión será concentrarnos brevemente en los cambios ocurridos desde dicha guerra y en la situación de que a partir de entonces Israel no volvió a participar en una guerra estatal abierta. Lo que siguió en adelante para Israel fueron diferentes clases de conflictos asimétricos incluyendo los conflictos híbridos y que como corolario culmino con el comienzo del uso del ciber espacio como campo de batalla complementario para asegurar el estatus quo de la región y seguir manteniendo su superioridad militar .

Si bien es cierto que desde 1973 Israel no se vio involucrado en una guerra convencional, los conflictos híbridos en los que se vio involucrado tuvieron que ver con actores subnacionales pero patrocinados por Irán.

Dado que Irán financia y apoya a hezbollah y Hamas y ha manifestado su deseo de desaparecer al estado judío de la faz de la tierra, Israel hará todo lo posible para que Irán no consiga el arma nuclear y para retrasar sus avances en dicha materia hasta que se pueda resolver por otros medios a través de la comunidad internacional.

Planteamiento del problema

De acuerdo a lo mencionado ut supra, el estado de Israel, se encuentra sumido en una visión de balance de poder regional descripto perfectamente por el realismo estructural de Kenneth Waltz en y en un sistema internacional anárquico, debido a que no hay una autoridad central que lo ordene y por otro lado en dicho marco los estados dependen de sí mismo para sobrevivir. En esta visión neorrealista, las capacidades de los estados juegan un rol preponderante y el estado de Israel debe vigilar a Irán en este caso y accionar en consecuencia a sus desarrollos o intentos de desarrollos de capacidades militares para mantener la balanza a su favor.

Con STUXNET se incorpora a la estrategia militar Israelí un nuevo dominio para la defensa del estado. Como los actores estatales son racionales y generan respuestas racionales, Irán percibió luego de esta inesperada acción por parte de Israel, la necesidad de contar con una ciberbrigada tanto defensiva como ofensiva de ahora en más.

Introduccion

Como se mencionó previamente, durante el desarrollo del presente trabajo, el cual aclaramos que no pretende ser exhaustivo sino tan solo el hilo de Ariadna para una mayor profundización futura, trataremos de dar respuesta a la pregunta acerca de si ¿El estado de Israel uso la primer ciber arma, STUXNET, como apoyo a las operaciones convencionales y de inteligencia para mantener su status quo con la intención de retrasar los planes nucleares de Irán?

Nuestra hipótesis es que el uso de STUXNET efectivamente tuvo como finalidad retrasar el programa nuclear iraní y cumplió su cometido con el objetivo de mantener su superioridad militar regional y asegurar la integridad de su territorio y la vida de sus ciudadanos y habitantes del estado de Israel. Se utilizó este nuevo dominio de la guerra primero para impedir un desbalance de poder regional y por otro lado no recurrir a un conflicto bélico abierto tradicional, lo cual hubiese costado muchos más recursos, apoyo internacional por parte de los Estados Unidos y Arabia Saudí y otros actores , y bajas humanas y materiales incalculables.

Dicho de otra manera Israel pretendió no ir a una guerra abierta ni volver a los clásicos bombardeos aéreos que uso contra otros países en casos similares, y sobre todo teniendo en cuenta que la planta nuclear de Natanz es una instalación de difícil acceso para el ataque con misiles y demasiado riesgoso para una incursión de fuerzas especiales Israelíes o del MOSSAD. Debido a ello decidió estratégicamente usar el quinto dominio para afectar de manera significativa las capacidades de las centrifugadoras de uraño, sin posibilidad de una atribución determinante de su autoría. En el ciberespacio no existen las declaraciones de guerra. De esta manera mantuvo el statu quo hasta el día de hoy de acuerdo a la doctrina Begin de ataques preventivos.

El objetivo general que pretende humildemente este trabajo, es analizar si STUXNET ha logrado su fin de retrasar el programa nuclear Iraní y mantener el statu quo regional de poder y si a partir de entonces ha continuado con su política de ciberdefensa hasta la actualidad de acuerdo a la doctrina Begin e identificar la respuesta iraní en el quinto dominio.

Para cumplir con este objetivo general nos proponemos presentar un contexto histórico, que permita entender el problema planteado desde la guerra de IOM KIPUR hasta el uso de STUXNET por parte de Israel y su continuidad de su estrategia de ciberdefensa y uso de Ciber armas.

Luego de ello explicar las características de STUXNET como ciber arma y por ultimo describir las consecuencias del uso de la misma.

Previamente haremos una descripción del marco teórico elegido que en nuestro caso es el neorrealismo o realismo estructural para sostener nuestra hipótesis y también describiremos brevemente la metodología utilizada.

Marco teorico

Todo trabajo académico científico tiene que contar con un marco teórico de una ciencia o disciplina que lo sostenga y sirve como paradigma para explicar la hipótesis que se plantea y su demostración o negación de la misma.

En nuestro caso hemos seleccionado el neorrealismo o realismo estructural y en particular las ideas de Kenneth Waltz, padre del neorrealismo. Como la palabra misma neorrealismo denota, si hay un neorrealismo es porque existió un realismo clásico previamente.

Para ello daremos cuenta de todos los puntos de convergencia que existen en el realismo clásico en general en sus diversas vertientes para luego explicar el aporte del neorrealismo a las relaciones internacionales y su aplicación a nuestro caso de estudio.

La visión del realismo comprende:

- El actor central de las relaciones internacionales es el estado.
- El sistema internacional es anárquico y conflictivo.
- Lo que mueve a los estados es el poder y la seguridad
- Los estados son racionales

Para el neorrealismo de Kenneth Waltz, el mundo internacional es un sistema compuesto por una estructura de unidades que interactúan entre sí. La estructura permite analizar al sistema como un todo. (SODUPE, 2004:84)

El realismo tiene una visión de pesimismo antropológico. Ve al hombre como un ser egoísta motivado por sus propios intereses y deseosos de poder. Es debido a ello que los hombres se organizan en estados y cada estado busca su poder en función de su interés nacional.

Por supuesto que ven el sistema internacional como anárquico porque no existe una autoridad central. Debido a ello los estados solo pueden confiar en sí mismos y su preocupación principal es mantener un margen apropiado de seguridad. Para lograrlo, los estados recurren al uso del equilibrio de poder y de la disuasión.

El primer exponente que históricamente se asocia al realismo es Tucidides y su obra: la historia de la guerra del Peloponeso.

También se encuentra entre sus padres fundadores a Maquiavelo quien ya profundiza en la naturaleza imperfecta del hombre y a Hobbes, quien es considerado otro de sus grandes exponentes que refiere que la naturaleza del estado es anárquica y que donde la norma es "*mantener sus armas en guardia y apuntando, y sus ojos fijos en el otro" (MINGST, 2004: 126)*

Por otro lado consideramos que uno de los mayores referentes que aplico el realismo a la política exterior fue El exponente político más influyente de la teoría realista es Henri Kissinger.

Para concluir este apartado debemos tratar de responder a dos preguntas:

1. ¿Para qué quieren poder los estados?
2. ¿Cuánto poder quieren los estados?

La respuesta al primer interrogante es por el principio ordenador anárquico de autoayuda. Los estados solo dependen de sí mismo y de sus capacidades.

La respuesta a la segunda pregunta es: los estados solo quieren sobrevivir y para ello necesitan seguridad. Adquirir poder es la mejor manera de adquirir seguridad. Evitar que otros estados se hagan más poderosos es una premisa central.

Según John Mearsheimer los estados desarrollan capacidades militares para defenderse de otros estados. El objetivo principal de los estados es su supervivencia. Por otro lado el mayor peligro es que los estados nunca podrán conocer la intención de los demás. Por lo tanto el estado como un actor racional siempre buscara maximizar su poder para sobrevivir (MEARSHIMER, 2006:73-74)

Contexto historico

Fundacion del estado de israel y sus tres guerras

El estado de Israel fue fundado el 14 de mayo de 1948. Al siguiente día tuvo que librar su primera guerra: la guerra por la independencia conocida como IOM HAZMAUT. A pesar de su incipiente ejército, logro una increíble victoria militar y se hizo con más territorio en todos sus frentes. A diferencia de otros países del mundo, este joven país contaba desde temprano con diversos servicios de inteligencia que lo orientaban y ayudaban a lograr la independencia. El primero de ellos se llamó SHAI, el cual tuvo diversas intervenciones y actividades pre independentista. Luego fue disuelto y se creó el SHIN BETH y el AMAN (LA INTELIGENCIA MILITAR ISRAELI) en 1948. Previamente en 1936 se creó la proto estrella de la inteligencia Israel: EL MOSSAD el cual opero hasta la creación del estado el cual en 1951 seria refundado bajo las directivas de Ben Gurion como el corazón de la inteligencia israelí.

Por ultimo en 1960 se creó una unidad de inteligencia separada llamada LEKEM, la cual se dedicaría únicamente a inteligencia científico-tecnológica. En 1985 se disolvió y sus funciones pasaron al ministerio de defensa y al ministerio de ciencia y tecnología.(NEJANKY, 2020: 20-21)

Israel además tuvo que soportar la guerra de los seis días en 1967 en la cual volvió a humillar a los ejércitos árabes agresores lo que le dio la sensación de superioridad militar indiscutible y su talón de Aquiles: el concepto.

La tercer guerra que tuvo que afrontar fue en 1973 conocida como la guerra de IOM KIPUR en donde esa falsa sensación de seguridad que se conoce en Israel como “el concepto” dejo al estado judío en las puertas del caos y la sorpresa estratégica que casi le cuesta una derrota total.

Esta falsa sensación de seguridad conocida como “El concepto” estaba fundada en la confianza excesiva en los servicios de inteligencia israelíes, y sobre todo de sus fuerzas de defensa de la capacidad de reacción con que contaban las fuerzas de defensa de Israel y por último la capacidad de movilizar 600000 soldados en horas a sus puestos de combate debido a un sistema estratégico de movilización y a su poca profundidad estratégica.

A pesar de ello el director del MOSSAD advirtió que la guerra con Egipto y Siria era inminente pero sin embargo el sesgo de “El concepto” fue más fuerte y llevo a no escuchar al General Zamir y la lamentable guerra estallo. Además cabe agregar que también existió un excelente uso de las operaciones de información por parte de los egipcios que filtraron por distintos medios que no atacarían Israel por que no podrían ganar jamás esa guerra.(NEJANKY, 2020)

Con respecto a las operaciones de información, podemos afirmar que no son algo nuevo en la historia militar a pesar de que su doctrina si lo es y se la relaciona con el ciberespacio. Sin ir más lejos Aníbal las utilizo para engañar a los romanos en la batalla de Canae.

Afirmaba el actual comandante del comando estratégico de los Estados Unidos, General John Hyten, que no hay algo tal como guerra espacial y cibernética solo hay guerras. Pero cambios recientes en la doctrina militar Americana le están dando mayor importancia a las operaciones de información dentro de los conflictos. Este cambio ocurrió luego de que el pentágono percibiera como el enemigo hace uso de las mismas y que tanto dentro del campo de batalla como fuera le permiten alcanzar logros tácticos y estratégicos.(VERTULI-LOUDON, 2018:xiii)

“la dificultad para distinguir entre el engaño deliberado y la revelación involuntaria de secretos, de diferenciar señales y ruidos, conduce en ocasiones a la necesidad de tratar a la

información de manera similar, pues todo es ruido hasta que los hechos ocurren" .(NEJANKY, 2020: 63)

Los Israelíes aprendieron la lección y desde 1981 con la doctrina Begin y a través de ataques preventivos que algunos autores incluso identifican como preentivos, debido a que consideran que todo estado tiene derecho a actuar aun cuando la amenaza aun sea potencial, no permitirán jamás que ningún enemigo de Israel ponga en jaque al estado nuevamente ni pueda afectar sus capacidades militares y de disuasión estratégica que posee para poder tener seguridad para su territorio y ciudadanos.

Para poder entender mejor el conflicto que mantiene Israel con Irán, vamos a analizar brevemente como ha sido su relación histórica.

Para ello y al solo efecto de comprender mejor sus antecedentes, dividiremos su análisis en dos periodos:

1. D, durante el periodo del Shah Reza Pahlavi, un aliado de occidente y en especial de Estados Unidos, en el cual Israel incluso cooperaba con Irán y en el cual los estados unidos le transfirió tecnología nuclear para usos pacíficos sobre todo de energía.
2. Un segundo periodo en donde el Sha abuso de la confianza y trato de tener un desarrollo nuclear con fines militares para lo cual se le retiro todo el apoyo y luego de la revolución del ayatollah Khomeini en adelante que se volvió a la idea de tener el arma nuclear.

Periodos de las relaciones de occidente con iran

Primer periodo

En el primer periodo que comienza durante la segunda guerra mundial y termina en 1979 y se caracteriza porque existe una colaboración e interés en Irán por parte de Estados Unidos y Gran Bretaña. Luego de la guerra también se interesa por el país persa la URSS compitiendo por concesiones petroleras.

Desde su creación en 1948, el estado de Israel causo gran conmoción en medio oriente. Aliado de estados unidos, occidental, anticomunista y contrario a los intereses de los países árabes de la región. Pero irán hay que recordar que no es un país árabe sino persa porque no se hable árabe sino Persa o Farsi. Israel luego de sus tres guerras pudo comenzar a identificar a sus enemigos en la región y a establecer cuáles eran sus prioridades y amenazas a su seguridad nacional. Por otro lado en 1968 irán firma el Tratado de no proliferación nuclear. Estados unidos provee de combustible nuclear con fines pacíficos durante 10 años. Pero el Shah tenía otras intenciones con el programa nuclear. En 1979 Khomeini se hace del poder en Irán y funda un estado teocrático contrario a occidente a diferencia del Shah y empieza a apoyar a grupos de izquierda como Hezbollah.(GOMEZ, 2017:7)

Segundo periodo

Como mencionamos ut supra este segundo periodo comienza con la toma del poder del ayatola Khomeini en 1971 y la fundación del califato que tiene como característica la impronta religiosa que tomaría el país de aquí en adelante.

Este es un periodo muy conflictivo, se crean varias organizaciones terroristas sobre todo para disputarle la soberanía a Israel e Irán las apoya con logística, armamentos, entrenamiento y financiación. El caso de Hezbollah en Líbano es un caso paradigmático porque crea un estado dentro de otro estado, participa en política y también tiene un ala que lleva a cabo operaciones terroristas en conjunto con Irán. Luego Irán tuvo una larga guerra con Irak en la cual salió

victorioso este último. Y de esta manera el ayatola se convenció de que necesitaban retomar el programa nuclear militar para tener disuasión. Como Estados Unidos ya no colaboraba en el programa, Irán busco nuevos socios como Pakistán y China para la transferencia de tecnología nuclear. China quien se había comprometido a venderles un reactor nuclear desistió como resultado de las presiones que ejerció estados unidos pero sin embargo esto no acabo con el programa nuclear Iraní. Israel ve con preocupación a Irán y a su programa nuclear teniendo en cuenta además de su cercanía, su patrocinio al grupo libanes Hezbollah y luego a Hamas y la posibilidad de que le entregue algún tipo de arma nuclear táctica. Esto empeora en 2001 cuando Irán comienza con su construcción subterránea en la ciudad de Natanz de una central nuclear para enriquecimiento de uranio. Comienzan las negociaciones internacionales para que irán detenga su programa nuclear pero para Israel esto no es suficiente. Si Irán consiguiera el arma nuclear además de una amenaza real al estado judío, implicaría un desbalance de poder regional que Israel no estaba dispuesto a aceptar. La decisión final de Israel de actuar preventivamente es tomada finalmente cuando el presidente de Irán anuncia que está dispuesto a construir 10 centrales nucleares nuevas. (GOMEZ, 2017:14)

Stuxnet

STUXNET no es solo la primer ciber arma de la historia sino es un hito que marca un antes y un después en la historia de la guerra. En el S XX las guerras se llevaban a cabo en enfrentamientos directos de sus fuerzas armadas. Con su ejército, fuerza aérea y armada enfrentaban cada conflicto bélico que ocurría. La historia cambio un poco durante la guerra fría. Luego de finalizada la segunda guerra mundial, los dos superpotencias ganadoras decidieron batirse a duelo por el dominio mundial. Pero existía un problema. No se podían enfrentar directamente porque ambos contaban con misiles nucleares y así se establece la doctrina de la mutua destrucción asegurada. Entonces la guerra se daría en la cabeza y en los corazones de los países alineados ideológicamente a uno u otro bando y el enfrentamiento entre estos iría demarcando quien sería el verdadero hegemon mundial.

En 1991 se produce la ruptura del sistema bipolar con la implosión de la Unión de Repúblicas Socialistas Soviéticas(URSS) que se encontraba exhausta por el esfuerzo que significó la carrera armamentística denominada iniciativa de defensa estratégica por un lado y, por el otro lado al haber fracasado el modelo propuesto por el comunismo el cual, prima facie, no pudo mejorar la vida de sus connacionales. Estados Unidos de América surgió como única potencia dominante al desaparecer el imperio soviético (Ozaran, 2006). Con el final de la Guerra Fría también comenzaba a delinearse lo que en relaciones internacionales es denominado nuevo orden mundial. Este denota cambios sustanciales con respecto al orden vigente durante la Guerra Fría en especial en cuanto a “las reglas de juego y a la distribución de poder” (Bartolomé, 2006, p., 76) Ozaran (2006 p., 20)opina que este nuevo orden mundial “no surgió por la globalización, la caída del muro de Berlín o la desintegración de la ex Unión Soviética sino que la suma de todos estos hechos fueron preparando el camino”.

Por otro lado hay que tener en cuenta como bien afirma Bartolomé (2006, p., 78) “nunca antes existió tanta democracia como en los inicios de la post Guerra Fría. Esto auguraba para los neo internacionalistas liberales un sistema internacional de baja conflictividad”.

El 11-S lo cambió todo, con él se esfumó definitivamente la idea que sostenían los neo internacionalistas liberales acerca de la baja conflictividad que deparaba el nuevo orden mundial. Se tuvo en cuenta la baja conflictividad interestatal pero no la de otro tipo de conflictos, ya sean transnacionales o intraestatales.

El siglo XXI incorporo un nuevo ambiente operacional a la guerra: el ciberespacio. Los conceptos de teatros de operaciones como espacios, duración de la campaña como tiempo y poder de combate como medios empiezan a perder algo de sentido y los estados comienzan a

pensar que las ciber armas tiene la capacidad de alterar la forma tradicional de hacer la guerra. Para poder estar a la altura de las circunstancias hace falta tener una estrategia de ciberdefensa, capacitar recursos humanos, desarrollar armas cibernéticas y ver la forma de adecuar todo esto al derecho interno e internacional(STEL,2005)

Según Koybko la revolución digital cambio los modos de vida social, política y económica y el ciberespacio pasó a ser otro teatro de guerra. Por otro lado hace más de 2000 años Sun Tzu entendió que era mejor la guerra por medios indirectos(2019:21)

Steven Metz ha manifestado que ha manifestado que la idea de asimetría hacía referencia a algún tipo de diferencia para tener algún tipo de ventaja sobre el adversario. Por lo general pretenden generar un impacto psicológico, que obste la iniciativa, libertad de acción o deseos del enemigo. (Bartolomé, 2006)

Las operaciones de información buscan dañar, destruir modificar la información contenida en las redes o sistemas de información para cambiar las percepciones de la población local e incluso del personal militar. (STEL,2005)

Por otro lado según Alvin Toffler el conocimiento es “el recurso central de la destructividad así como lo es de la productividad” la forma en que hacemos la guerra siempre es la misma de la que hacemos la riqueza. También afirma Toffler que la información se está convirtiendo en el recurso principal de la guerra.(VERTULI-LOUDON, 2018:9-10)

Ya son muchos los autores que afirman que la ciberguerra es la guerra por excelencia en el S XXI. Esto no quiere decir que la guerra convencional vaya a desaparecer. Es una guerra más propicia, barata y sin sangre. Lo único que se necesita es contar con la infraestructura y los recursos humanos pertinentes que son mucho más económicos que los recursos convencionales y un solo ciber soldado puede apagar una ciudad entera, dejarla sin transporte o envenenar las aguas. Por otro lado esto da lugar a conceptos como el de ciberguerra que es llevada a cabo por estados contra otros estados dirigida a dañar gravemente las capacidades del enemigo, para sustraerle información clasificada, sabotear sus infraestructuras críticas. La guerra cibernética se caracteriza por su asimetría, complejidad, objetivos limitados, etc.(MADERO, 2012:125)

Podemos decir que un cibera taque es una acción realizada en el ciberespacio para penetrar, causar daño, afectar, destruir sistemas informáticos, computadoras o dispositivos controladas por ellas. Para ello se valen de malware o programas maliciosos como virus o troyanos. Podemos decir que existen tres principales clases de cibera taques: los que perturban tomando el control de infraestructuras críticas como el SCADA y su intención es causar un daño físico. Cibera taques no intrusivos como los de DDoS y por último los intrusivos usados con el fin de conseguir información a través de malware info-stealer que se usan para actividades de ciberespionaje. En el caso de Israel está dentro de la órbita del MOSSAD, a través de su unidad especial Kidon, y la unidad 8200 de AMAM de las FDI. Normalmente combinan los ataques ciber con operaciones convencionales y no convencionales sobre todo de fuerza aérea bombardeando blancos específicos, sabotajes por detonación de explosivos, sumado a otras operaciones especiales de inteligencia como asesinatos selectivos para retrasar el programa nuclear Iraní (ROCA, 2013:8)

En el año 2010 es detectada la ciber arma STUXNET por la empresa de seguridad informática Bielorrusa VirusBlokAda. La particularidad de este gusano es que aprovecha la vulnerabilidad de MS10-4416 del sistema operativo Windows CC, que funcionan con los sistema del tipo SCADA, de la empresa Siemens y tiene la particularidad de atacar infraestructuras criticas como oleoductos, plataformas de petróleo, centrales nucleares, eléctricas, etc. y permite sabotearlos. Este virus troyano no se introduce a través de internet sino está diseñado para hacerlo a través de una memoria USB. Una vez que es introducido el USB en una de las computadoras, se oculta en el Rootkit firmando con certificados previamente robados a los

fabricantes del hardware. Después de ello se mantiene oculto y camuflado hasta que su director decide activarlo. De ahí en más se multiplica a si mismo e infecta todas las computadoras de la intranet permitiendo a su autor robar información o sabotear el sistema ocultando los cambios. Técnicamente usa para propagarse el archivo autorun.inf y aprovecha una vieja y conocida vulnerabilidad LNK del día cero que hace que con solo ver los archivos en Windows, se ejecutan automáticamente y a través de recursos de red compartidos se propaga. Lo más destacable de STUXNET, que es considerada la mejor ciber arma hasta ese momento inventada es que se trata del primer rootkit que se preparó para atacar el sistema SCADA. El resultado lo conocemos:20 % de las centrifugadoras destruidas en la planta de Natanz.(SANCHEZ MADERO, 2012:129-130)

Como bien es sabido en ciberdefensa el problema de la atribución es difícil de lograr. Por declaraciones posteriores de altos funcionarios Israelíes y norteamericanos, STUXNET habría sido un desarrollo conjunto pero ejecutado por el MOSSAD a través de una operación de HUMINT que consistió en dejar abandonados varios pen drives llamativos en el estacionamiento de la planta nuclear de Natanz para que alguno o varios de sus empleados los conecten a un puerto USB e infecten el equipo.

Este tipo de ciber armas es conocida como fire and forget(disparar y olvidar) lo estratégico de STUXNET es que pudo atacar y reprogramar el equipo blanco. Este ataque afecto a los niveles físicos, lógicos, de información, etc. Este tipo de refinamiento en los conocimientos apunta a que solo un estado o conjunto de ellos estaban en capacidad de desarrollarlo. Tanto el NY Times como un experto en seguridad informática de Alemania apuntan a Israel y Estados Unidos e incluso van más lejos afirmando que pudieron utilizar sus propias centrales nucleares para probar el arma cibernética. Por otro lado el mismísimo SNOWDEN afirmo que STUXNET fue desarrollado en conjunto por Israel y Estados Unidos. Si bien en el momento del ataque Irán desmintió daños, más adelante el presidente Ahmadinejad lo admitió pero minimizando su verdadero alcance. *“ Stuxnet evidencia que este tipo de armamento es real y tiene la capacidad de afectar estructuras criticas del estado”* .(GOMEZ, 2017:18-20)

Consecuencias de stuxnet

Como bien nos ilumina el maestro de la diplomacia internacional, Henry Kissinger, antes de la ciber era se podía hablar de distinciones entre periodos de paz y de guerra. Los servicios de inteligencia existían para evaluar y en algunos casos intervenir en el desarrollo de capacidades de otros estados. Un actor en solitario contando tan solo con algunos conocimientos específicos y un ordenar puede acceder al ciberespacio y destruir infraestrtura critica desde un cuasi anonimato.(KISSINGER, 2016:345)

Irán comprendió que había sido sorprendido por lo que Nassim Taleb denomino “Cisne Negro” que es un suceso que ocurre por sorpresa, que nadie vio venir o lo pudo prever y que tienen un gran impacto y repercusiones trascendentales.(SANTANDER.ES, 2021)

Entonces el presidente Iraní comprendió que comenzaba una nueva era, con nuevas amenazas, en especial en el campo del ciberespacio y que hacia falta destinar recursos financieros, tecnológicos y humanos para librar guerras en el quinto dominio. Creo una unidad de ciberdefensa tanto pasiva como activa. Y desde entonces empezaron a intercambiar cibera taques con Israel hasta el día de la fecha conjuntamente con operaciones especiales de inteligencia como sabotaje y asesinatos.

Oficiales de alto rango de la CIA identificaron a Irán como responsable del ataque a la empresa Saudí Aramco utilizando el malware SHAMOON. También lo señalan como responsable de ciber ataques a entidades bancarias de Estados Unidos ese mismo año. (ROCA, 2013:42)

Y entonces hizo su aparición FLAME: una nueva Ciberarma que supera a su antecesor STUXNET. Esto reafirma que las Ciberarmas son para Israel una parte importante de su

estrategia en el ciberespacio en contra de Irán. Esta nueva ciber arma es un gusano de ciberespionaje que afecto a varios países de medio oriente. La empresa de seguridad informática Kaspersky determino que fue utilizada para un sabotaje al sector petrolero iraní.

Flame comparte muchas características con STUXNET aunque el primero se considera el más complejo detectado hasta el momento. Esta herramienta de ataque básicamente da acceso a un backdoor, funciona como un troyano y logra infectar redes locales, unidades removibles a través de comandos remotos. Además en lugar de destruir como STUXNET, espía de manera invisible. También tiene funciones de ataque. Una vez infectada la maquina permite robar archivos, cambiar la configuración remota, encender micrófonos para grabar , interceptar la información ingresada por teclados, capturar pantallas y chats y también interferir comunicaciones telefónicas por VoIP.(BEJARANO, 2012:1-4)

En la actualidad existe o más bien continúa desde STUXNET una guerra soterrada entre Irán e Israel que combina el ciberespacio con operaciones encubiertas y especiales.

Irán sufrió doce misteriosos ataques entre junio y julio de 2020 consistente en incendios y explosiones. Esto ocurrió luego de que un cibera taque por parte de Irán hacia Israel intentara dañar a la población civil envenenando su agua potable elevando los niveles de cloro. Esto elevo la ciberguerra entre ambos países llevándola a terrenos físicos como advertencia.

El 23 de abril de 2020 Israel detecto alteraciones en una planta de agua potable donde hackers cambiaron los niveles de cloro y de químicos del agua que podrían haber sido fatales. Israel determino que el ataque se produjo desde Irán utilizando servidores europeos y americanos. El director nacional de Ciber de Israel declaro en ese momento que se cruzaron todas las líneas rojas. La primer contra respuesta fue un cibera taque al puerto iraní de Sajid rajaee. El Washington post se lo atribuyo a Israel. La guerra en el quinto dominio es cada vez más común entre estados, daña sin ser divisado y evita escaladas militares.(INSEG.ES, 2020)

Conclusiones

Dice Henri Kissinger que “cada época tiene su leiv motiv” osea una cosmovisión en la cual basar nuestras ideas y creencias dándonos un paradigma para entender al mundo. “ en la época medieval era la religión, en los siglos xix y xx fue la ilustración y su fe en la razón humana… en el s xxi es la ciencia y la tecnología… estas han permitido más avances que en cualquier otra época pero también han creado armas capaces de destruir a la humanidad…”(KISSINGER, 2016:331)

Durante el desarrollo del presente trabajo final integrador logramos demostrar nuestra hipótesis acerca de que STUXNET logro retrasar los planes nucleares iraníes y que a partir de entonces Israel continuo con su doctrina de cibera taques para colaborar con el mantenimiento del status quo vigente regional sin llegar a un enfrentamiento en el mundo físico o por lo menos acotándolos a ciertos sabotajes y algún asesinato selectivo de algún científico nuclear iraní.

Está claro que Israel desde la doctrina Begin en adelante se ha manejado en un marco teórico de las relaciones internacionales del neorrealismo dado que actuó en un sistema internacional anárquico donde cada estado solo busca poder frente a otros estados para asegurar su supervivencia que está directamente relacionada con sus capacidades militares. En este caso concreto Israel debilito las capacidades nucleares de Irán para no desbalancear el poder regional que encabeza. Como Kenneth Waltz Israel le da suma importancia a la estructura en donde interactúan las unidades dentro del sistema internacional.

Referencias bibliográficas

- Bibliografía Teórica

Bartolomé, M. (2006). La seguridad internacional en el siglo XXI, Más allá de Westfalia y Clausewitz.Academia Nacional de estudios políticos y estratégicos. Ministerio de Defensa, Chile.

Bejerano, M. Jose(2012) en línea:https://dialnet.unirioja.es/descarga/articulo/7468740.pdf flame: una nueva amenaza de ciberespionaje.

Buzan, B. (1998). Security, A new Framework for Analysis. Lynne Rienner Publishers, Boulder-Colorado.

Calle, F. y Merke, F. (2004). La Estrategia de Seguridad Nacional de EE.UU. en la Era Bipolar. Agenda Internacional Año 1, N° 3, Diciembre 2004. Enero/Febrero 2005.

Cardona, D.; Duarte, I. y Jiménez, N. (2004). La Estrategia de Seguridad Nacional de los Estados Unidos en la Administración Bush: Una Lectura desde América Latina. CEPI, Universidad del Rosario, Bogotá.

CIDOB. Anuario Internacional 2008, 2007, Claves para interpretar la política exterior española y las relaciones internacionales en 2007, relaciones de la Unión Europea con la Federación Rusa. Recuperado de http://www.cidob.org.

Clarke, R. (2004). Contra todos los enemigos. Taurus. Buenos Aires.

González, R. (2010). La Estrategia de Seguridad Nacional de los Estados Unidos. Publicado en el Consejo Argentino para las Relaciones Internacionales. Recuperado de www.cari.org.ar. .

Jiménez, B. F. (2011). Racionalidad pacífica. Una introducción a los Estudios para la paz. Dykinson, Madrid.

Kepa, Sodupe(2003) “la teoria de las relaciones internacionales a comienzos del siglo xxi”, Universidad del Pais Vazco.

Korybco, Andrew(2019) “guerras hibridas. revoluciones de colores y guerra no convencional”, Batalla de ideas

Kissinger, Henry(2016) “orden mundial”, Ed Debate, Bs As

Lobell, S. E., Ripsman, N. M. y Taliaferro, J. (2009). Neoclassical Realism, The State And Foreign Policy. Recuperado de https://core.ac.uk/download/pdf/233941226.pdf.

Llinas Gomez, Alejandro(2017) “analisis del ciberataque para la seguridad de los estados y su incidencia en la transformacion del status quo: stuxnet el virus informatico”, Universidad del colegio mayor de nuestra Sra. Del Rosario, Bogota.

Medero, Gema(2012) https://dialnet.unirioja.es/servlet/articulo?codigo=4331298La ciberguerra: los casos de Stuxnet y Anonymous

Mearsheimer, J. (2001). The Tragedy of Great Power Politics. W.W. Norton & Company, E.E.U.U.

Mijares, V. M. (2015). Realismo neoclásico: ¿El retorno de los estudios internacionales a la ciencia política? Revista de Ciencia Política / Volumen 35 / Nº 3 / 2015 / 581 – 603.

Mingst, Karen(2006) “fundamentos de las relaciones internacionales”, CIDE

Nejanky, Paul(2020) “las fallas de la inteligencia israeli. analisis de una sorpresa en la guerra de iom kipur”.punto aparte.

Rodríguez Moreno, A. (2013). Giorgio Agamben y los Derechos Humanos: Homo Sacer I, el poder soberano y la nuda vida. Recuperado de

www.academia.edu/2091837/giorgio_agamben_los_derechos_humanos_homo_sacer_I.

Roca Xavier(2013) https://dialnet.unirioja.es/servlet/articulo?codigo=7494996ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de irán: de la neutralización selectiva de objetivos al "cuerpo ciber" iraní

Rubbi, L. (2018). Guerra asimétrica: La estrategia de defensa de la República Popular China en el período 2012 – 2016. Tesis de maestría. Universidad Torcuato Di Tella, Buenos Aires.

Stel. Enrique(2005)" guerra cibernetica", Circulo Militar

Valdez Ugalde, J. L. y Duarte, F. (2013). Del poder duro al poder inteligente. La nueva estrategia de seguridad de Barack Obama o de la sobrevivencia de la política exterior de Estados Unidos. Norteamérica, Año 8, número 2, julio-diciembre de 2013.

Vertuli, -mark y Loudon, Bradly(2018) "percepciones son realidades", Circulo Militar

Walt, S. M. (1985). Alliance Formation and the Balance of World Power. International Security, 9(4), 3-43.

Waltz, K. N. (1979). Theory of international politics. Addison, Wesley.

Zakaría, F. (2008). The Post-American World, Allen Lane, New York.

Bibliografía Metodológica

Maxwell, J. (1996). Qualitative Research Design. An Interactive approach. Sage Publicatios. Recuperado de http://catedras.fsoc.uba.ar/guemure/bibliografia/Maxwell1.pdf.

Taylor, S. y Bogdan, R. (1987). Introducción a los métodos cualitativos de investigación: La búsqueda de significados. Editorial Paidós Básica, Barcelona.

Vasilachis, I. (2006). Estrategias de Investigación Cualitativa. Gedisa, Barcelona.