FACULTAD DE CIENCIA POLÍTICA
Y RELACIONES INTERNACIONALES
UNIVERSIDAD NACIONAL DE ROSARIO

Licenciatura en Relaciones Internacionales

Tesina de grado

"La política de ciberseguridad iraní en el ámbito doméstico e internacional (2009 - 2021)"

Alumna: Bianca Lombardi

Director: Ruben Paredes Rodríguez

Fecha: 22/5/2023

Índice

Agradecimientos

A mi familia, que me acompañó y me apoyó desde el inicio de este camino. Gracias por confiar en mí, por darme aliento cuando lo necesité y por celebrar conmigo cada pequeño hacia la meta. Son la base fundamental de este gran logro.

A Alejo, mi compañero de vida, quien estuvo al lado mío durante todo el proceso, siempre con tanto amor y paciencia. Gracias por tu incondicionalidad y tu compañía lo largo de todos estos años.

A mis amigos. Los de siempre, los nuevos, los de la facultad. Gracias a cada unos de ellos por hacer que todo sea más fácil; y por tantos momentos compartidos, los buenos y los no tan buenos que nos ayudan a crecer.

A Rubén Paredes, quien dirigió y corrigió esta Tesina. Y a la FCPOLIT, por tantos años de educación pública y de calidad.

Introducción

Las tecnologías emergentes y el uso cada vez más intensivo y extensivo de Internet han derivado en un alto grado de interdependencia a nivel global. Consecuentemente, este fenómeno trajo aparejado una preocupación cada vez más presente en las agendas estatales: maximizar la protección ante los ataques ocurridos en el ciberespacio. En términos de seguridad y defensa, este ámbito debe ser entendido como un dominio comparable con otros escenarios militares tradicionales - como son el mar, el aire, la tierra y el espacio -; excepto que aquí el *target* es primordialmente la información (Paredes Roibás, 2018).

Una de las mayores dificultades al momento de diseñar políticas ligadas al ciberespacio, radica en identificar las atribuciones de los ataques. Siguiendo a Newmeyer, Cubeiro y Sánchez (2015) "a diferencia de los ataques militares históricos, la estela de un cohete cibernético no deja trazos que marquen el punto de lanzamiento" (p. 83).

Al mismo tiempo, la habilidad de los actores no estatales para perpetrar ciberataques complejiza la definición de la respuesta que un Estado puede dar a esta agresión (Tsagourias, 2012). Por último, otro aspecto que obstaculiza la comprensión de los ciberconflictos, es que el ciberespacio ha sido creado exclusivamente por el hombre y con fronteras inciertas, por lo que abundan en esta materia las lagunas legales (Newmeyer, Cubeiro y Sánchez, 2015).

Desde la aparición del ciberespacio, los países del Medio Oriente y Norte de África (*MENA* por sus siglas en inglés) realizaron grandes esfuerzos para incrementar su ciberpoder. Para muchos Estados de la región, este nuevo dominio representó oportunidades para consolidar la autoridad gubernamental y modificar el equilibrio de poder regional, facilitando el desarrollo de guerras asimétricas (Lubin, A. 2020).

En junio de 2010 investigadores de Kaspersky[1] y Symantec[2] descubrieron *Stuxnet*, un virus seis veces más pesado que otros *malwares* que tuvo como principal blanco a la República Islámica de Irán. Investigadores de las mencionadas compañías observaron que el virus dañó severamente los PLC[3] (Programmable Logic Controller) que programaban y controlaban las

[1] Fundada en Moscú en 1997, la empresa se especializa en productos que brindan seguridad informática, firewall, anti-spam y antivirus.

[2] Es una compañía californiana creada en 1978 que ofrece servicios de seguridad de la información.

[3] Un PLC (Programmable Logic Controller) es un controlador de programación que activa los componentes de la maquinaria para que desarrollen actividades automáticas o potencialmente peligrosas para las personas.

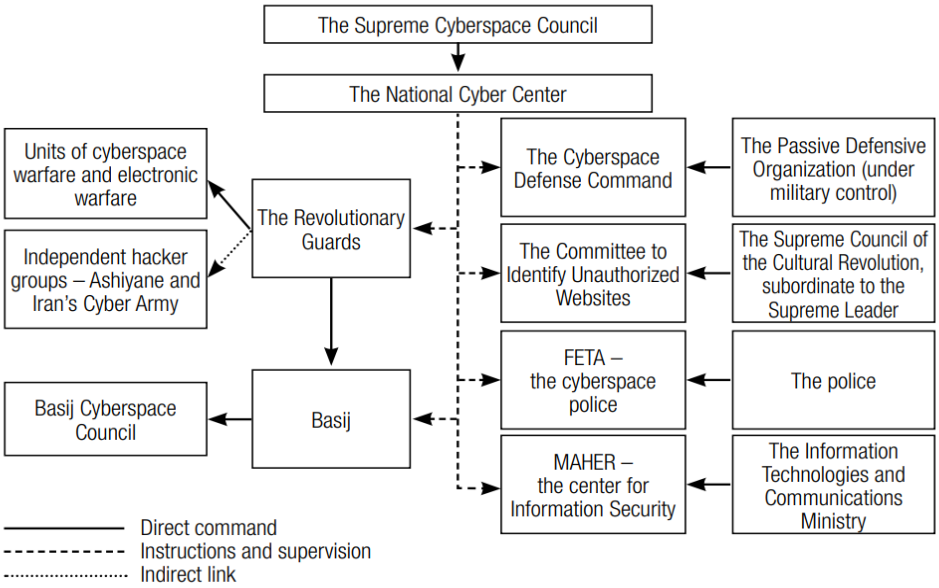
centrifugadoras de uranio en las plantas nucleares de Natanz y Bushehr, causando serios retrasos en el programa nuclear iraní. Si bien debido a la naturaleza del ataque no ha sido posible acceder a pruebas respecto a su procedencia, gran parte de la bibliografía consultada afirma que se trató de una operación realizada de forma conjunta entre los servicios de inteligencia de EE.UU. e Israel. De acuerdo a Sanger (2011), el virus fue desarrollado en Maryland (EE.UU.) por la Agencia de Seguridad Nacional (NSA) y la Agencia Central de Inteligencia (CIA), y testeado en Israel.

Ocurrida esa ofensiva - también conocida como *Operación Juegos Olímpicos* - la búsqueda por incrementar los recursos de ciberseguridad se convirtió en un objetivo fundamental de la política iraní, tanto a nivel doméstico como internacional. La misma se nutrió de dos supuestos fundamentales: el primero se refiere al desarrollo de capacidades defensivas para resistir ataques externos de naciones y entidades hostiles al régimen[4], así como también operaciones por parte de oponentes al gobierno en el frente interno; el segundo alude a las capacidades ofensivas, enfocadas principalmente en incrementar el desarrollo de ciberataques que permitan a Irán posicionarse como un potencia en materia cibernética.

Esto dio inicio a la construcción de un tejido de instituciones relacionadas al ciberespacio. Se estructuró una organización jerárquica con un plan de acción claro; asignaciones de recursos estratégicos; y con la capacidad de preservar y difundir información, *know-how* y datos relevantes.

El organigrama a continuación recuperado de Siboni y Kronenfeld (2012) nos permite comprender cómo se estructura dicho entramado, y cuál es la lógica organizacional:

[4] El régimen espera evitar la penetración de ideas e información occidentales a través del ciberespacio que entran en conflicto con sus intereses; evitando así el desencadenamiento de una *soft revolution* (Siboni y Kronenfeld, 2012).



Dentro de las *instituciones defensivas*, destacamos las siguientes:

El ***Consejo Supremo Cibernético*** es el organismo de más alto nivel encargado de tomar decisiones determinantes en materia de ciberseguridad (BBC Persian, 2018). Creado en 2012, está encabezado por el presidente iraní y compuesto por representantes gubernamentales de alto rango - entre los que se encuentran el comandante superior de la Guardia Revolucionaria, el jefe del Majlis, los Ministros de Ciencia, Comunicaciones y Cultura, el jefe de policía y el presidente de la organización de propaganda islámica - que trabajan en la planificación e implementación de una estrategia unificada en el ciberespacio [5](Siboni y Kronenfeld, 2012).

El consejo fundó bajo sus auspicios el ***Centro Cibernético Nacional***, a los fines de integrar toda la actividad del ciberespacio iraní, reunir y difundir información e instrucciones, y supervisar la aplicación de las directivas del Consejo por todos los organismos pertinentes (Siboni y Kronenfeld, 2012).

Por su parte, el ***Comando de Defensa del Ciberespacio*** es una organización central, que opera dentro de la Organización de Defensa Pasiva, perteneciente al Estado Mayor de las Fuerzas Armadas (Siboni y Kronenfeld, 2012). Su principal objetivo es desarrollar una doctrina defensiva integral para las instituciones estatales e infraestructuras contra las ciberamenazas.

[5] De hecho de acuerdo a Craig y Valeriano (2016) el presupuesto destinado al Consejo Supremo Cibernético en el año 2014 fue de $40 millones de dólares; el mayor presupuesto de TIC de Irán.

A su vez, este creó el ***Centro de Inspección de Delitos Organizados***, cuyo propósito es investigar el crimen organizado, el terrorismo, el espionaje y los delitos económicos en el espacio virtual (Golkar, 2011).

Bajo aspicios del el Centro Cibernético Nacional, también se fundó el ***Centro para la Seguridad de la Información*** - también conocido como ***MAHER*** - el cual opera en el marco del Ministerio de Comunicaciones y Tecnologías de la Información. Es el principal responsable de activar una respuesta inmediata ante incidentes de seguridad informática y ciberataques. Este centro también capacita a los recursos humanos sobre conocimientos técnicos en materia de almacenamiento y seguridad de datos. Asimismo se ocupa de defender los sitios *web* del gobierno, y los de aquellas las empresas privadas que operan en su favor.

La ***Comisión de Identificación de Sitios Web Desautorizados*** es una agencia que se concentra principalmente en el control de actividades cibernéticas intra iraníes que van en contra de los intereses del régimen. Tal cual su nombre lo indica, el propósito de la Comisión es identificar los sitios *web* cuyos contenidos y actividades sean incompatibles con los principios del gobierno, y está autorizado a bloquear el acceso a dichas páginas. Cada proveedor de Internet o ISP - en inglés Internet Service Provider - trabaja bajo la jurisdicción de la Autoridad Reguladora de la Comunicación de Irán, la cual hace cumplir las políticas de censura establecidas por la Comisión para identificar los contenidos ofensivos.

Finalmente, la última de las organizaciones defensivas es la ***Policía para la Esfera de la Producción e Intercambio de Información*** - mejor conocida como ***FATA*** -, creada en 2011 con el objetivo de contar con una unidad policial en el ciberespacio. Su rol se centra en investigar y combatir delitos cibernéticos - tales como el fraude, el robo de información personal y propiedad intelectual, entre otros -, así como también monitorear redes sociales de usuarios iraníes y cibercafés (BBC Persian, 2018).

Con relación a las *capacidades ofensivas*, se destacan fundamentalmente dos organizaciones:

El ***Ejército Cibernético Iraní,*** un grupo compuesto por especialistas altamente calificados en tecnología de la información y hackers profesionales. Entre sus tareas más importantes, se destacan desarrollar *software* infectados mediante la inserción de códigos maliciosos en programas informáticos falsificados capaces de reproducirse en redes y equipos de los *targets*; generar capacidades para bloquear las comunicaciones y las redes WiFi; y crear herramientas que recopilen datos y los envien a servidores remotos (BBC Persian, 2018). Un gran número de académicos con conocimiento en el tema sostiene que este grupo de hackers está

directamente vinculado con la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés), por lo que apuntan fundamentalmente a irrumpir cualquier tipo de influencia occidental mediante sitios *web* y aplicaciones, redirigiendo el tráfico de información hacia páginas pro-iraníes (Siboni y Kronenfeld, 2012).

Sumado al Ejército Cibernético Iraní, se creó otra institución denominada ***Fuerza Paramilitar Basij.*** El papel más relevante de la misma es garantizar el apoyo de la población al régimen mediante la publicación de contenido a favor del gobierno en blogs y redes sociales (BBC Persian, 2018). La evidencia indica que esta institución también está fuertemente relacionada con la IRGC (BBC Persian, 2018).

Como se puede observar, desde el ataque de *Stuxnet* Irán ha realizado grandes esfuerzos destinados a incrementar sus recursos cibernéticos, en el marco de una política de ciberseguridad que se ha acelerado e intensificado desde 2010. La misma se ha aplicado a través de distintos canales y herramientas tanto en el ámbito doméstico como internacional.

En el nivel interno, el gobierno apunta a controlar la divulgación de ideas y la propagación de movimientos en contra del régimen, monitoreando a políticos opositores, periodistas, minorías religiosas no afines al chiismo, figuras populares y organizaciones terroristas contrarias al gobierno. El hecho de que el Movimiento Verde[6] en 2009 se haya organizado a través de las redes sociales suscitó un punto de inflexión en la relevancia que adquirió la política de ciberseguridad aplicada al ámbito doméstico.

Concretamente, se observa que luego de ocurrido dicho Movimiento, se iniciaron procesos para diseñar una estructura de red nacional propiamente iraní. Para el año 2012, se estima que alrededor de 10.000 computadoras ya incluían el sistema propio de Internet *Halal Internet* (Berman, 2013). En suma, aplicaciones como *Facebook*, *Twitter*, *Telegram* y *Google Plus* - además de páginas relacionadas a salud, ciencia, deporte y compras - fueron prohibidas; a la vez que se creó la plataforma *Mehr* como alternativa a YouTube (Bowen y Marchant, 2018).

En el nivel externo, la República Islámica aspira a capitalizar ciberpoder con el fin de que las capacidades cibernéticas actúen como un factor de disuasión militar ante cualquier ataque convencional que se lleve a cabo en contra de Irán; y tiene el foco puesto principalmente sobre

[6] El Movimiento Verde iraní fue una corriente ideológica de carácter liberal formada por grupos con diferentes finalidades políticas y sociales, que reclamaban por el respeto a los derechos civiles y elecciones verdaderamente libres en el país. Este movimiento estuvo mayormente representado por intelectuales, jóvenes, mujeres y minorías étnicas (Castro Torres, 2019).

EE.UU., Israel y Arabia Saudita. Una de las mayores ventajas que tiene el país persa en este campo, es que gran parte de la infraestructura continúa siendo controlada por sistemas mecánicos - no cibernéticos -, lo que naturalmente reduce las vulnerabilidades a las que se expone en este campo.

A su vez, Irán presta apoyo cibernético a grupos y organizaciones *proxies* como el Ejército Cibernético Yemení, el Ejército Electrónico Sirio y Hezbolá (Daricili, 2019); en el contexto de rivalidad con Arabia Saudita e Israel por el liderazgo en la región de Medio Oriente.

En síntesis, se observa que la política de ciberseguridad iraní a nivel interno y externo contribuye al propósito mayor de proteger la integridad del régimen y posicionar a Irán como potencia regional.

De este modo, cabe preguntarse ***¿Cómo se desarrolló la política de ciberseguridad de Irán en el ámbito doméstico e internacional en el período 2009 - 2021, y cuáles fueron sus resultados?*** De dicho interrogante se desprenden las siguiente preguntas específicas:

- ¿Cuáles fueron los principales objetivos, *targets* y herramientas de la política de ciberseguridad iraní a nivel doméstico?
- ¿Cómo se desarrolló la política de ciberseguridad persa en su accionar externo, en el marco de la rivalidad con EE.UU., Arabia Saudita e Israel?
- ¿Cuáles fueron los resultados de la política de ciberseguridad iraní en la dimensión doméstica e internacional?

Se sostiene como ***hipótesis*** principal que luego de ocurrido el Movimiento Verde en 2009, y de los ataques del virus *Stuxnet* a las centrifugadoras de uranio en la planta nuclear de Natanz y Bushehr en 2010, Irán intensificó su política de ciberseguridad - tanto en materia defensiva como ofensiva - en el ámbito doméstico e internacional, logrando proteger la integridad del régimen y posicionar a la República Islámica como potencia cibernética regional.

El ***objetivo general*** de esta investigación es analizar la política de ciberseguridad iraní en la dimensión doméstica e internacional en el período 2009 - 2021, y los resultados de la misma.

En tal sentido, los ***objetivos específicos*** son los siguientes:

- Examinar los principales objetivos, *targets* y herramientas de la política de ciberseguridad iraní a nivel doméstico.

- Estudiar la política de ciberseguridad de la República Islámica en el plano internacional; en el marco de la rivalidad con EE.UU., Arabia Saudita e Israel.
- Analizar cuáles fueron los resultados de la política de ciberseguridad en la dimensión doméstica e internacional que le permitieron alcanzar los objetivos de proteger la integridad del régimen y posicionar a Irán como potencia regional cibernética durante el periodo de estudio seleccionado.

La irrupción del ciberespacio a finales del siglo XX vino a romper con el esquema de teorías de las relaciones internacionales existente hasta el momento. Si bien la teorización en torno a este fenómeno está lejos de ser exhaustiva, el ***marco teórico-conceptual*** de este trabajo incorporará aportes de la ***teoría realista*** y de la ***teoría de la interdependencia compleja.*** En suma, se definirán conceptos que nos permitirán abordar el desarrollo de las nuevas tecnologías cibernéticas en las relaciones internacionales.

La primera perspectiva teórica, nos permite comprender nuestro objeto de estudio - la política de ciberseguridad iraní - como un área dentro de la esfera de la seguridad nacional. Pese a que la misma está basada fundamentalmente en acontecimientos desarrollados en el plano virtual, la ciberseguridad se convirtió en una herramienta que vela por la seguridad del Estado, y que hoy en día podría categorizarse como "alta política" en términos realistas. Tal como lo plantea esta teoría, en materia de ciberseguridad el Estado continúa siendo un actor central (aunque no el único), cuyo accionar en este campo - tanto reactivo como proactivo - tiene grandes implicancias para otros actores - principalmente para la sociedad civil -.

Respecto a los aportes tomados de la interdependencia compleja, se observa que la naturaleza misma del ciberespacio ha vuelto al mundo más interconectado y por ende más interdependiente, lo que aumenta las vulnerabilidades a las que los distintos sujetos de la comunidad internacional - entre ellos, los Estados - se exponen en este dominio. También se retoma de esta teoría, la diversidad de actores que emergieron en el sistema internacional. En este sentido, los avances tecnológicos y la aparición de Internet tuvieron un rol preponderante a la hora de dar visibilidad y capacidad de acción a sujetos más y menos poderosos - individuales y colectivos -.

Al mismo tiempo, podemos identificar tres perspectivas a través de las cuales interpretar la relación entre el ciberespacio y los Estados: la utópica, la regulatoria y la realista (Manjikian, 2010). La ***utópica*** entiende al ciberespacio como una entidad normativa que está por fuera del

control que pueda ejercer un gobierno. La visión ***regulatoria*** por su parte, propone que el ciberespacio es un bien común global que debe ser regulado mediante regímenes normativos, para preservarlo como un bien público. Finalmente, la corriente ***realista*** plantea que la denominada "aldea global" planteada por la perspectiva utópica, se convierte en un espacio de batalla virtual donde se disputa el poder (Manjikian, 2010).

En este trabajo de investigación, se realizará una lectura de la política de ciberseguridad de Irán desde esta última perspectiva, ya que se observa que el ciberespacio pasa a ser un escenario más de confrontación política. Siguiendo a Kuehl (2009), podemos definir al ***ciberespacio*** como "un dominio global dentro del entorno de la información cuyo carácter distintivo y único se enmarca en el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando tecnologías de la comunicación y la información" (p.4).

A los fines de esta tesina, el ciberespacio es un concepto troncal, dado que es el medio principal a través del cuál Irán aplica la política de ciberseguridad; a la vez que un dominio en el cual tienen lugar pujas por el poder - tanto en la dimensión doméstica como internacional -. Es por esta razón, que será un concepto que atravesará todo el trabajo.

La extensión y delimitación del ciberespacio es un área en la cual todavía no ha habido suficiente concordancia. Newmeyer, Cubeiro y Sánchez (2015) sostienen que las fronteras inciertas de este dominio, y el hecho de que fue creado por el hombre, derivan en la abundancia de lagunas legales.

Si bien esto es verdad, también es cierto que, tal como afirma Paredes Roibas (2018) los Estados tienen soberanía en el plano físico del ciberespacio, relacionado con las redes, la infraestructura y las computadoras que se encuentren bajo su jurisdicción. A modo de ejemplo, desde un punto de vista legal un Estado puede promulgar leyes que requieran de firmas electrónicas, encriptaciones y demás sistemas de seguridad a la hora de realizar una actividad en la red; así como también pueden bloquear el acceso a determinadas páginas *web* (Paredes Roibas, 2018).

En consonancia con lo planteado por Paredes Roibas (2018), Irán representa un caso empírico del poder y el control que un Estado puede ejercer en materia cibernética sobre su territorio. Como se desarrollará en el capítulo I, a nivel interno se observa que luego de las manifestaciones que se dieron en el marco del Movimiento Verde en 2009, se iniciaron

procesos para diseñar una estructura de red nacional; a la vez que aplicaciones como *Facebook, Twitter, Telegram* y *Google Plus* fueron prohibidas (Bowen y Marchant, 2018).

Ligado al surgimiento y la centralidad que adquiere el ciberespacio, surge otro concepto que se relaciona con la manera de accionar dentro de ese dominio: la ***ciberseguridad***. La rapidez con la que evoluciona la ciberseguridad como concepto y práctica, y sus convergencias con otras formas de seguridad, han obstaculizado el consenso para su definición - al igual que para muchos otros términos relacionados al mundo virtual -.

Stevens (2018) propone una interpretación amplia del término, definiéndolo como "un medio no sólo para proteger y defender a la sociedad y a sus infraestructuras de información esenciales, sino también como una forma de desarrollar políticas nacionales e internacionales a través de medios informáticos" (p. 2). La relevancia de esta lectura, radica en que comprende a la ciberseguridad no sólo desde una óptica defensiva o reactiva, sino también ofensiva y proactiva, plausible de utilizarse para fines políticos e intereses concretos.

La ***política de ciberseguridad*** es el conjunto de acciones diseñadas y ejecutadas por el Estado para el cumplimiento simultáneo de varios roles en materia de ciberseguridad: ser garante de la seguridad cibernética y promover leyes al respecto sobre su jurisdicción; a la vez que ser una institución que imponga límites y restricciones para ciertos grupos sociales y países (Cavelty y Egloff, 2019).

En Irán, dicha política es aplicada a nivel doméstico e internacional - si bien tal como lo afirma Górka (2021) no es sencillo trazar una distinción clara entre las dos esferas -; y está orientada al cumplimiento del propósito mayor de proteger la integridad del régimen y de posicionar a Irán como potencia cibernética regional.

Según Bebber (2017), se considera ***potencia cibernética*** a aquellos Estados que demuestran tener la capacidad de utilizar los recursos humanos y materiales disponibles dentro de un entorno estratégico, para generar efectos en y a través del ciberespacio; y así proyectar poder sobre otros actores. Es decir, no basta con poseer recursos cibernéticos, sino que es necesario saber emplearlos en los diferentes escenarios, haciendo uso del quinto dominio. En el capítulo III, observaremos que la República Islámica no sólo acrecienta significativamente sus cibercapacidades, sino que logra efectivamente generar un impacto en la sociedad civil y en sus vecinos del Medio Oriente; quienes lo ven como una potencial amenaza a su seguridad.

Esto se debe al tinte ofensivo que adquiere la política de ciberseguridad persa por momentos, para interferir en las actividades que los países occidentales y los opositores al gobierno puedan organizar en el ciberespacio. Organizaciones como la FATA, la Fuerza Paramilitar Basij y el Comité para Identificar Sitios No Autorizados, participan constantemente en ataque cibernéticos que buscan ocasionar bloqueos de Internet, insertar contenido pro-iraní y desviar el rumbo del tráfico en la *web*.

Al mismo tiempo, Irán presta apoyo cibernético a organizaciones ***proxies*** - esto es, grupos que actúan en la arena regional en favor de los intereses iraníes (Deutsch, 1964) - como el Ejército Cibernético Yemení, el Ejército Electrónico Sirio y Hezbolá (Daricili, 2019), en un contexto de ***rivalidad***[7] con Arabia Saudita e Israel por el liderazgo en la región de Medio Oriente.

Como mencionamos previamente, un punto de inflexión en la política de ciberseguridad de la República Islámica fue el ciberataque de *Stuxnet* a las centrifugadoras de uranio de las plantas nucleares de Natanz y Bushehr, llevado a cabo por parte de EE.UU. e Israel hacia Irán en el año 2010. Se entiende por ***ciberataque*** a cualquier acto que se categorice como ***cibercrimen*** - delitos como el faude, el lanzamiento de *malwares*, el robo, y la falsificación de caudales públicos mediante computadoras y redes -, ***ciberguerra*** - conflictos bélicos que en vez de tener lugar en campos de batallas convencionales, se llevan a cabo en el ciberespacio utilizando como armas aplicaciones y tecnologías provistas por sistemas sofisticados -, o ***ciberterrorismo*** - la forma de terrorismo que utiliza las tecnologías de la informacion para intimidar, coaccionar, o causar daños a grupos sociales, con fines poíticos o religiosos (Urueña Centeno, 2015).

Siguiendo a Stevens (2015), las tecnologías de la información y el Internet se han convertido en un recurso poderoso para la persecución de intereses y la proliferación de ideas de actores no estatales como organizaciones no gubernamentales, empresas, grupos terroristas, o la misma sociedad civil. Sin embargo, esto no se tradujo necesariamente en una pérdida de la autoridad y el control del Estado. Por el contrario, la República Islámica ha sabido adaptarse al nuevo contexto.

La propaganda ocupa un lugar central en la política de ciberseguridad persa. Irán invierte recursos considerables en la creación y reproducción de una estructura de múltiples niveles que

[7] Entendemos por "rivalidad" a una relación hostil en la cual la competencia entre los actores puede derivar en un enfrentamiento militar (Goertz y Diehl, 2003).

sea capaz de monitorear y controlar ofensivas en el ciberespacio, para evitar una ***soft revolution*** - es decir, una revolución pacífica iniciada a raíz de la penetración de información proveniente de occidente o de otros Estados enemigos como es el caso de Israel - (Siboni y Kronenfeld, 2012).

El devenir de estas acciones y la acumulación de *know how* en materia cibernética, se tradujo en la capitalización del ciberpoder. Venables, Shaikh y Shuttleworth (2015) definen al ***ciberpoder*** como "la capacidad de alterar el comportamiento de un sujeto a través del ciberespacio, en el contexto de la seguridad nacional y el conflicto" (p. 5). Dicho poder puede ser ejercido por actores estatales o no estatales a través de campañas cibernéticas - que comprenden un evento singular o una serie de eventos - mediante la utilización de medios coercitivos, persuasivos o técnicos, para lograr un efecto específico (Venables, Shaikh y Shuttleworth, 2015).

El ciberpoder es fungible, dado que puede favorecer el alcance de objetivos concretos y diversos - asociados al *hard power* y al *soft power* - como influir en la formación de opinión pública; degradar o destruir el servicio o los datos de dispositivos particulares; combinar mecanismos técnicos y políticos para fortalecer, adaptar y defender la infraestructura; adaptar recursos disponibles para contrarrestar campañas cibernéticas e incluso tomar medidas de represalia (Venables, Shaikh y Shuttleworth, 2015).

En este sentido, en el capítulo II se argumentará que la República Islámica aspira a capitalizar recursos de ciberpoder con el propósito de que actúen como un factor de disuasión militar ante cualquier ataque convencional - o no convencional - que se lleve a cabo en su contra (especialmente proveniente de EE.UU., Israel o Arabia Saudita). Dado que gran parte de su infraestructura continúa siendo controlada por sistemas mecánicos - no cibernéticos -, naturalmente se reducen las vulnerabilidades a las que se expone el país en el ámbito virtual.

Como lo afirman Siboni y Kronenfeld (2012) el esquema cibernético persa debe comprenderse de manera similar a su programa nuclear: no es particularmente sofisticado, pero nunca deja de avanzar. De hecho, Jones (2016) plantea que los obstáculos puestos a su programa nuclear, incentivaron el desarrollo cibernético, al punto de que la República Islámica se estaría perfilando rápidamente como la sexta superpotencia cibernética - por detrás de EE.UU., Gran Bretaña, Israel, Rusia y China -.

En otras palabras, la aparición de la cibernética ha facilitado el desenvolvimiento de la ***guerra asimétrica***. Según Rodríguez Peña (2001), "podemos partir este concepto en dos: son procedimientos no convencionales que buscan evitar o minimizar las capacidades militares del enemigo; y a la vez aprovechar sus vulnerabilidades mediante tecnologías o medios inéditos" (p. 61).

Siguiendo a Venables, Shaikh y Shuttleworth (2015), el ciberespacio puede entenderse como un ***ecualizador***, lo que significa que Estados nacionales - con mayor o menor poder relativo - y los actores no estatales pueden competir en términos relativamente iguales. Este dominio puede ofrecer a entidades con diferentes capacidades la misma velocidad, alcance, anonimato y protección; a la vez que la posibilidad de desarrollar sus propias armas cibernéticas a bajo costo (Venables, Shaikh y Shuttleworth, 2015).

En el capítulo II, expondremos cómo la República Islámica de Irán supo comprender los beneficios que otorga inmiscusión en el espacio cibernético, y aprovechar el mencionado factor ecualizador para acotar la brecha de poder militar con naciones rivales como EE.UU. e Israel.

La tecnología le ha permitido beneficiarse del ciberespacio de manera rentable y con bajos riesgos (Daricili, 2019). Para este autor, "tener una capacidad efectiva de ataque cibernético proporcionará disuasión militar contra cualquier ataque convencional que pueda llevarse a cabo contra Irán" (Daricili, 2019, p. 410).

Respecto a la ***metodología*** de esta tesina**,** se trata de una investigación de diseño cualitativo que estudia los resultados de la política de ciberseguridad iraní aplicada al ámbito doméstico e internacional en el período 2009 - 2021.

El período de análisis inicia con las movilizaciones del Movimiento Verde de 2009, debido a que se concibe como un punto de inflexión en el enfoque que Irán tiene hacia la ciberseguridad. A su vez, el trabajo finaliza en el año 2021, con la culminación del mandato de Rouhaní - quien fue presidente desde 2013 y escaló la cuestión de la ciberseguridad en la agenda estatal de seguridad nacional -.

En base a la naturaleza de los objetivos de investigación que se han planteado, se considera que la técnica de investigación más adecuada es el análisis de datos y/o documentos oficiales junto con la recopilacion y sistematizacion de bibliografía especializada en la temática y portales de noticias, tanto de autores y medios occidentales como no occidentales.

Respecto a la organización de esta tesina, la misma se dividirá en tres capítulos. El primero tendrá el propósito de examinar los principales objetivos, herramientas y *targets* de la política de ciberseguridad iraní a nivel doméstico. El segundo capítulo estará destinado a estudiar la política de ciberseguridad persa en el plano internacional; en el marco de la rivalidad con EE.UU., Arabia Saudita e Israel. En el tercero, analizaremos cuáles fueron los resultados de la política de ciberseguridad iraní en la dimensión doméstica e internacional que permitieron proteger la integridad del régimen y posicionar a Irán como potencia cibernética regional durante el periodo de estudio seleccionado.

Finalmente, esbozaremos una conclusión acerca de lo investigado en este trabajo.

Capítulo I

Desde hace aproximadamente dos décadas las interacciones en el dominio cibernético tienen un impacto cada vez más grande en las decisiones y las políticas adoptadas por los Estados a nivel mundial. Precisamente los Estados del MENA han destinado un gran volumen de recursos a nivel nacional para controlar sus paisajes sociopolíticos - especialmente luego de ocurridas las manifestaciones en el marco de la Primavera Árabe -. Siguiendo a Sexton y Campbell (2020) en el Medio Oriente la transformación digital ha consistido más en un esfuerzo de las autoridades por controlar a sus ciudadanos, que en una ampliación de los espacios donde la sociedad puede resistir a la autoridad.

Como se adelantó en la introducción de este trabajo, en el caso particular de Irán el papel de las redes sociales en las movilizaciones que siguieron a las elecciones presidenciales de 2009 y el ciberataque de Stuxnet en 2010 contra la República Islámica, provocaron que la arena cibernética se convirtiera en un pilar de la doctrina de seguridad nacional del régimen persa. Las repercusiones de estos fenómenos en la política de ciberseguridad iraní se vieron reflejadas en el inmediato comienzo de la construcción de un entramado de instituciones que tienen como fin regular y tener una participación activa en el ciberespacio - objetivo alineado con el propósito mayor de proteger al régimen y posicionar a Irán como líder regional -.

En el apartado a continuación procederemos a desarrollar brevemente en qué constó el Movimiento Verde y su relevancia en la arena política y de ciberseguridad que coadyuvó en la sistematización y profundización de la misma. Luego, identificaremos los objetivos de ésta y los principales targets en el ámbito doméstico; prosiguiendo con la evolución del capital tecnológico utilizado para su ejecución en la dimensión doméstica. Finalmente, arrojaremos luz sobre lo que consideramos son hitos que marcaron el rumbo de la estrategia de seguridad nacional en el ciberespacio; para luego pasar a las conclusiones del apartado.

1. Movimiento Verde: el inicio de una política de ciberseguridad más asertiva y rigurosa

Como se mencionó en la introducción de esta tesina, identificamos al Movimiento Verde como una variable fundamental a la hora de comprender la relevancia que adquiere la política de ciberseguridad iraní aplicada al ámbito doméstico. Observamos que, en este contexto, el ciberespacio se convirtió en una vía de doble entrada.

Por un lado, los usuarios participaron activamente en la red compartiendo y publicando contenido e información relacionado a aspectos de la vida política y social. Por el otro, los mismos candidatos a la presidencia y el gobierno hicieron uso de este dominio - especialmente a través de redes sociales - para difundir propaganda a su favor de forma económica y eficiente. Esto da cuenta de la cualidad ecualizadora que caracteriza al ciberespacio; dado que ambas partes - con más y menos poder - participaron activamente en la red y lograron tener un impacto en la contraparte.

Siguiendo a Castro Torres (2019), podríamos definir al Movimiento Verde iraní como una corriente ideológica de corte liberal, conformada por grupos con diferentes finalidades políticas y sociales, pero que compartían el reclamo por el respeto a los derechos civiles y la búsqueda de elecciones verdaderamente libres en el país. A este movimiento se han sumado intelectuales, jóvenes, mujeres, minorías étnicas e incluso *Artesh* (soldados del ejército regular).

Empíricamente, el Movimiento Verde comenzó con reivindicaciones reformistas luego de las elecciones presidenciales de junio de 2009, como respuesta a las políticas opresivas de Ahmadineyad - quien se consagró como presidente por segunda vez consecutiva luego de estos polémicos comicios -. La disputa electoral del 12 de junio de ese año giraba en torno a dos candidatos: el conservador Mahmud Ahmadineyad y el líder reformista Mir-Hossein Mousavi.

Las redes sociales han tenido un rol esencial tanto en durante la campaña electoral como luego de los comicios. En un país con alrededor de 23 millones de internautas y una comunidad virtual con más de 6.000 blogs, la red se convirtió para los votantes iraníes en una herramienta fundamental para informarse acerca de las propuestas presidenciales (García Orta, Alonso González y Carreras Álvarez, 2010).

Tal como lo afirman García Orta, Alonso González y Carreras Álvarez (2010), entrevistas *on line* de los candidatos, *Facebook, Twitter* e infinidades de blogs irrumpieron en la vida política de uno de los países geoestratégicamente más importantes del Medio Oriente. Efectivamente, ambos contrincantes aprovecharon las ventajas que ofrece Internet para promocionarse durante la campaña electoral, a través de sus blogs personales, de videos en *Youtube*, y de la creación de cientos de cuentas en *Twitter* que publicaban contenidos y opiniones a su favor.

En suma, muchos usuarios utilizaron una aplicación vinculada con *Facebook* que les permitía colorear de verde la foto de perfil en señal de apoyo al candidato reformista; de rojo para los seguidores de Ahmadineyad; o de azul para los partidarios de boicotear las elecciones.

Ocurridos los comicios, las sospechas ante la falta de transparencia ocasionó que el propio Mousavi, respaldado por la oposición, denunciase las elecciones por fraudulentas. En un primer momento, el Ayatollah Jamenei se inclinó por las sendas del diálogo y la conciliación entre las partes. No obstante, ante la intensificación de los reclamos y las manifestaciones en la vía pública, el gobierno comenzó una dura campaña de represión y detenciones - incluso hacia propios conservadores - que en algunos casos terminó con sentencia de muerte.

En 2011, al calor de los comienzos de la Primavera Árabe en Túnez y Egipto, la oposición iraní encontraría fuerzas renovadas y un contexto regional favorable para intervenir en la escena política y social del país; pero nuevamente las fuerzas gubernamentales sofocaron esas intenciones. Pese a los grandes esfuerzos por parte del régimen iraní de silenciar las protestas y evitar que salgan a la luz estos acontecimientos, el fenómeno de la *web* 2.0[8] permitió revelar estos hechos al resto del mundo.

La primera reacción de la cúpula gubernamental fue fundamentalmente la censura a los medios de comunicación más tradicionales. Esta fue aplicada a los principales periódicos pro reformistas y de oposición a Ahmadineyad - los cuales fueron cerrados o inhabilitados para criticar los resultados -, a la vez que cadenas de televisión nacionales, según afirma la ONG Reporteros Sin Fronteras (RSF) (La Vanguardia, 2009).

Otros medios tradicionales también sufrieron la injerencia del gobierno iraní en su derecho a informar. Entre ellos se encontraban la BBC - un periodista y un camarógrafo fueron detenidos -, la cadena flamenca VRT, la italiana RAI, la agencia Reuters y la radio-televisión francófona RTBF - cuyos corresponsales fueron retenidos y golpeados por agentes persas - (García Orta, Alonso González y Carreras Álvarez, 2010).

No obstante, los blogs y las redes sociales se convirtieron en los nuevos canales por los que circuló mayormente el caudal de información, caracterizadas por ser gratuitas y rápidas - atributos que hacen que estos medios sean más difíciles de controlar -.

Aplicaciones como *Twitter*, *Flickr* y *YouTube*, han dado paso a un nuevo paradigma de comunicación denominado "periodismo ciudadano" o el mencionado "*web 2.0*" (Ruiz San

[8] Lo que diferencia fundamentalmente a la *web* 2.0 de su predecesor, la *web* 1.0, es un cambio en el paradigma comunicativo, ya que el usuario de la red pasa de ser meramente un consumidor de contenidos digitales, a participar en la construcción de los mismos. Los medios más destacados que funcionan dentro del modelo participativo de la *web* 2.0, son los blogs y las redes sociales, debido a que se convierten en plataformas de difusión de información en situaciones de censura gubernamental de los medios convencionales.

Miguel y Blanco, 2005), donde cualquier usuario de la red pasa de ser un consumidor pasivo de contenidos, a participar activamente en la elaboración de los mismos. Según Ruiz San Miguel y Blanco (2005) "se ha perdido la confianza en los medios tradicionales y el receptor de la información ha decidido emitir su propia información y además verificar la información que nos llega a través de los medios de comunicación de masas" (p.5).

Siguiendo la evolución del nuevo paradigma comunicacional, y con el Movimiento Verde como punto de inflexión[9], la política de ciberseguridad aplicada al ámbito doméstico se intensificó, pasando a ser más asertiva y más rigurosa. Con la censura como principal medida, de acuerdo al informe anual de 2017 de RSF, Irán ocupa el puesto 165 de 180 en la Clasificación Mundial de la Libertad de Prensa de ese año (RSF, 3 de enero de 2018).

Un artículo de RSF, afirma que desde 2009 *Facebook* y *Twitter* están prohibidos en Irán (2018); y para el año 2012, se estima que alrededor de 10.000 computadoras ya incluían el sistema de Internet nacional *Halal Internet* (Berman, 2013). Esta red utiliza un "filtrado inteligente" que permite restringir el acceso a Internet en general y a las redes sociales en particular. Además, controla que los sitios contengan exclusivamente publicaciones permitidas desde la interpretación estricta de la ley islámica. En suma, *Telegram* y *Signal* están bloqueados desde inicios de 2018; a la vez que se creó la plataforma *Mehr* como alternativa a YouTube (Bowen y Marchant, 2018).

En síntesis, se observa que la política de ciberseguridad iraní ha ido evolucionando en consonancia con el avance tecnológico y comunicacional en el ciberespacio. Iniciando con las censuras a los medios más tradicionales - nacionales y foráneos - y las expulsiones de corresponsales de medios extranjeros, se pasó luego a aplicar un control más riguroso sobre las aplicaciones y la red en general.

Lo que se observa es un incremento de lo que Venables, Shaikh y Shuttleworth (2015) denominan como ***ciberpoder***; estos es, un aumento en los recursos utilizados para controlar y alterar el comportamiento de otro - en este caso, de la sociedad civil -, por medio del ciberespacio.

[9] De hecho, estas manifestaciones fueron denominadas como "Revolución de Facebook/Twitter" en referencia al importante papel que jugaron las redes sociales en las protestas a la hora de mostrar al mundo lo que en realidad estaba ocurriendo en el interior del país (García Orta, Alonso González y Carreras Álvarez, 2010).

2. Objetivos **y targets de la política de ciberseguridad iraní en el ámbito doméstico**

Dado que el ciberespacio desdibuja los límites entre la dimensión nacional e internacional, es menester aclarar que los objetivos en materia de ciberseguridad a nivel interno y externo no se diferencian tajantemente. De hecho, se constituyen como dos caras de una misma esfera orientada al cumplimiento de objetivos primordiales: proteger la integridad del régimen y posicionar a Irán como potencia cibernética regional.

En la dimensión doméstica observamos que los esfuerzos están mayormente destinados a garantizar la seguridad y estabilidad del gobierno, tarea que resulta un tanto compleja dada la heterogeneidad y el tamaño de la población iraní. Desde el nacimiento de Irán como Estado-nación, el territorio está compuesto por un crisol de etnias y religiones diversas que conviven y se distribuyen a lo largo y ancho del país. No obstante, dado que la mayoría de la población es persa y chiita, la representación, la estructura jurídica y el gobierno se estructuró casi exclusivamente en torno a esta porción de la población.

Siguiendo a Daricili (2019) el propio tejido social iraní lleva a que el gobierno identifique a ciertos grupos como *targets* que deben mantenerse continuamente controlados, con el propósito de asegurar la supervivencia del régimen. Por la capacidad de acción que tienen en el ciberespacio, los blancos son fundamentalmente minorías religiosas y étnicas; opositores al gobierno, e *influencers* en redes sociales.

2.1 Minorías étnicas y religiosas

Las minorías étnicas iraníes - como los azaríes, baluchis, árabes y kurdos entre otros - se enfrentan a una vulneración de derechos más profunda en comparación con la población persa y chiita. La falta de representacion política y de integración en la economía; las dificultades al momento de acceder trabajos de calidad; la escasez de recursos y servicios básicos como aguan luz y gas; la violación a derechos liguísticos y educacionales; y la represión y persecución ante el mínimo intento de manifestación organzada son algunas de los obstáculos que deben atravesar.

En cuanto a las minorías religiosas, debemos comprender en primer lugar que aproximadamente el 89% de los iraníes son musulmanes chiítas. El 11% restante está compuesto por bahá'íes, cristianos, zoroastrianos, musulmanes sunitas y judíos. Múltiples académicos concuerdan en que en mayor o menor medida las minorías religiosas también sufren discriminaciones sistemáticas por parte del Estado, particularmente en las esferas del

empleo, la educación y la vivienda; siendo los bahá'íes los que más se ven perjudicados (Hassan, 2007).

El Ministerio de Inteligencia y Seguridad iraní - mancomunadamente con otros organismos estatales - supervisa de cerca las actividades de estos grupos y las organizaciones religiosas, comunitarias y culturales; las escuelas; y los eventos públicos que éstos llevan a cabo (Hassan, 2007).

La comunidad bahá´í requiere una especial atención, dado que esta religión no se encuentra amparada en la Constitución. Documentos gubernamentales publicados por la Comunidad Internacional Bahá'í revelan que esta minoría es víctima de una política secreta de discriminación gubernamental registrada en documentos, cartas y memorandos del régimen. Irán es la base de múltiples eventos de relevancia en la historia de la comunidad, por lo que muchos textos bahá'íes han sido revelados en persa. En consecuencia, existe un vínculo profundo entre la religión bahá'í y el idioma, la cultura y la sociedad iraníes.

Los bahá'íes creen que las obras de Bahá'u'lláh y sus enseñanzas brindan una visión unificadora del futuro de la sociedad humana. Según esta creencias, la humanidad ha alcanzado la madurez colectiva. Los cambios revolucionarios que tuvieron lugar en el mundo desde el nacimiento de esta religión, suponen el reflejo de la transición de la infancia - cuando los hombres se consideraban como individuos aislados - a la madurez propia de una civilización global armoniosa, de la cual forman parte todas las etnias, religiones y géneros (bahaisofiran.org)

De acuerdo a Jiménez Majidí (2022), "el avance científico y tecnológico en las áreas de la comunicación y de los medios de transportes están contribuyendo, inexorablemente, a la materialización de la visión bahá'í de una sociedad global que vive en unidad y armonía" (p. 220). El establecimiento del sistema global enunciado en los escritos bahá'íes parecía en los orígenes de esta religión una meta extremadamente lejana. 'Abdu'l-Bahá[10] afirma que el establecimiento de la unidad de toda la humanidad era algo inalcanzable debido a carencia de los medios materiales necesarios para lograrlo. Con el paso del tiempo, la ciencia y la tecnología facilitaron la unión y la globalización pregonada por los bahá'íes.

[10] 'Abdu'l-Bahá (Persia, 1844 - Palestina, 1921), era el hijo mayor de Bahá'u'lláh. Fue designado por su padre en su testamento como cabeza visible de la comunidad mundial bahá'í, a la vez que el único intérprete autorizado de sus escritos hasta su fallecimiento. En consecuencia, su palabra - escrita y oral - tienen autoridad dentro de la comunidad bahá'í y son considerados como fuente inspiración divina (bahaisofiran.org).

Al tener en cuenta los postulados que guían a esta fe - la igualdad entre hombres y mujeres, la búsqueda de la verdad proveniente a la vez de la ciencia y la religión, la creencia de que en algún momento la sociedad internacional se convertirá en una aldea global común y acogedora con todas las religiones y etnias, entre otros - no resulta sorprendente que el régimen destine grandes esfuerzos para aplacar cualquier posible brote que se pueda traducir en la expansión y el crecimiento de la religión bahá'í en el territorio nacional (Jerez, 2016).

En este sentido, el avance cibernético con la creación de Internet y más aún el arribo de las redes sociales, proveyeron a la comunidad de nuevas herramientas para divulgar sus creencias y manifestar al mundo la opresión que sufrían por parte del gobierno Iraní. Un ejemplo de la utilización de estos canales digitales en pos de reclamos políticos de los bahá'íes fue la viralización del reclamo por la expropiación de las tierras de Ivel. Esta es una aldea ubicada en la provincia de Mazandaran, que data como el lugar de origen de una de las comunidades bahá'íes más antiguas de Irán.

La protesta tuvo eco a nivel global, dando una gran visibilidad a los reclamos y a la comunidad en sí misma. En este sentido, se observa que las persecuciones y la opresión ejercidas sobre esta población fue mutando en relación a los instrumentos y los canales utilizados en la era digital, donde se aplicó principalmente la censura, el monitoreo, y las restricciones a páginas *web* que van "en contra de los intereses nacionales".

En conclusión, observamos que la política de ciberseguridad aplicada por la República Islámica sobre estas comunidades, se traduce principalmente en la restricción de una amplia gama de actividades *on-line* y en el bloqueo a contenidos considerados contrarios a los valores religiosos, socioculturales y políticos del sistema.

Asimismo, comunidades como la kurda y la judía también son consideradas como un potencial peligro para la integridad del régimen. La primera debido a los movimientos independentistas y a su proximidad con kurdos en Irak, Siria y Turquía; y los segundos por considerarlos cercanos al 'régimen sionista' de Israel, enemigo de Iran y gran rival en el Medio Oriente.

Dado que estas minorías no se encuentran aisladas sino que sus redes trascienden las fronteras (hacia Irak el kurdistán, hacia Azerbaiyán los azeríes, etc.), no es sorprendente que el gobierno los vea como una amenaza a su seguridad, identidad y existencia.

En un mundo donde la tecnología ha llegado a casi todos los rincones del planeta, el gobierno iraní encontró instrumentos para mitigar esas interconexiones por medio del ciberespionaje. La

prohibición de ciertas redes sociales, los obstáculos puestos al acceso a Internet en algunas regiones, y la preferencia por las comunicaciones mayormente en farsí para dificultar la comprensión de noticias, serán cuestiones -entre otras- que desarrollaremos más adelante.

2.2 Oposición

En cuanto a la estrategia cibernética utilizada contra la oposición, nuevamente la campaña electoral de 2009 se presentó como un hito. Además de la aplicación de la censura digital, funcionarios y empresarios del círculo más cercano de ambos candidatos fueron blanco de operaciones de ciberespionaje y amenazas [11] (Daricili, 2019). Al mismo tiempo, otras figuras políticas de relevancia - como el anterior presidente Mohammad Khatami - estuvieron expuestos a actividades de ingeniería social del Ministerio de Inteligencia de Irán y la Guardia de la Revolución Islámica.

Cuando el *establishment* político dio cuenta del potencial que tienen las aplicaciones y las redes sociales al momento de realizar campañas electorales - dada la excelente relación costo-beneficio que caracteriza a estas plataformas cibernéticas como medios de divulgación económicos y eficaces -, se dio inicio a un vínculo entre política-tecnología que se fortaleció progresivamente.

No obstante, a finales de noviembre de 2008 - a unos meses de los comicios - el gobierno (liderado por el conservador Mahmud Ahmadineyad, quien buscaba la reelección) bloqueó *Youtube* y *Facebook* bajo el argumento de que el Internet provocaba daños sociales, políticos, económicos y morales para el país. Ese mismo año se aprobó una Ley sobre delitos en línea que permite la pena de muerte para blogueros y editores *web* responsables de páginas que "promuevan la corrupción, la prostitución y la apostasía" (Labio Bernal, A. y García Orta, M. J.; 2010).

A su vez, la conectividad durante ese período también disminuyó. El entonces ministro de Comunicación y Tecnologías de la Información, Mohammad Soleimani, declaró públicamente

[11] De hecho, el sobrino del líder opositor Mir Hossein Mousavi fue asesinado el domingo durante las manifestaciones que siguieron a las elecciones de 2009 - (Daricili, 2019).

que “una conexión de 56 KB es ampliamente suficiente para los internautas iraníes”, conexión que los haría retroceder a los inicios de la red en la década de los noventa .

De acuerdo a Labio Bernal, A. y García Orta, M. J. (2010), para el año 2010, Irán tenía prohibido el acceso a más de cinco millones de páginas *web*, tanto de ciudadanos iraníes en el exilio como de opositores al régimen dentro del propio país[12]. La mayoría de esos sitios son blogs que tienen por bandera la defensa de los derechos humanos y la libertad de expresión.

De hecho, se estima que la República Islámica tiene la blogosfera política más rica y activa del mundo. A modo de comparación, en 2004, cuando los blogs españoles apenas llegaban a los 1000 usuarios, en Irán había más de 200.000 (Labio Bernal, A. y García Orta, M. J.; 2010).

Desde entonces, la blogosfera iraní no ha dejado de crecer, desarrollándose como un entorno deliberativo extenso y políticamente influyente. En suma, Irán devino en el tercer país con más blogueros en el mundo y el farsí se convirtió en la cuarta lengua utilizada en los blogs.

Tal como lo afirma la bloguera iraní y defensora de los derechos de la mujer, Farnaz Seifi, “la red ofrece un instrumento para que las voces reprimidas se escuchen en una sociedad donde todos los medios están controlados por el Estado” (p. 239, Labio Bernal, A. y García Orta, M. J.; 2010). Además de los blogs, *Facebook* y *Twitter* se convirtieron en los medios más elegidos por la clase media y alta iraní para manifestarse contra el gobierno.

Habiendo ganado las elecciones el entonces presidente Ahmadineyad con el 63% de los votos, los opositores al gobierno denunciaron fraude electoral, alegando entre otras cuestiones que se contabilizaron más votos que la cantidad de población habilitada para votar. A raíz de esos hechos, comenzaron una serie de manifestaciones - el luego conocido y extendido Movimiento Verde - para exigir respeto democrático y la repetición de las votaciones con dos proclamas generalizadas: “Éste no es mi voto” y “Abajo el gobierno golpista” (p. 241, Labio Bernal, A. y García Orta, M. J.; 2010).

En un intento de extinguir las protestas, el régimen persa bloqueó las transmisiones de mensajes de texto por teléfono móvil y las llamadas internacionales, retiró las acreditaciones de los periodistas de medios extranjeros y redujo el ancho de banda para evitar la publicación de

[12] Según Amnistía Internacional (2009: 55), entre los sitios *web* que se filtran están la Organización Kurda de Meydaan, que ofrecía información sobre los derechos de la mujer; y Cambio por la Igualdad, que aboga por el fin de la discriminación femenina. Con el pretexto de que eran “inmorales o contrarios a los principios del Islam”, las autoridades cerraron muchos sitios que ofrecían información sobre violaciones de derechos humanos.

videos y fotografías de las manifestaciones. Sin embargo, la oposición logró evadir parte de los controles gubernamentales y utilizó primordialmente *Twitter* (además de otras redes sociales) para convocar a sus partidarios y difundir en tiempo real contenido que revelaran gráficamente los enfrentamientos entre los manifestantes y la policía. Los partidarios de Mussavi enviaban enlaces a fotos donde se podían ver a civiles heridos o videos narrando el desarrollo de los acontecimientos (Elmundo.es, 2009).

Por otro lado, en *Facebook*, se registraron grupos y *hashtags* como "Me IRAN", "Me love Iran" y "Apoyo a las libertades, los derechos humanos y la democracia en Irán". Consecuentemente, ambas redes sociales volvieron a ser bloqueadas y desde entonces hasta 2021 continuaron estando prohibidas.

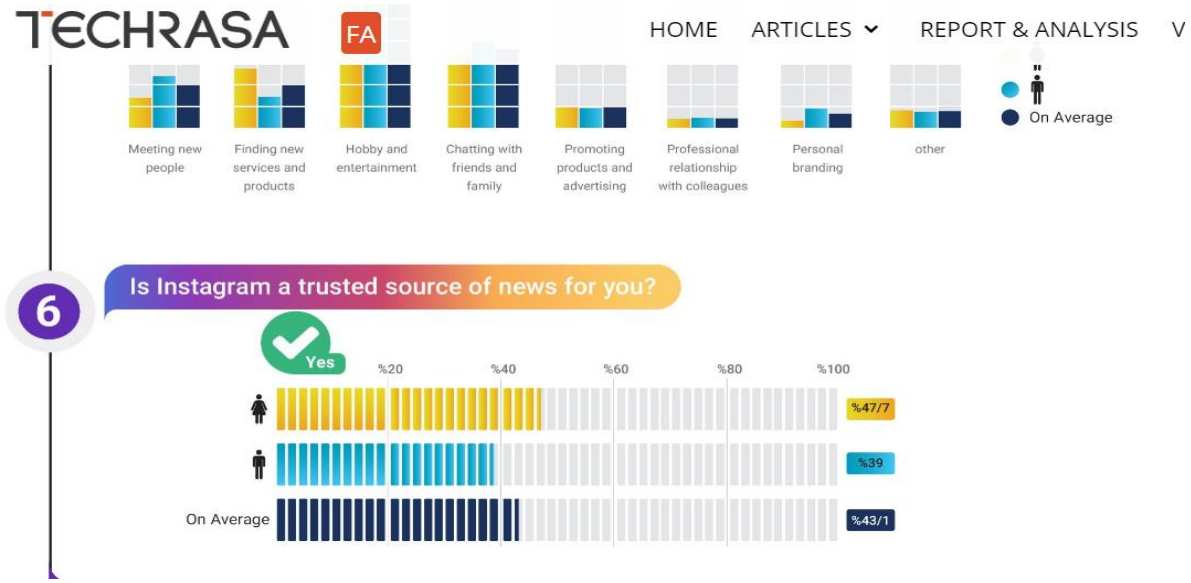
2.3. Influencers

Tradicionalmente, eran los medios masivos de comunicación - como la radio, la televisión y los medios gráficos - los que tenían mayor influencia en el debate público. Sin embargo, en la era digital la divulgación de la información y de pensamientos corrieron su eje hacia otros canales como plataformas *on-line* y redes sociales.

En este nuevo paradigma comunicacional apareció un actor que tendrá un papel de suma relevancia en la formación de opiniones y en la generación y difusión de contenidos: los *influencers*. De acuerdo a MacGregor (2020) en su artículo publicado en *Made for Minds*, entendemos por *influencer* a aquella persona que crea y comparte contenido en la *web* - a través de plataformas y redes sociales -, atrayendo a un gran número de seguidores.

El rol social de los *influencers* en la última década podría caracterizarse como fungible. Si bien su exposición pública puede tener consecuencias altamente positivas - por ejemplo para empatizar con sus audiencias, levantar banderas de luchas sociales, etc. -; también ese gran poder puede ser utilizado para difundir noticias falsas - o *fake news* - y promover mensajes de odio. Esto obstaculiza la comprobación del rigor científico de sus publicaciones, y dificulta la diferenciación entre lo inventado y lo real.

En ese sentido, una encuesta hecha a la población iraní llevada a cabo por *Nazar Bazaar Market Research Platform* para *Techrasa* en el año 2017 refleja claramente las confusiones que muchas veces se generan tras el bombardeo de información.



La misma da cuenta de que para el 43,1% de la sociedad, *Instagram* es una fuente confiable de la cual obtener información, mientras que para el 56,9% restante no lo es (Azali, 2017).

Generalmente, sucede que algunos mensajes resultan peligrosos para ciertas personas, pero no para otras. Lo que se observa en el caso de Irán, es que el abanico de discursos que caben dentro de esa categoría desde la óptica del gobierno, es mucho más amplio que en otros países. Dado que prácticamente cualquier tipo de contenido publicado que no esté alineado directamente con el sistema político y religioso del gobierno es considerado como una amenaza, quien los publica puede ser fácilmente identificado por el régimen como un *target*.

Luego de que el gobierno bloqueara *Twitter* y *Facebook* tras las elecciones presidenciales en 2009, gran parte de la población iraní migró a otra red del holding Metaverso: *Instagram*. De acuerdo a Mirghaderi (2021), *Instagram* tiene una cantidad mucho mayor de usuarios iraníes activos que las redes antes mencionadas, en parte porque se creó un año después de las revueltas de 2009[13].

Si aplicamos la lógica del *establishment* iraní, cabe preguntarnos entonces por qué razón el gobierno no aplicó a esta red las mismas medidas de restricción y censura que fueron aplicadas

[13] Siguiendo a Azali (2017), si bien no hay estadísticas oficiales confiables que contabilicen la cantidad de usuarios de Instagram en Irán, es posible acercarse a un número aproximado en base a las descargas de esta aplicación. En Café Bazaar - el *marketplace* de Android más popular en la República Islámica - se registraron más de 16 millones de descargas de Instagram para el año 2017. Si a esto sumamos las descargas a través de Google Play y de Apple Store - se estima que para ese mismo año había entre 6 y 7 millones de iPhones en el país -, debería haber más de 20 millones de usuarios de Instagram en Irán. Estos cálculos llevan a que cerca del 3% de los usuarios de Instagram a nivel global sean iraníes - incluyendo en estos números a personas que son originarias de este país pero que habitan en el exterior - (Azali, 2017). En 2018, Irán ocupó el 7º lugar en el mundo de cantidad de usuarios de Instagram (Financial Tribune, 2018)

a *Twitter* y *Facebook*. Es aquí donde los móviles ideacionales - intentar alinear a la sociedad bajo el paraguas político gubernamental, persa y chiita - chocan con los intereses materiales: en el período estudiado, podemos observar un crecimiento exponencial de la valorización de las redes sociales - y de los *influencers* - en la economía del país.

Según Mirghaderi (2021) "el impacto de la cultura de los *influencers* en Irán está a un nivel en el cual los funcionarios del gobierno estimaron que restringir el acceso a *Instagram* puede implicar una pérdida de ingresos para más de un millón de iraníes" (p. 4). Las redes sociales - especialmente *Instagram* - permitieron reducir notablemente el costo destinado a publicidad para marcas y empresas. La promoción de productos y servicios a través de *influencers* es un método que ganó una gran participación en la estrategia de marketing, dado que los seguidores suelen confiar en - y muchas veces imitar a - los *influencers*.

3. Capital tecnológico y herramientas para ejecutar la política de ciberseguridad a nivel doméstico

Irán rápidamente desplegó una amplia gama de medidas que se manifiestan en una serie de instituciones y proyectos, como por ejemplo la *Red Nacional de Información* (NIN) o *Halal Internet*, un régimen integral de Internet independiente aislado de la *World Wide Web*. La misma se desarrolló en el Ministerio de Tecnología de la Información y las Comunicaciones en 2005; y para el año 2012 se estima que alrededor de 10.000 computadoras ya incluían el sistema propio de Internet *Halal Internet* (Berman, 2013).

De acuerdo a la página oficial de la NIN, el Consejo Supremo del Ciberespacio Irán la define como una "Red basada en el Protocolo de Internet con conmutadores, enrutadores y centros de datos que permite que las solicitudes de datos eviten ser enrutadas fuera del país y proporciona redes de Internet seguras y privadas (Red Nacional de Información, 2020)."

Desde Teherán aseguran que en el marco del Quinto Plan de Desarrollo Económico de Irán, la NIN - con un ancho de banda de 4.000 gigabytes por segundo - permitirá el acceso a servicios de gobierno electrónicos, a servicios digitales dentro del país, a comunicaciones de alta velocidad, y a servicios nacionales. Tasnim News Agency, una agencia alineada estrechamente con la Guardia Revolucionaria de Irán, describió a la NIN como "un nuevo sistema de Internet con alta seguridad que será hasta 60 veces más rápido que las mejores velocidades actualmente disponibles"(Tasnim News Agency, 2016).

La investigadora y tecnóloga persa Masha Alimardani (2016) afirmó en su nota para Global Views que el gobierno iraní ha asignado alrededor de $USD 200 millones para el desarrollo de infraestructuras y de contenido electrónico de NIN. Según el *establishment* persa, una de las principales misiones es romper el monopolio de Internet. En 2016, el entonces presidente moderado Hassan Rouhani definió a *Halal* como "uno de los componentes claves de la independencia del país" (Alimardani, 2016). De hecho, aseguró que la NIN debería ser una Internet sostenida por centros de datos que sean completamente indetectables e impenetrables a fuentes externas y permita la creación de redes de intranet privadas y seguras" (Alimardani, 2016). Las autoridades han enfatizado en cómo esta red puede ayudar a proteger la seguridad de la información que circula en la red contra ciberataques como el de la *Stuxnet*, dirigida a las instalaciones nucleares de Natanz y Busher. A su vez, aseguran que la red no interferirá con el acceso de los iraníes a la Internet global.

Sin embargo, Alimardani expresó a Global Voices:

> "En general, parece que el plan es alentar a los sitios *web* iraníes a reubicar su alojamiento en Irán mediante la aplicación de precios discriminatorios del ancho de banda para la conexión a Internet nacional frente a la internacional. Alojar la mayoría de estos sitios *web* dentro del país facilita al gobierno iraní la desconexión de Internet si fuera necesaria" (Alimardani, 12 de septiembre de 2016, Global Voices).

De hecho, la periodista especializada en tecnología de la BBC Persian Nima Akbarpour realizó una encuesta en *Twitter* y les preguntó a sus 107 mil seguidores si estaban preocupados sobre esta inauguración de *Halal*. Las respuestas mostraron que una abrumadora mayoría - 70% de los votantes - estaban preocupados, mientras que el 30 % indicó que no se sentían amenazados (Alimardani, 2016).

Una de las particularidades que más interesan al régimen es el atributo de filtrado inteligente con el que cuenta la NIN. Se trata de una de las tecnologías de filtrado más sofisticadas del mundo, junto con las de China y Túnez. El sistema puede escanear la navegación de los usuarios e identificar ciertas palabras clave prohibidas, negando así automáticamente el acceso a ese sitio (Kelly y Cook, 2011).

Además del filtrado aplicado a *Halal*, la República Islámica también desarrolló otras tecnologías de esta naturaleza en conjunto con la compañía persa Amnafzar Ltd. El producto

se denomina Separ, y se destaca por su capacidad de actualizar constantemente su estrategia de filtrado para limitar los esfuerzos de los usuarios de evadir los filtros (Kelly y Cook, 2011).

De acuerdo a las conclusiones de la *OpenNet Initiative*[14], se observa un gran aumento en la utilización de filtrado cibernético a escala global. Para el año 2009, los investigadores de *OpenNet* descubrieron que este recurso es aplicado en más de tres docenas de países sobre los 71 que fueron examinados. Esto da cuenta de un aumento respecto de los 25 países que aplican filtros según un informe de 2006, que examinó un total de 46 naciones (Talbot, 2009).

La investigación presentada en 2009 también reveló un incremento en la cantidad de bloqueo a sitios *webs*, redes sociales y blogs - especialmente en el MENA - (Talbot, 2009). Se observa que en comparación con esta medida, el filtrado de palabras clave es una herramienta de control mucho más matizada que otras tecnologías, dado que permite el acceso a un sitio *web* determinado, pero no a un artículo o contenido en particular que contenga una palabra clave confidencial en su ruta URL.

La primera - la prohibición de páginas *web,* blogs y/o aplicaciones – es una de las herramientas preferidas del gobierno iraní. Se estima que casi el 50% de los quinientos sitios *web* más visitados del mundo están bloqueados, entre los que se encuentran aplicaciones como *Facebook*, *Twitter, Telegram* y *Google Plus* - además de páginas relacionadas a salud, ciencia, deporte y compras - (Aryan, Aryan y Halderman, 2013). Esto dio lugar a lo que Sexton y Campbell (2020) denominaron como "autoritarismo digital", refiriéndose a la censura aplicada sobre la propia población no sólo para silenciar a los disidentes después del Movimiento Verde, sino también para socavar la formación de movimientos opositores en primer lugar (Sexton Campbell, 2020).

Si bien en la era digital la censura se vio obligada a diversificar sus campos de acción, la misma existe desde el nacimiento propio de los medios de comunicación. Según datos recabados por *Journalism is not a crime*[15], desde la aparición de los medios de comunicación modernos en

[14] La *OpenNet Initiative* es un proyecto mancomunado entre varias instituciones de prestigio internacional entre la cuales se encuentran la Universidad de Harvard, la Universidad de Toronto, la Universidad de Oxford y la Universidad de Cambridge. El mismo estudia la difusión de la censura en Internet y la vigilancia a nivel mundial.

[15] *Journalism is not a crime* (en español "el periodismo no es un crimen") es un sitio *web* que contiene, analiza y difunde una base de datos completa con todos los periodistas que han sido apuntados, amenazados, perseguidos, denunciados o incluso ejecutados por los sucesivos gobiernos iraníes. El mismo cuenta con una sección denominada "The Wall of Shame" (el Muro de la Vergüenza) donde se desarrollan testimonios de los reporteros, editores, fotógrafos, blogueros y periodistas que fueron encarcelados por difundir noticias y análisis en contra del *establishment* político persa. En esta página *web* también se publican noticias diarias sobre censura, arrestos,

Irán en 1905, los sucesivos gobiernos han intimidado, torturado y encarcelado sistemáticamente a periodistas y activistas que difundían ideas y noticias - no convenientes para el gobierno - a través de los medios de comunicación. De acuerdo a *Journalism is not a crime*, estas persecuciones hacia figuras mediáticas ha empeorado desde la Revolución Islámica de 1979**.**

4. Casos testigos: las revueltas de 2017/2018 y 2019

El 28 de diciembre del 2017 en Mashad - la segunda ciudad más grande de Irán - cientos de personas se autoconvocaron en las calles para reclamar al gobierno por la situación económica del momento, con el desempleo como principal preocupación. Las protestas en Mashad rápidamente se expandieron a otras ciudades, abarcando un rango geográfico sin precedentes.

En esa ocasión no serían *Twitter* y *Facebook* las redes sociales que más relevancia tuvieron, sino *Telegram*. Este servicio de mensajería instantánea - que contaba con más de cuarenta millones de usuarios al momento de las protestas -, fue el elegido como canal de comunicación. Las ventajas de esta aplicación era que no precisa demasiados megas (a diferencia de *Instagram* por ejemplo);tiene mucha capacidad de descarga; y permite la comunicación entre las personas y la difusión a través de canales de comunicación abierta. Sumado a eso, también se pueden programar los mensajes con autodestrucción lo que imposibilita el rastreo de la información.

A finales de 2017 las autoridades iraníes bloquearon temporalmente *Telegram* e *Instagram*, las cuales se desbloquearon por decisión de Rouhani el 4 y 13 de enero de 2018 respectivamente. Pero para el caso de la primera, el desbloqueo duraría poco. Desde marzo distintos funcionarios comenzaron a demostrar su apoyo a una restricción definitiva de la misma. A inicios de 2018 el poder judicial acusó a la red de mensajería de "perturbación de la unidad nacional", "propaganda contra la República Islámica", e "insultos a lo sagrado".

Para mayo de ese mismo año el Poder Judicial obligó a todos los proveedores de Internet el bloqueo a la aplicación y el sitio *web* de Telegram. A pesar de las restricciones, los ciudadanos iraníes han sabido evadir las trabas puestas a la plataforma contactandose a VPNs (redes virtuales privadas) o aplicando una retórica en la que se expresan opiniones evitando utilizar puntualmente las palabras que pueden caer en el filtrado inteligente del gobierno. De hecho, el

encarcelamientos y todas las acciones tomadas por el gobierno iraní para limitar la libertad de expresión. Más información en https://journalismisnotacrime.com.

número de usuarios de *Telegram* aumentó desde su prohibición. En pleno 2021, se estima que más de 45 millones de iraníes utilizaron la red a pesar del bloqueo, enviando un promedio de 15 mil millones de mensajes cada día. (Górka, 2021).

Otro caso testigo donde se visibiliza la política de ciberseguridad a nivel doméstico, así como también la reacción de la población, es la movilización de 2019. Los últimos meses de ese año encontró a la sociedad iraní nuevamente movilizada luego de que el 15 de noviembre el gobierno anunciara un aumento en el precio de combustible más de un 50%. Sumado a esto, la inflación anual rondaba el 40%, un 30% más alta que la de 2017 (Castro Torres, 2019).

La respuesta del régimen fue rápidamente reprimir, llevando las fuerzas a las calles para aplacar a la población. Con el antecedente del rol que habían tenido las redes sociales y la *web* en general en las revueltas de 2009 y 2017/2018 - no solo respecto a la convocatoria sino también a la difusión -, el mismo 15 de noviembre a la noche el gobierno ordenó el bloqueo total de Internet. De acuerdo a informes de *Human Rights Watch*, la violencia utilizada contra los manifestantes llegó a ser en muchos casos letal; pero debido al apagón de Internet no fue posible conocer a ciencia cierta la brutalidad de la represión y el número de muertos. (Human Rights Watch, 2019).

Amnistía Internacional en conjunto con The Hertie School llevó adelante un proyecto de investigación denominado Detección y Análisis de Internet (IODA) sobre las protestas en cuestión. El 16 de noviembre, cuando las protestas ya habían comenzado a expandirse por distintas ciudades y los reclamos se habían radicalizado, IODA detectó que las señales de Internet comenzaron a descender en distintos puntos del país. Los operadores de celulares comenzaron a desconectarse a partir de las las 2 p.m de Irán, y para la tarde ya había descendido totalmente. Cinco días después, el 21 de noviembre a las 10 a.m IODA detectó que comenzaba a subir -y recuperarse- la señal de Internet. En este contexto de aislamiento de la sociedad iraní del resto del mundo, Amnistía Internacional asegura que tuvo lugar la represión más violenta. De las 323 muertes verificadas entre el 15 y 19 de noviembre, 237 se llevaron a cabo entre el 16 y el 21 de noviembre (Amnistía Internacional, 2020).

En síntesis, observamos que lo que tienen en común estas revueltas (2009; 2017/2018; y 2019) – además del evidente rol preponderante que tuvieron el ciberespacio y las redes sociales - es que en todos los casos la respuesta del gobierno iraní tuvo como norte evitar una posible *soft*

revolution; lo que en los términos de Siboni y Kronenfeld (2012) es una revolución pacífica por medio de las redes sociales, alimentada por la penetración de información de occidente.

5. La política de ciberseguridad iraní en tiempos de pandemia

La República Islámica de Irán fue epicentro de la crisis de COVID-19 en el Medio Oriente. En materia cibernética, la pandemia ha venido a acelerar procesos y tendencias que se venían desarrollando con antelación. La traspolación del plano real al virtual como consecuencia de la cuarentena, coadyuvó en un aumento exponencial de las actividades *online* y de las interacciones entre los internautas.

Lo que se observa en este período, es que la política de ciberseguridad persa en la dimensión doméstica se focalizó principalmente en lanzar una "campaña de desinformación" en términos de Ayesha Ilyas (2020). A nivel práctico, las instituciones cibernéticas apelaron a intensificar el control sobre las páginas *web*s que podrían contener información sobre el virus, publicaron datos de salud pública distorsionados, y prohibieron el acceso a sitios relacionados a salud (Ilyas, 2020). La versión oficial asegura que el coronavirus fue deliberadamente planificado por EE.UU., como consecuencia de una guerra biológica iniciada por el mismo. De acuerdo a Ilyas (2020), el principal objetivo de la campaña era intensificar los desacuerdos entre EE.UU. y sus aliados, y así presionar a Washington para que suspendiera las sanciones hacia la República Islámica.

Al mismo tiempo, la agencia de noticias estatal Islamic Republic of Iran Broadcasting (IRIB) subestimó la gravedad del virus. Por ejemplo, el febrero de 2020, Atefe Mirseyedi - presentadora de televisión de IRIB y comentarista de salud - afirmó que el virus no era más que un resfrío. Siguiendo a Dubowitz y Ghasseminejad (2020), podemos decir que la negación y la minimización sustituyeron la preparación.

El Ministerio de Cultura y Orientación Islámica (MCIG) y el Ministerio de Inteligencia juegan un papel fundamental en la imposición de la censura. Son los responsables de otorgar el visto bueno a revistas, periódicos, libros, películas, música y centros culturales; así como también de vigilar a reporteros extranjeros en territorio nacional. En marzo de 2020, ante la necesidad de reducir la propagación de noticias respecto al COVID-19, el MCIG prohibió la impresión y

distribución de todos los periódicos y revistas. De esta forma, se dio inicio a una fuerte campaña propagandística tanto a través de medios tradicionales como digitales. A modo de ejemplo, el 23 de marzo de 2020 el Ministerio de Asuntos Exteriores tuiteó: "Si @StateDept afirma que las crecientes preguntas globales sobre el papel de EE. UU. en la pandemia de #COVID19 son meras 'teorías de conspiración hechas por Irán', entonces EE. UU. debe responder algunas de estas preguntas formuladas por Global Research." Este tuit incluía un enlace a un artículo publicado por el sitio *web* Global Research, que afirmaba que el origen del virus era estadounidense. IRIB - el cual mantiene el monopolio de la transmisión televisiva en Irán - es la herramienta principal de Teherán para la propaganda interna. En este contexto, se focalizó en minimizar la propagación de la pandemia de Irán y difundir versiones distorsionadas.

6. Conclusiones parciales del capítulo I

Como se pudo examinar a lo largo de este capítulo, la política de ciberseguridad iraní aplicada al ámbito doméstico ha ido evolucionando con mayor ahínco desde el año 2009. Atravesando por hitos como las revueltas de 2017/2018 y 2019, y la pandemia de COVID-19; la política de ciberseguridad defensiva y ofensiva aplicada a nivel nacional se fue perfeccionando y adaptándose con rapidez y precisión a los advenimientos tecnológicos.

En otras palabras, la estrategia gubernamental en el ciberespacio se fue desarrollando en forma de espiral, abarcando cada vez más aristas e incluyendo recursos más sofisticados. Como mencionamos previamente, la misma fue tomando tintes de una estrategia cada vez más asertiva y más rigurosa, con un objetivo último en claro: garantizar la seguridad y la integridad del régimen iraní.

El régimen y el entramado cibernético institucional han sabido leer los distintos contextos para afinar la estrategia de ciberseguridad más apropiada. Más específicamente, consideramos que las organizaciones más relevantes en lo que respecta a la protección del régimen fueron las ramas cibernéticas de la IRGC . Al calor de los comicios del año 2009 y luego del advenimiento de la Primavera Árabe, el foco estuvo puesto en el control y restricción de las redes sociales - principalmente *Facebook* y *Twitter*, que desde entonces y hasta el momento de escribir esta tesina estuvieron prohibidas-.

La indiscutible relevancia que tuvieron primero en la divulgación de ideas y luego arrojando luz a lo que acontecía en Irán durante las protestas fueron razones suficientes para que el gobierno decida bloquearlas. Con los levantamientos de finales de 2017 e inicios de 2018 el medio de comunicación que prevaleció fue *Telegram*, por lo cual fue el principal apuntado por

el gobierno; y en 2019 las medidas de control del ciberespacio desbloquearon un nivel al cual nunca antes se había llegado: durante días directamente se interrumpió el acceso a Internet en los focos de levantamiento. Finalmente, la pandemia de COVID-19 y la consecuente virtualización de múltiples espacios de interacción, aceleró y afinó la política de ciberseguridad que venía desarrollándose desde 2009.

A partir de esto, observamos que la aparición de Internet y el desarrollo tecnológico posterior reforzaron la idea planteada por la teoría de la interdependencia compleja; según la cual los actores de la comunidad internacional son cada vez más numerosos, y las interconexiones se multiplican.

Asimismo, la constante adaptación del gobierno iraní a las últimas tecnologías y al nuevo paradigma comunicacional, dan cuenta de que pese a la pluralidad de jugadores en la arena política – nacional e internacional – el Estado continúa siendo el actor por excelencia - un aporte troncal de la teoría realista -. En suma, luego de lo analizado observamos que tal como afirma Paredes Roibas (2018) en su teorización acerca del ciberespacio, los Estados tienen soberanía en el plano físico de este dominio – esto es, en la infraestructura y las computadoras que se encuentren bajo su jurisdicción -; y pueden también prohibir el acceso a determinadas páginas *web*. Esto se ve con claridad, por ejemplo, en los mencionados bloqueos a las redes sociales; e incluso en el apagón de Internet de 2019. En este sentido, el Estado sigue teniendo una ventaja evidente respecto a otros actores de la comunidad internacional.

En el próximo capítulo, nos focalizamos en identificar los objetivos y las acciones de la política de ciberseguridad persa en su accionar externo, en el marco de la rivalidad con EE.UU., Arabia Saudita e Israel.

Capítulo II

Gran parte de la bibliografía consultada coincide en identificar el ciberataque del virus Stuxnet como un detonante de la política de ciberseguridad iraní en el plano internacional. Este tuvo lugar en junio de 2010 y afectó las instalaciones nucleares iraníes de Bushehr y Natanz, provocando retrasos de entre uno a dos años al programa nuclear iraní.

Si bien debido a la naturaleza del ataque resulta difícil conocer a ciencia cierta el origen del mismo; numerosos autores - occidentales y no occidentales - afirman que se trató de una operación planificada y ejecutada mancomunadamente entre los servicios secretos de EE.UU. (EE.UU.) e Israel.

En primer lugar, desarrollaremos acerca de este virus, que se convirtió en un punto de inflexión del devenir de la política de ciberseguridad iraní en el plano internacional -.

En segunda instancia, abordaremos la rivalidad existente entre la República Islámica y EE.UU., Arabia Saudita e Israel (con los dos últimos especialmente en el escenario regional) durante el período estudiado. Observaremos que los medios a través de los cuales tiene lugar la disputa por el poder con estos países fueron mutando, pero siempre con los mismos objetivos en claro para Irán: preservar la integridad del régimen y convertirse en una potencia cibernética regional.

A continuación, identificaremos los aliados - gubernamentales y no gubernamentales - y las cibercapacidades *con las que cuenta Irán para la ejecución de la política de ciberseguridad en el plano internacional. Finalmente, esbozaremos una conclusión parcial de este capítulo.*

1. *Stuxnet*: el antes y después de la política de ciberseguridad en la dimensión internacional

1.1 Características del ciberataque

Es plausible afirmar que, a raíz de este ciberataque - que según algunos autores formó parte de un plan mayor conocido como *Operación Juegos Olímpicos* -, el gobierno iraní posicionó el tema de la seguridad cibernética en lo más alto de su agenda de seguridad nacional e internacional.

Solo luego de meses de investigación, las compañías Kaspersky[16] y Symantec[17] descubrieron, entre otras características, que el propósito de *Stuxnet* no era espiar, sino comprometer el funcionamiento de las centrifugadoras.

Si bien el virus infectó computadoras alrededor de todo el globo, se estima que aproximadamente un 60% de las mismas estaban ubicadas en Irán (Matrosov et al. 2010). Una vez dentro del sistema, el virus tomó el mando de los controladores lógicos programables (o PLC[18]), que se utilizan para regular la potencia de dispositivos industriales (De Falco, 2012).

Además, de acuerdo a Chen y Abu-Nimeh (2011), *Stuxnet* también podía comunicarse con otras máquinas infectadas y enviar la información recopilada a servidores en Dinamarca y Malasia. El mecanismo empleado por el virus para descomponer las centrifugadoras se basó en un constante cambio de velocidad de las mismas, causando su recalentamiento y consecuentemente daños irreparables (Langner, 2013). [19]

1.2 Presuntos desarrolladores del virus

Como se mencionó previamente, resulta casi imposible conocer a ciencia cierta quiénes y cuántas partes estuvieron involucradas en la planificación y elaboración de *Stuxnet*. No obstante, se considera que los dos principales apuntados (Israel y EE.UU.) contaban no sólo con los recursos humanos y económicos para desarrollarlo, sino también los móviles políticos.

Ambos son declarados enemigos iraníes desde la Revolución Islámica de 1979, y no veían con buenos ojos que su rival - con las capacidades militares y la influencia que posee - ejecute con éxito el programa nuclear que podría traducirse en la creación de una bomba de esta naturaleza.

En suma, expertos de *Symantec* afirmaron haber identificado evidencia de implicación israelí en las líneas de codificación (Zetter, 2011). Por ejemplo, se descubrió que la palabra "*myrtus*" era parte del código, y que el mismo nombre llevaba el archivo donde se almacenó el virus

[16] Fundada en Moscú en 1997, la empresa se especializa en productos que brindan seguridad informática, *firewall*, anti-spam y antivirus.

[17] Es una compañía californiana creada en 1978 que ofrece servicios de seguridad de la información.

[18] Un PLC (Programmable Logic Controller) es un controlador de programación que activa los componentes de la maquinaria para que desarrollen actividades automáticas o potencialmente peligrosas para las personas.

[19] Irán utiliza centrifugadoras IR-1, un modelo europeo que data de finales de los años 60´ y principios de los 70´, que son - además de antiguas - altamente vulnerables a los cambios de velocidad - condición que los desarrolladores de Stuxnet lograron identificar y explotar (Langner, 2013).

cuando se estaba desarrollando. La relevancia está en que esta palabra es una referencia a la reina Ester, quien de acuerdo al antiguo testamento de la biblia salvó a los judíos de una masacre en manos de los persas (Baezner y Robin, 2017).

Además, se sostiene que el ciberataque fue la piedra angular dentro de la mencioanda *Operación Juegos Olímpicos*. En el marco de la misma, tuvieron lugar los asesinatos de los científicos iraníes en 2010 y 2011 - piezas claves del programa nuclear persa -, que también fueron atribuidos a EE.UU. e Israel (De Falco, 2012).

Alternativamente, Farwell y Rohozinski (2011) argumentaron que el diseño de mosaico de *Stuxnet* indica que este virus podría haber sido desarrollado - al menos en parte -, por un grupo de hackers profesionales dedicados al cibercrimen, específicamente de origen ruso. Estos autores explican que algunos elementos del código tienen el mismo diseño que la codificación escrita por las comunidades rusas de programación asociadas a la ciberdelincuencia (Farwell y Rohozinski, 2011).

A su vez, siguiendo a Farwell y Rohozinski (2011), no resulta descabellado plantear que Moscú estuviera detrás del ataque, dado que numerosos trabajadores que tenían acceso a las instalaciones nucleares en Irán eran de nacionalidad rusa. Respecto al móvil para llevar a cabo el ciberataque, es menester mencionar que Rusia no sólo tiene las capacidades para desarrollar el *malware*, sino que con la producción de energía nuclear comprometida, Irán se vería obligado a recurrir al Kremlin para comprar uranio enriquecido (Baezner y Robin, 2017).

1.3 Impacto de nacional e internacional de Stuxnet:

A nivel internacional, *Stuxnet* representó una llamada de atención para los países. De repente, el diseño de una política de ciberseguridad escaló en las agendas estatales, al igual que aumentaron las preocupaciones en torno a la protección de las infraestructuras críticas vinculadas al ciberespacio.

Ocurrió lo que Baezner y Robin (2017) caracterizan como un sentimiento global de inseguridad. El temor del surgimiento de nuevas versiones de *Stuxnet* se vio incrementado ante la probabilidad de que estos virus caigan en manos de grupos dedicados al cibercrimen.

Al mismo tiempo, este ciberataque también trajo cierta calma a la comunidad internacional, debido a la ralentización del programa nuclear iraní que éste generó. Desde que la Asociación

Internacional de Energía Atómica (AIEA) había dado a conocer al mundo la existencia del mismo en 2002, las tensiones internacionales en torno a este asunto habían incrementado.

Para Irán particularmente, este ataque fue altamente costoso en términos económicos. Por un lado, debido a los embargos internacionales la República Islámica no tenía acceso al mercado internacional para comprar materiales relacionados a la energía nuclear - principalmente uranio enriquecido -. Por el otro, se perdieron millones de dólares que se habían invertido en la fabricación de centrifugadoras de las cuales casi 1.000 dejaron de funcionar como consecuencia del ciberataque (Matrosov et al.,2010).

Stuxnet también tuvo repercusiones económicas a largo plazo debido a los retrasos en la producción de uranio y a las inversiones que necesariamente se tuvieron que realizar en el fortalecimiento de las medidas de ciberseguridad en las instalaciones nucleares. Irán tardó aproximadamente un año en recuperarse totalmente de los efectos de *Stuxnet* y en volver a un nivel de producción similar a noviembre de 2009 (Matrosov et al.,2010).

En el plano político, el ciberataque desacreditó al gobierno persa al mostrarse incapaz de proteger sus instalaciones nucleares ante un ciberataque extranjero. La cúpula gubernamental iraní se mostró indecisa acerca de cómo reaccionar ante la noticia de que un virus informático había infectado cientos de sus centrifugadoras.

En un primer momento, se limitaron a confirmar que los únicos aparatos que habían sido afectados eran las computadoras de parte del personal, pero que no estaban conectadas con las instalaciones de Bushehr y Natanz. Más tarde, Teherán admitió que *Stuxnet* había estado activo en sus plantas nucleares durante más de un año. (Zetter, 2011).

2. El devenir de la política de ciberseguridad iraní en el marco de la rivalidad con EE.UU., Arabia Saudita e Israel

El desarrollo iraní en el ciberespacio no debe comprenderse como un hecho aislado y azaroso, sino que debemos enmarcarlo en un contexto de candente rivalidad con EE.UU, Arabia Saudita e Israel. A continuación, analizaremos cómo la competencia con estos países funcionó como un incentivo para que Irán acelerara el desarrollo en su política de ciberseguridad en la dimensión externa – especialmente luego de verse truncado programa nuclear -.

2.1 Rivalidad entre Irán y EE.UU.

Los objetivos de la política exterior estadounidense e iraní se oponen fuertemente entre sí en múltiples niveles. EE.UU. ve a Irán como un estado canalla y una fuente de inestabilidad en el MENA, posicionándose como una amenaza directa para los aliados e intereses norteamericanos en la región (Mehran, 2008).

Al mismo tiempo, la cúpula gubernamental iraní considera a EE.UU. como un hereje que hace uso y abuso de su poder cuasi hegemónico, al instalarse militarmente en el Golfo Pérsico, Afganistán e Irak para asegurarse para sí y para sus aliados el acceso a los vastos recursos regionales (Mehran, 2008).

Si bien las rispideces entre Irán y EE.UU. venían en alza desde finales de la década del ´70, las relaciones se agudizaron especialmente luego de que George W. Bush - el entonces presidente norteamericano - diera un discurso ante el congreso el 29 de enero de 2002, en el cual hace alusión a la necesidad de combatir el "eje del mal" en pos de la seguridad internacional. Dentro de esa lista negra se enumeraban los principales Estados considerados como patrocinadores del terrorismo global y poseedores de armas de destrucción masiva. La misma estaba encabezada por Irak, seguido por Irán y en tercer lugar, Corea del Norte.

No obstante, la República Islámica aseguró que su programa nuclear no violaba en absoluto el Tratado de No Proliferación Nuclear (TNP), en vigencia desde 1970, dado que se ampara en el punto 1 del artículo 4: "*Nada de lo dispuesto en este Tratado se interpondrá en el sentido de afectar el derecho inalienable de todas las Partes en el Tratado de desarrollar la investigación, la producción y la utilización de la energía nuclear con fines pacíficos (...)"* (Tratado de No Proliferación Nuclear, 1970, p. 16).

Existe un consenso entre la comunidad académica occidental en entender la estrategia implementada por Irán como *bombs in a fog*, es decir, un ocultamiento y falta de transparencia en torno al programa nuclear, debido a la ausencia de evidencias de las intenciones pacíficas esbozadas por el gobierno (Waltz, 2012).

Con el arribo de Barak Obama a la presidencia estadounidense, se puede ver un péndulo que oscila de Irak hacia Irán en relación al orden de prioridades que estos países pasaron a tener en la agenda de Washington hacia el Medio Oriente. En términos empíricos, vemos que EE.UU. se retira finalmente de Irak en 2011 y aumenta su preocupación en torno al programa nuclear iraní, que desembocará en la firma del Plan de Acción Integral Conjunto (JCPoA por sus siglas en inglés) firmado el 14 de julio de 2015.

El objetivo más importante de este acuerdo - firmado por Irán, EE.UU., Rusia, China, Reino Unido, Francia y Alemania - fue reorientar el mencionado programa hacia fines exclusivamente pacíficos - limitando la producción de uranio enriquecido permitida a un 3.673% -; a cambio de un levantamiento de las sanciones que tanto las seis potencias, como la Unión Europea (UE) y la ONU habían impuesto a la República Islámica.

Desde la denuncia de la AIEA en 2002, y pasando por la adopción de varias sanciones multilaterales y unilaterales desde 2006, la economía iraní se ha ido deteriorando: se redujeron las exportaciones de un 2,5 millones de barriles de petróleo diarios a sólo 1 millón, y su PBI disminuyó en torno al 9% cada año a partir de las sanciones, según los datos revelados por el Real Instituto Elcano (Núñez Villaverde, 2015). Fue el impacto de todas estas acciones las que llevaron a Irán a aceptar la firma de un acuerdo.

Sin embargo, la llegada de Trump a la Casa Blanca puso fin a la relativa tregua que se había alcanzado entre los dos países con el acuerdo nuclear. El entonces Consejero de Seguridad Nacional de Trump, Michael T. Flynn, declaró que Irán volvía a estar "en la mira" cuando en febrero de 2017 lanzó un misil balístico en aparente violación de la resolución 2231[20] del Consejo de Seguridad de la ONU y del Acuerdo Nuclear.

El conflicto con Irán tiene también otras facetas. Su profundo involucramiento con la guerra de Siria, apoyando el régimen de Bashar al-Asad; su considerable influencia política y militar en Irak; y su financiamiento a Hezbollah en el Líbano y los Hutíes en Yemen - identificados por el *establishment* nosrteamericano como organizaciones terroristas -; representan amenazas directas a los intereses de EE.UU. y de sus aliados de la región.

Esas rispideces, sumado al descreimiento por parte del gobierno estadounidense respecto a las intenciones del programa nuclear, coadyuvaron a que el la Casa Blanca se retirara del Acuerdo en mayo de 2018 . Quizás haya pasado desapercibido desde el punto de vista de las relaciones internacionales que las disputas por el poder entre Washington y Teherán tenían también lugar en el dominio virtual, un terreno poco explorado desde el punto de vista académico.

[20] La resolución 2231 del Consejo de Seguridad del año 2015 insta a que se aplique plenamente el JCPoA dentro de los plazos previstos en su anexo V y establece las siguientes medidas para la supresión definitiva de las sanciones del Consejo de Seguridad contra Irán.

De acuerdo a Craig y Valeriano (2016) EE.UU. e Irán tienen un largo historial de ciberconflicto entre sí. Entre 2001 y 2011 la República Islámica fue mayormente receptor de ciberataques lanzados por EE.UU.

Inicialmente, el único incidente documentado librado por Irán había sido el hackeo de *Twitter* en 2009, que redireccionaba a los usuarios a una página *web* donde se veía una imagen de una bandera verde con el nombre del tercer Imán chiíta, Imán Hussaín; y rezaba "este sitio ha sido hackeado por el Ejército Cibernético de Irán" (Craig y Valeriano, 2016). También incluía un poema en persa que decía: "Debemos golpear si el líder lo ordena, debemos perder nuestras cabezas si el líder lo desea. Aquellos que siguen el camino de la lucha de Dios ganarán" (BBC Mundo, 2009).

A raíz de este hecho, la Casa Blanca comenzó a percibir a Irán como una fuente de amenazas cibernéticas latentes. En su discurso frente al Comité de Inteligencia del Senado en 2012, el Director de Inteligencia Nacional, James Clapper, advirtió que las operaciones de inteligencia de Irán contra EE.UU. habían aumentado dramáticamente en los últimos años (Craig y Valeriano, 2016).

Por lo tanto, no resulta sorprendente que los datos presentados sobre el gasto que destina EE.UU. en la guerra cibernética muestre aumentos notables. De hecho, la evidencia sugiere que ambos países desarrollaron sus capacidades como reacción ante el accionar de su oponente. Aquí se vislumbra el tono altamente competitivo - propio de las carreras armamentistas tradicionales - que adquiere la guerra en el ciberespacio, reflejado en el aumento rápido y mutuo de las capacidades cibernéticas (Craig y Valeriano, 2016).

Para el año 2012 Irán ya se encontraba posicionado de otra manera en el quinto dominio. Tal fue la evolución de Irán que el jefe del Comando Espacial de la Fuerza Aérea norteamericano, el general William Shelton, declaró ante los medios en enero de 2013 que Irán se había convertido en un país del cual no se debían subestimar sus potenciales capacidades cibernéticas (Shalal-Esa, 2013). A su vez, solicitó aumentar el gasto destinado a la ciberseguridad y anunció planes para aumentar la cantidad de personal cibernético (Shalal-Esa, 2013).

Si bien tal como lo recalcan Sexton y Campbell (2020) Irán apunta con mayor frecuencia a los adversarios en el MENA, se han dirigido múltiples ataques contra EE.UU., incluida la Operación Ababil en el año 2012 (también conocida como Mahdi), que tuvo como *target* el Sands Casino en Las Vegas y causó daños por $40 millones de dólares.

Teniendo también como blanco al sector financiero norteamericano al año siguiente tuvo lugar lo se conoció como el ataque cibernético más eficiente que haya organizado Irán contra EE. UU.: *la Operación Babel* (Siboni y Kronenfeld, 2012). Según datos recabados por el FBI, 46 importantes empresas financieras y bancos como JP Morgan Chase (JPM.N), Wells Fargo (WFC.N) y American Express (AXP.N) se vieron afectados (Siboni y Kronenfeld, 2012).

Este tipo de ataques continuó en los años siguientes, pero no fueron tan efectivos como los que fueron lanzados en julio de 2013. Durante la ejecución de los mismos, múltiples transacciones bancarias no pudieron realizarse, los titulares de cuentas no pudieron retirar dinero, y el *home-banking* de estas compañías dejó de funcionar. Se afirmó que la pérdida fue de unos $10 millones de dólares (Siboni y Kronenfeld, 2012).

Irán ha ganado notoriedad entre sus adversarios regionales y los EE. UU. por su sofisticada estructura de ciberseguridad; razón por la cual la Casa Blanca ha otorgado mayor libertad a los comandos militares y las agencias de inteligencia para responder a los ataques cibernéticos con fuerza cinética y ataques cibernéticos de represalia. Siguiendo a Sexton y Campbell (2020)**, "**la actividad en el ciberespacio puede ser considerada tanto un síntoma como una causa de los cambios geopolíticos, y se debe esperar que tenga ramificaciones en el plano físico" (p. 9).

Un claro ejemplo de esto fue lo acontecido en junio de 2019, cuando el entonces presidente de EE.UU., Donald Trump, ordenó un ataque cibernético para desactivar una base de datos que la IRGC había utilizado para atacar seis de petroleros cerca del Estrecho de Ormuz dos meses antes. Dos días antes de que el Comando Cibernético de EE.UU. (USCYBERCOM) se responsabilizara por el ataque contra la base de datos iraní, un dron norteamericano que sobrevolaba el espacio aéreo en disputa fue derribado por un misil persa. Rápidamente Trump aprobó los ataques aéreos contra varias baterías de radar y misiles iraníes.

2.2 Rivalidad con Arabia Saudita

Al igual que con EE.UU, la rivalidad entre la República Islámica y Arabia Saudita tiene una larga trayectoria; y en este caso la variable religiosa se presenta como un elemento crucial a los fines de comprender esta guerra fría. Mientras que Irán posee un 80% de población chiita, el reino saudí profesa el wahabismo, el ala más conservadora dentro del sunismo.

En materia de política exterior, Irán aspira a exportar la revolución al resto de la región, promoviendo y financiando a diversos grupos, milicias, partidos políticos y gobiernos; a la vez

que ve a EE.UU. como un hereje y su principal enemigo. Arabia Saudita por su parte pretende mantener el *status quo*, generalmente mediante una política exterior reaccionaria, y mantiene sólidas relaciones con Washington - fundamentalmente en el ámbito económico y militar -.

Al margen de estas grandes divergencias, ambos actores cuentan con significativos recursos que respaldan las aspiraciones regionales de cada uno. Las enormes reservas de petróleo de similar calidad radicadas en sus territorios – según el Observatorio de la Energía, Tecnología e Infraestructura para el Desarrollo Arabia Saudita goza de un 17% de las reservas mundiales e Irán de un 10% (Sabbatella, 2015) -, son un factor esencial de su poder material .

En relación a las fuerzas militares, Irán posee un gran y complejo aparato de seguridad y defensa. La base troncal de este sistema es la IRGC, que a la vez opera coordinadamente junto con otras divisiones fuera del territorio, como las Fuerzas Quds. Por el contrario, Arabia Saudita está supeditada íntegramente a la protección que le brinde EE.UU. en esta materia, lo cual convierte a Washington en uno de sus aliados más valiosos.

Si bien hasta el momento no ha tenido lugar una confrontación directa entre los dos poderes, la competencia entre ambos se desarrolla por medio de guerras *proxies* en un juego de suma cero, donde las ganancias o pérdidas de un actor se traducen en ganancias o pérdidas del otro. Los escenarios más relevantes en los se desenvuelven estas tensiones sectarias son Siria, Yemen e Irak.

Esta rivalidad también se trasladó a planos no físicos - más específicamente en el ciberespacio - que en muchas oportunidades permitió mantener vigente la categorización de "guerra fría" para hacer referencia a la competencia entre estos dos actores.

Como una muestra física de las capacidades cibernéticas ofensivas que estaba desarrollando la República Islámica, ésta lanzó el ciberataque de tipo *wiper*[21] denominado "*Shamoon*" en agosto[22] de 2012 contra la compañía petrolera saudita Aramco (Craig y Valeriano, 2016). Se

[21] Un malware *Wiper* es un tipo de programa malicioso que dispone de un único objetivo: borrar los datos de un ordenador de manera integral e irreversible.

[22] los perpetradores del ataque aprovecharon la noche del Laylat al-Qadr (la Noche del Destino o del Poder), una de las noches más sagradas para el Islam durante el mes de Ramadán que conmemora la revelación del Corán a Mahoma (Sánchiz, 2019).

trata de una empresa estatal valorada en $1.7 billones de euros y productora de más del 10% del petróleo del mundo (Sánchiz, 2019).

Según un artículo publicado por *World Trade Energy*, este incidente implicó una filtración de datos y logró descomponer tres cuartas partes de las computadoras de la petrolera (World Trade Energy, 2022). "Los ciberataques son uno de los principales riesgos a los que nos enfrentamos en Aramco, al mismo nivel que las catástrofes naturales o los ataques físicos", dijo Amin Nasser - presidente y director ejecutivo de la empresa - en la Cumbre Global de Inteligencia Artificial de 2022 celebrada en Riad (Sánchiz, 2019).

De acuerdo a Siboni y Kronenfeld (2012), los hackers originales de este virus dejaron imágenes de una bandera estadounidense en llamas en las computadoras de Aramco y RasGas Co Ltd - la empresa de gas qatarí - en su primer ataque en 2012. El principal sospechoso de llevar a cabo el ciberataque es el grupo de hackers conocido como *Cutting Sword of Justice* (Cyber Law Toolkit, 2012), quienes publicaron un comunicado en la *web* PasteBin donde se puede leer una justificación por las afrentas producidas por el régimen de Al-Saud (Sánchiz, 2019).

Shamoon vuelve a aparecer el 17 y el 19 de noviembre de 2016 y el 23 de enero de 2017. De acuerdo al laboratorio Kaspersky, el virus es prácticamente el mismo que el de 2012, aunque con algunas mejoras técnicas como por ejemplo la posibilidad de utilizar el navegador como vector de entrada para inyectar el *wiper* directamente en la memoria sin usar drivers (Sánchiz, 2019).

Sus objetivos principales continúan siendo la eliminación de datos críticos y la destrucción masiva de operaciones; pero en este caso las víctimas del ataque fueron también los sistemas informáticos de la Autoridad General de Aviación Civil (GACA) de Arabia Saudita (Finkle y Wagstaff, 2016). Tras un intento fallido en 2018, en 2021 ARAMCO volvió a ser blanco de *Shamoon*. En esta oportunidad, la petrolera fue víctima de una filtración de datos que fue objeto de una petición de rescate de 50 millones de dólares en criptomoneda (World Trade Energy, 2022).

Si bien el gobierno Iraní no dio declaraciones públicas acerca de este hecho, investigadores del laboratorio Kaspersky aseguran que la República Islámica es el único país con acceso al código *wiper* original (Siboni y Kronenfeld, 2012). Lo cierto es que la cúpula gubernamental iraní tampoco negó los vínculos con *Cutting Sword of Justice* luego de que numerosos medios de

comunicaciones y portales - como CNN, Al Arabiya News, Cyber Law Toolkit - denunciaran la cercanía del grupo a teherán.

De esta forma, a través de un ataque concreto - atribuido a un *proxy* aparentemente independiente - orientado hacia una empresa (y no una institución política o instalación militar), "Irán reforzaba de manera indirecta su capacidad de ciberdisuasión, evitando el riesgo de una respuesta bélica por parte del reino saudí" (Torres Soriano, 2017, p. 28).

Tal como lo describe Torres Soriano en su artículo *"Guerras por delegación en el ciberespacio"* (2017*), "*Irán ya había sufrido por parte de EE.UU. e Israel el ciberataque más importante conocido hasta el momento (*Stuxnet*), y deseaba hacer un alarde público de sus nuevas capacidades de ciberguerra dirigiendo una acción contra su principal rival regional, y aliado de su enemigo estadounidense" (p. 28).

No obstante, siguiendo a Siboni y Kronenfeld (2012), *Shamoon* no se caracteriza por el mismo nivel de sofisticación tecnológica que *Stuxnet*. Los escritores del código malicioso no parecen ser profesionales altamente capacitados - como los escritores de *Stuxnet* -, dado que el código estaba plagado de errores. Además, el propósito del ciberataque fue la destrucción total de los datos y las computadoras del blanco (Siboni y Kronenfeld, 2012).

2.3 Rivalidad con Israel

Desde que en el año 2002 la AIEA dio a conocer el programa nuclear que la República Islámica estaba desarrollando, Irán se convirtió en una preocupación aún mayor para Israel. La combinación entre la supuesta búsqueda de Irán de desarrollar armas nucleares y su retórica virulenta contra el Estado judío - no en pocas oportunidades la cúpula gubernamental iraní hizo alusión a su ilegitimidad - coadyuvó en una escaladad de tensiones sin precedentes.

Desde que llegó al poder en el 2005, Ahmadineyad ha desatado la condena internacional al decir que el Holocausto era un "mito" y que Israel era un "tumor" en Oriente Medio (Steven, 2010). "El pretexto (el Holocausto) para la creación del régimen sionista (Israel) es falso (...) Es una mentira basada en una reivindicación mítica e improbable", declaró Ahmadineyad en la Universidad de Teherán al final de la manifestación anual anti israelí "Día de Qods (Jerusalén)" (Hafezi, 2009). "Hacer frente al régimen sionista (Israel) es una obligación religiosa y nacional", añadió (Hafezi, 18 de septiembre de 2009).

De acuerdo a Steven (2010), el primer ministro israelí, Benjamin Netanyahu, comparó a Irán con los amalecitas, quienes según la Biblia intentaron exterminar a los israelitas. El mayor temor de las autoridades israelíes no es tanto un ataque nuclear per sé por parte de Irán, sino que más bien que utilice esta ventaja como un incentivo para tomar medidas arriesgadas Steven (2010).

Similar a la guerras *proxies* [23] liberadas por bandos aliados a Irán y Arabia Saudita en territorios ajenos, Israel también ha intentado frenar la influencia persa a través del apoyo de grupos afines, principalmente en Siria. Aquí no sólo ha apoyado a facciones sunitas en guerra contra el régimen de Bashar Al-asad - aliado de Teherán -; sino también al Frente Nusra, una rama de Al Qaeda situada al suroeste de Siria en los Altos del Golán que luchan contra Hezbollah - respaldado por Irán (Tanios, 2015).

Previo a 2015 Israel consideró avanzar con una acción militar unilateral para poner un freno al avance nuclear de Irán (Steven, 2010). De hecho, de acuerdo a un artículo publicado en el diario Israelí Haaretz, se sospecha que Israel efectivamente llevó a cabo una amplia gama de acciones encubiertas durante años con el fin de frenar el progreso del programa (Green, 2018).

Sin embargo, sus líderes optaron por tomar una postura más pasiva, y dejar que sea EE.UU. junto con los cinco europeos quienes por medio del JCPoA obliguen a la República Islámica a limitar su programa nuclear.

A su vez, otros factores llevaron a que Israel deseche la idea de lanzar un ataque físico unilateral contra Irán. Las autoridades israelíes pronto observaron que por medio del desarrollo de capacidades cibernéticas, podían obtener el mismo resultado - la ralentización del programa nuclear - a un costo menor, con anonimato y sin la condena de la comunidad internacional.

Desde finales del siglo pasado, Israel considera a la ciberseguridad como un tema de alta política. De hecho, para el año 2010 el estado judío ya contaba con la red cibernética más importante de la región MENA, a la altura de las potencias cibernéticas de primer nivel - como EE.UU., Rusia y China - (Kausch, 2017).

Al igual que en el caso iraní, el año 2012 representó un antes y un después en la estructura de ciberseguridad israelí. Ese año se creó el Consejo Nacional de la Oficina Cibernética, y tres

[23] Entendemos por "guerras proxies" a aquellas conflagraciones donde se enfrentan grupos que actúan en la arena regional en favor de los intereses de otros Estados. Generalmente, este tipo de guerras tienen lugar en terceros países, y no en el territorio de los propios Estados que apoyan a uno y otro grupo (Deutsch, 1964).

años más tarde se estableció la Oficina Cibernética Nacional como órgano de coordinación de las actividades estatales en el ciberespacio.

Al mismo tiempo, el gobierno estableció un clúster de investigación de amenazas cibernéticas en la ciudad de Beersheba, que contempla una combinación de expertos cibernéticos del gobierno, del sector privado y de instituciones de investigación (Kausch, 2017).

Tal fue la relevancia que adquirió la ciberseguridad en este país, que la Unidad 8200 del ejército de Israel - responsable de las operaciones cibernéticas vinculadas a la labor militar-, es la unidad más grande de las Fuerza de Defensa de Israel (LatamIsrael, 2019). Netanyahu - quien ya desde entonces era el primer ministro israelí -, adoptó la ciberseguridad como una prioridad personal. En 2011, el primer ministro prometió públicamente convertir a Israel en una "potencia cibernética mundial"; y a principios de 2016, este Estado ya contaba con 300 empresas de ciberseguridad y el 20% de la inversión de los privados ligados al dominio cibernético del mundo (Kausch, 2017)

En el año 2015, una firma de seguridad cibernética israelí descubrió un ciberataque a gran escala codificado con un *malware* destinado a robar datos confidenciales. El mismo estuvo dirigido hacia cuerpos militares, empresas de telecomunicaciones, medios de comunicación y universidades israelíes.

La compañía en cuestión aseguró que el *proxy* iraní Hezbolá había estado detrás del ataque, marcando un cambio en el alcance de la batalla digital del Estado judío con sus adversarios regionales (Krausch, 2017). A medida que países como Irán e Israel se consolidan como poderes cibernéticos indiscutibles, otros estados de la región aspiran a al menos no quedar demasiado atrasados respecto a los primeros.

2.4 Interacciones cibernéticas en el Medio Oriente como reflejo de la competencia regional

El cuadro a continuación muestra las operaciones cibernéticas - conocidas públicamente - patrocinadas y recibidas por distintos Estados del Medio Oriente.

CUADRO 1: CIBER OPERACIONES SPONSOREADAS POR ESTADOS PÚBLICAMENTE CONOCIDAS EN EL MEDIO ORIENTE 2010 - 2017 (fuente: Council on Foreign Relations, "Cyber Operations Tracker.")

Publicly Known State-Sponsored Cyber Operations in the MENA 2010–2017[24]

Country	Sponsored Attack	Victim of Attack
Iran	19	18
Israel	5	11
Saudi Arabia	0	16
United Arab Emirates	1	6
Syria	0	8
Turkey	0	6
Qatar	0	4
Lebanon	0	4
Iraq	0	3
Bahrain	0	1
Jordan	0	4
Kuwait	0	3
Yemen	0	2
Morocco	0	2
Algeria	0	3
Tunisia	0	1
Egypt	0	4
Libya	0	2

Se puede vislumbrar que desde el año 2010 al 2017, la carrera armamentística cibernética es ante todo un asunto entre Irán, Israel y Arabia Saudita, dentro de los cuales este último tiene una clara desventaja - dado que recibió 16 ciberataques y no lanzó ninguno -. No obstante, si analizamos la tabla elaborada por Sexton y Campbell (2020), que estudia casos de 2010 a 2020, podemos observar un salto en la cantidad de ciberataques recibidos y perpetrados por estos países.

CUADRO 2: CIBER OPERACIONES SPONSOREADAS POR ESTADOS PÚBLICAMENTE CONOCIDAS EN EL MEDIO ORIENTE 2010 - 2020 (Sexton y Campbell (2020)

PUBLICLY KNOWN STATE-SPONSORED CYBER OPERATIONS IN MENA (2010-20)

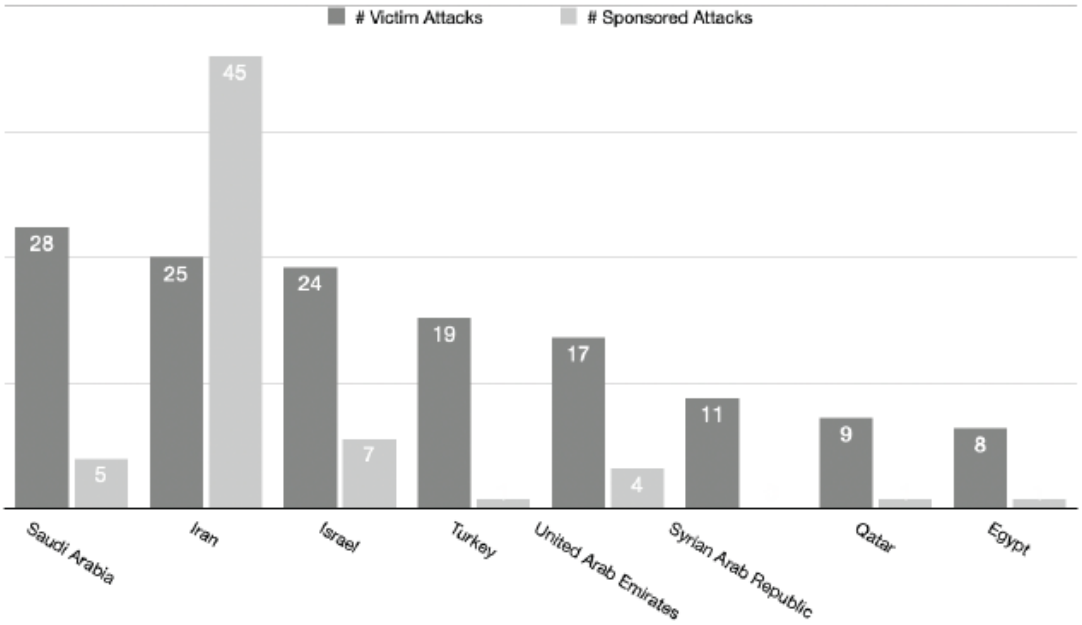


FIGURE 1.1 PLOTS THE EIGHT MENA COUNTRIES MOST FREQUENTLY VICTIMIZED BY CYBERATTACKS (DARK GRAY) AND THE FREQUENCY WITH WHICH THEY SPONSORED ATTACKS AGAINST OTHER STATES (LIGHT GRAY) FROM 2010-20. DATA: "CYBER OPERATIONS TRACKER," COUNCIL ON FOREIGN RELATIONS, 2020.

Si comparamos ambos cuadros, esto nos indica que hubo un aumento exponencial en el número de ciberataques entre 2017 y 2020. Sin embargo, vemos que los actores más involucrados continúan siendo los mismos: Irán, Arabia Saudita e Israel.

También se observa que Arabia Saudita ha sido el Estado que mayor número de ataques ha recibido en ese período; y si bien Irán ha sido víctima de un número similar de operaciones que Arabia Saudita e Israel, también ha sido el patrocinador la mayor cantidad de ciberataques que cualquier otro país del MENA.

Nuevamente, el concepto de ciberseguridad de Stevens (2018) resulta particularmente útil para leer esos datos; ya que comprende a la política de ciberseguridad como un conjunto de prácticas con objetivos defensivos y ofensivos, fuertemente interrelacionado con los objetivos de política exterior – y en este caso, regional -.

Se estima que, ya sea por medio de artillería física o cibernética, un aumento de las mismas en la región probablemente contribuiría a un mayor endurecimiento en los frentes disputados entre Irán y Arabia Saudita por un lado; e Israel por el otro (Kausch, 2017).

3. Aliados y ciber capacidades de la política de ciberseguridad iraní en la esfera internacional

3.1 Aliados gubernamentales

Como consecuecia del aislamiento internacional que sufre Irán desde el descubrimiento del programa nuclear y la aplicación de las sanciones, el Estado se vio imposibilitado de acceder al mercado financiero para obtener el capital necesario e invertir en tecnologías altamente sofisticadas. Ante tal escenario, Teherán recurrió a sus aliados más poderosos – Rusia y China, con quienes comparte una política exterior caracterizada como anti-EE.UU. (Daricili, 2019) - no sólo para conseguir asistencia financiera, sino también para proveerse de sistemas informáticos y aparatos de última tecnología.

Los frutos de este *partnership* se pueden ver por ejemplo en el software de filtrado inteligente de Internet adquirido por Teherán, que fue provisto por la empresa China Huawei Telecom Company (Daricili, 2019). Este sistema permite escanear la navegación de los usuarios e identificar ciertas palabras clave prohibidas, y negar automáticamente el acceso a un sitio particular (Kelly y Cook, 2011).

Para China, tender relaciones en materia de tecnología con Irán implica reforzar un frente de oposición a EE.UU. en este rubro (Sexton y Campbell, 2020). En el marco de la disputa global entre EE.UU. y China por el dominio en las cadenas de suministro de IT, la asociación con la República Islámica abre puertas al gigante asiático en el Medio Oriente. A su vez, si Irán logra aprovechar la experiencia y apoyo de China para convertirse en el máximo representante cibernético contra EE. UU., la dinámica del conflicto sino-estadounidense puede cambiar significativamente (Doffman, 2019).

Respecto de Rusia, se observa su continuo esfuerzo por albergar servidores de prueba para los ciberdelincuentes iraníes, los piratas informáticos respaldados por el Estado y los grupos *proxies*; dado que casi todas las direcciones IP iraníes están bloqueadas en EE. UU. y múltiples naciones europeas (Sexton y Campbell, 2020). Si bien la relación entre Rusia e Irán en torno a la cuestión cibernética no es tan sólido como entre el último y China; la cooperación con el Kremlin fue poco a poco incorporando esta temática en las conversaciones bilaterales.

En este sentido, en enero de 2021 el ministro de Relaciones Exteriores de Rusia, Sergey Lavrov; y su homólogo iraní, Javad Zarif, firmaron un acuerdo de cooperación en materia de ciberseguridad y tecnologías de la información y las comunicaciones (TIC). El acuerdo ampara

la transferencia de tecnología, la capacitación combinada y la coordinación en foros multilaterales, como las Naciones Unidas (Council Foreign Relations, 2021).

Aunque la cooperación con Moscú podría mejorar las capacidades cibernéticas ofensivas de Teherán, el acuerdo es mayormente defensivo, motivado por la confrontación compartida de los dos países hacia EE.UU. y la influencia estadounidense en el Medio Oriente (Council Foreign Relations, 2021).

3.2 Aliados no gubernamentales

Sumado a los aliados gubernamentales, para Irán también es una prioridad desarrollar capacidades cibernéticas de la mano de organizaciones *proxies,* construyendo un vínculo *win-win.* De acuerdo a Sexton y Campbell (2020), la República Islámica tiene un historial demostrado de inversión en recursos financieros y humanos en sus representantes cibernéticos, de los cuales los más importantes son Ciber Hezbollah, el Ejército Electrónico Sirio, Hamás y el Ejército Cibernético de Yemen.

La cúpula gubernamental persa encontró en esa cooperación una oportunidad para desarrollar un sistema de ciberataques evitando realizar grandes inversiones de cero, paliando así la falta de financiamiento internacional. Consecuentemente, Irán pretendió obtener una ventaja competitiva frente a Estados y grupos de la región a los que considera una amenaza, aumentando su eficacia en la lucha por el liderazgo regional y fortaleciendo la independencia del país (Sexton y Campbell, 2020).

Por su parte, los actores no estatales que operan en la región se ven beneficiados, dado que encuentran el camino más allanado para llevar a cabo actividades delictivas en el ciberespacio acorde a sus intereses de grupo, como el comercio digital de armas, la propagación de información falsa e ideologías extremas o ciberataques a blancos puntuales. Para los grupos fundamentalistas que buscan ejercer el control territorial e influencia en la región, las operaciones de información resultaban existenciales. Tal como afirman Sexton y Campbell (2020), si la descentralización de actos violentos es una técnica, el alto volumen de mensajes es un refuerzo clave para la validación de su sistema ideológico.

De modo esquemático, el vínculo cibernético entre la República Islámica y estos grupos *proxies* ha sido el siguiente: Irán dota a estas organizaciones mayormente de recursos financieros, tecnología y capacitación en su uso; a cambio de que éstas protejan a sus patrocinadores estatales de la culpabilidad de algunas de sus operaciones (Sexton y Campbell, 2020).

En 2015 - por ejemplo -, tuvo lugar un ataque conocido como “Cedro Volátil”, el cual tuvo como objetivo principal las Fuerzas de Defensa Israelí (FDI) y se cree que fue ejecutado por Hezbolá (Sexton y Campbell, 2020). La investigación realizada por la empresa de seguridad cibernética israelí Check Point Software Technologies Ltd evidencia que el ciberataque fue perpetrado desde el Líbano (Sexton y Campbell, 2020).

Los factores recopilados por esta fuente que dan cuenta de su origen son numerosos. Entre ellos, se destacan el hecho de que los servidores para la primera versión del virus se alojaron en una importante empresa de alojamiento libanesa; y que la información del registrante DNS de varios de los servidores de infraestructura muestra que estuvieron registrados previamente bajo contactos con una dirección libanesa muy similar (Sexton y Campbell, 2020).

Además, la dirección de correo electrónico vinculada al ciberataque conduce a cuentas de redes sociales que muestran una afinidad clara y pública hacia Hezbolá. En suma, dada la especificidad de los blancos - mayormente organizaciones estatales israelíes -, se plantea que el móvil del/los responsable/s está más vinculado a intereses políticos más que financieros. Cedro Volátil tenía el propósito de extraer información sensible de los objetivos que podían ser de gran utilidad para grupos afiliados al Líbano (Sexton y Campbell, 2020).

Por su parte, en abril de 2013 la cuenta de Twitter de la agencia de noticias Associated Press fue hackeada por el mencionado Ejército Electrónico Sirio, que afirmaba tener una capacidad de ataque cibernético activa con el apoyo de Irán y del gobierno de Bashar Al Asad (Daricili, 2019).

Según el *tweet* publicado por el Ejército Electrónico Sirio a través de esta cuenta de noticias, el entonces presidente Barak Obama había resultado herido como consecuencia de una explosión en la Casa Blanca. Previo a que el secretario de prensa confirmara en conferencia de prensa que se trataba de una *fake news* (Strum, 2013*)*, el Dow Jones[24] llegó a bajar unos 130 puntos, produciendo una reducción de $ 130 millones en la Bolsa de Valores de Nueva York (Daricili, 2019).

El Ejército Electrónico Sirio también atacó a otros medios de comunicación occidentales de enorme repercusión, como por ejemplo CBS, la BBC, The Washington Post y The Onion. En

[24] E*l Dow Jones Industrial Average* es el índice bursátil de referencia de la bolsa de valores de Nueva York. El mismo refleja la evolución de las 30 empresas industriales con mayor capitalización bursátil que cotizan en este mercado (El Economista.es)

estos casos, el motivo fue tomar represalias por lo que consideraban una cobertura unilateral de la guerra civil siria.

Finalmente, también mencionamos el vínculo entre el Ejército Cibernético de Yemen y el Ministerio de Inteligencia de Irán. En un marco de cooperación entre la parte yemení y la Fuerza Paramilitar Basij - encargada de garantizar el apoyo régimen dentro y fuera del país - tuvo lugar la operación que logró robar más de un millón de documentos del Ministerio de Relaciones Exteriores de Arabia Saudita.

El Ejército Cibernético de Yemen - entrenado y apoyado por el gobierno iraní - se infiltró por medio de ciberespionaje en los registros de la institución saudita y divulgó los documentos a través de Wikileaks (Kausch, 2017). De acuerdo a Kausch (2017), si el apoyo de Irán a organizaciones *proxies* para llevar a cabo operaciones militares en su nombre significó una contribución directa para el liderazgo iraní, en el ciberespacio esta ventaja se potencia.

Sin embargo, como argumenta Michael Sulmeyer, la confianza excesiva de Irán depositada sobre los *proxies*, puede conllevar una serie de riesgos: los intereses de estos grupos pueden diferir - o incluso entrar en conflicto con los del Estado patrocinador -; puede que los *proxies* tengan un incentivo menor que el sponsor para reclutar nuevos afiliados en sus filas; y a diferencia de la provisión de armamentos o explosivos, que requieren una constantemente la reposición de suministros, la transferencia de herramientas y recursos cibernéticos no precisa de un continuo abastecimiento sino que una vez adquiridos ya están bajo el poder de estos grupos. El último punto también genera una baja en la dependencia de las organizaciones hacia el patrocinador, dado que los dota de mayor independencia (Kausch, 2017).

4. Conclusiones parciales del Capítulo II

Como vimos a lo largo de este capítulo, la política de ciberseguridad iraní se posicionó en lo más alto de la agenda de seguridad y defensa con el devenir de la segunda década del siglo XXI. Esta evolución se dio en un contexto de fuerte rivalidad con EE.UU., Arabia Saudita e Israel, al calor de los avances tecnológicos y la complejización del ciberespacio.

Es así que en el plano internacional, Irán desarrolló una política de ciberseguridad respaldada por aliados gubernamentales - especialmente China y Rusia - y no gubernamentales - las organizaciones *proxies* desplegadas en la región -; y logró desarrollar las cibercapacidades

suficientes para convertirse en un referente en materia de ciberseguridad en el Medio Oriente -a la par de Israel -.

De esa forma, acortó las distancias respecto a rivales con un gran poder militar tradicional -como EE.UU. - aplicando una estrategia típica de guerra asimétrica. El desarrollo nuclear ya no es la única carta que tiene la República Islámica para disuadir a sus enemigos; sino que también demostró que mediante el lanzamiento de ciberataques por ejemplo, puede causar fuertes golpes en el mundo occidental a un muy bajo costo.

Es por esta razón que adherimos a la corriente realista propuesta por Manjikian (2010) para interpretar la relación entre el ciberespacio y los Estados. De acuerdo a la misma, la denominada "aldea global" que plantea la perspectiva utópica, se convierte en un espacio de batalla virtual donde se disputa el poder. Esto se observa en los registros de ciberataques lanzados mutuamente entre los Estados – demostrados en los cuadros expuestos anteriormente -, lo cual da cuenta que las rivalidades existentes en el plano físico, se trasladan al plano virtual.

En el próximo capítulo, analizaremos cuáles fueron los principales aspectos y estrategias de la política de ciberseguridad iraní en la dimensión doméstica e internacional que permitieron proteger la integridad del régimen y posicionar a Irán como potencia cibernética durante el periodo de estudio seleccionado.

Capítulo III

Tras haber desarrollado la política de ciberseguridad iraní en la dimensión doméstica e internacional, observamos que la misma se fue intensificando al calor de la evolución tecnológica y de los movimientos geopolíticos de la región. En ese sentido, notamos que el énfasis puesto en el despliegue de cibercapacidades ofensivas y defensivas, facilitó a la República Islámica - al menos durante el período que abarca esta tesina - el cumplimiento de los objetivos macro de la cúpula gubernamental: preservar la integridad del régimen y escalar hasta posicionarse como uno de las potencias cibernéticas del Medio Oriente.

Estas dos caras de la política de ciberseguridad iraní - una reactiva y otra proactiva -, son un reflejo de la noción de ciberseguridad propuesta por Stevens (2018), quien la entiende tanto en términos defensivos – esto es, como un mecanismo de protección ante posibles ciberataques librados por bandos enemigos -; como ofensivos - como una herramienta para ejecutar política nacional e internacional a través de Internet -.

Como explicamos con antelación, mientras que la política de ciberseguridad interna estuvo más comprometida con el primer objetivo, la estrategia cibernética aplicada a nivel internacional estuvo más bien vinculada con el segundo. La interrelación entre ambos objetivos residió en que para convertirse en un Estado poderoso a nivel regional, era imprescindible mantener una estructura interna fuerte que sea capaz de sobrevivir a los vaivenes propios de las luchas de poder.

La corriente realista del ciberespacio nos fue de gran utilidad para entender que este escenario de disputa es una extensión del plano físico, donde la competencia entre los Estados continúa. En este punto, el concepto de ciberpoder elaborado por Venables, Shaikh y Shuttleworth (2015) juega un rol clave; dado que se refiere a la capacidad de alterar el comportamiento de otros a través del ciberespacio. Observamos que Irán efectivamente logró tener un impacto en actores domésticos e internacionales en el quinto dominio; por medio de la ejecución de una política de ciberseguridad sólida y cada vez más sofisticada.

A continuación, daremos cuenta de cuáles fueron los resultados de esa política aplicada en ambas esferas, que desde nuestra óptica facilitaron el cumplimiento de los objetivos previamente mencionados.

1. **Preservación del régimen iraní: intervención en el ciberespacio e hipervigilancia**

Tal como mencionamos con antelación, el Movimiento Verde se caracterizó por ser pionero en la implementación de un nuevo paradigma comunicacional en el cual, gracias a Internet, cualquier persona de una sociedad puede ejercer "periodismo ciudadano". Internautas iraníes con lemas como “cada iraní, un medio” y “usted es los medios” transmitían un torrente de noticias, imágenes y videos a través de la *web* hacia Irán y el mundo entero (Golkar, 2011). Esta noción de “periodismo ciudadano” es un reflejo del rol preponderante que adquirió el individuo como un actor más de la comunidad internacional, un postulado troncal de la teoría de la interdependencia compleja. La tecnología dio lugar a que personas comunes y que a prima facie parecen aisladas, con acceso a Internet pueden influenciar a miles de pares y ejercer presión sobre las agendas públicas.

La relación entre tecnología y olas políticas es simple: las personas publican sugerencias o ideas en blogs, sitios *web* y/o redes sociales; luego éstas se discuten en las distintas plataformas; y finalmente los usuarios pueden trasladar estos planteos al mundo real, movilizando individuos en su favor y creando un efecto de onda de información (Golkar, 2011).

En otras palabras, Internet facilita y acelera la creación de olas, permitiendo a los usuarios sugerir nuevos mecanismos para ampliar las protestas y recopilar comentarios. Este avance, implicó un paulatino resquebrajamiento del monopolio de información y comunicación que mantenía el gobierno hasta ese entonces. Se trata de un terreno que rápidamente intentó recuperar, al considerar este asunto de vital importancia para garantizar la estabilidad del régimen.

Estos temores a la democratización de la información no eran infundados. La difusión de imágenes y videos que mostraban la violenta represión ejercida por el gobierno en los distintos levantamientos que tuvieron lugar en entre 2009 y 2021, coadyuvaron a una deslegitimación del régimen y a severas críticas tanto internas como de la comunidad internacional.

Luego de aplicar una estrategia más tradicional para aplacar las revueltas, identificamos que el gobierno optó por intervenir los blogs y las redes sociales – en múltiples ocasiones llegando a prohibir el acceso a las mismas - para poner un freno al nuevo paradigma comunicacional.

Estas cuestiones, provocaron que Irán se posicione como uno de los países con menor libertad en la *web* a nivel global. De acuerdo a un estudio llevado a cabo por Reporteros Sin Fronteras (RSF) en marzo de 2013, la República Islámica se encontraba dentro del top 5 de lo que la

organización denomina como “Enemigos Estatales de Internet”, acompañado de Siria, China, Bahréin y Vietnam (Reporteros Sin Fronteras, 2013). En los términos de RSF, esto implica que los gobiernos están altamente involucrados en una “vigilancia activa e intrusiva" de los proveedores de noticias, lo que resulta en graves violaciones de la libertad de información y los derechos humanos y la libertad” (Reporteros Sin Fronteras, 2013).

El reporte *Freedom on the Net* (libertad en Internet) elaborado por Kelly y Cook para *Freedom House* en el año 2011, ha denominado a Irán como el Estado “menos libre” en términos de libertad en la *web* (Kelly y Cook, 2011). Esta investigación evalúa una gama más amplia de sistemas políticos, revisando leyes y prácticas relevantes relacionadas a Internet, comprobando la accesibilidad de sitios *web* y entrevistando a una diversa variedad de fuentes.

Aunque los hallazgos del estudio indican que las amenazas a la libertad en Internet han ido creciendo y se han vuelto más diversas (incluso en sistemas democráticos como Brasil, India, Indonesia, Corea del Sur, Turquía y el Reino Unido); también se observa una ampliación de los mecanismos que han encontrado los ciudadanos para eludir algunas de las restricciones gubernamentales[25] (Parsa, 2008).

La investigación también resalta que en muchos casos los escenarios previos a las elecciones resultan propicios para poner en marcha o robustecer los controles de la *web*. A su vez, los autores dan cuenta de que las autoridades de aquellos países que ya habían mostrado cierta tendencia hacia la censura política en Internet aceleraron dramáticamente esta tendencia luego de 2010 y crearon nuevas instituciones específicamente con este fin (Kelly y Cook, 2011). Ambas tesis se cumplen en el caso iraní.

Tal como lo afirma Roozbeh (2018), el ciberespacio le brindó a los gobiernos en general excelentes oportunidades para vigilar a la sociedad, dándole acceso a una mayor calidad y cantidad de información personal. Desde el punto de vista gubernamental, permitir el derecho a la libertad de expresión y a la organización atentaba directamente contra la integridad del régimen y contra la seguridad nacional; y por lo tanto debían tomarse acciones con efecto inmediato. Esa perspectiva del gobierno se vio reflejada también en el accionar que tomó el

[25] Parsa (2008) observa que gracias a la expansión de las redes sociales y al aumento exponencial del tránsito de noticias e interacción en el ciberespacio, los iraníes han desarrollado un fenómeno denominado *weblogistán*, donde las noticias y opiniones se extienden con mayor rapidez de lo que intenta suprimir la censura. El activismo *on-line* ha buscado estrategias para evitar la represión ocultando identidades, usando VPNs o utilizando una retórica en la que se expresan opiniones evitando utilizar puntualmente las palabras que pueden caer en el filtrado del gobierno.

tejido institucional vinculado a la ciberseguridad en las movilizaciones de 2019; cuando en los momentos más álgidos de la represión a los manifestantes, se bloqueó directamente la red, inhabilitando cualquier tipo de conexión dentro y fuera de Irán (Humans Right Watch, 2019).

De esa forma, Irán se convirtió en uno de los países con menor libertad de prensa a nivel mundial – a la par de países como China y Corea del Norte (RSF, 2018) -. Tal como lo explica Golkar (2011), así como los jóvenes iraníes usan Internet para librar una guerra psicológica contra el régimen, éste utiliza la *web* para provocar desunión entre los opositores, inducir miedo en la sociedad y crear autocensura entre los usuarios.

A modo de ejemplo, la rama cibernética de la IRGC envía regularmente correos electrónicos a los usuarios advirtiendo que están siendo observados para desincentivar cualquier manifestación en contra del gobierno (Golkar, 2011).

Otro de los mecanismos empleados para sembrar temor en la población es publicar fotos de opositores y activistas en sitios *web* gubernamentales y ofreciendo recompensas para identificarlos y rastrearlos (West, 2010). El objetivo de este accionar es, sin lugar a dudas, despolitizar a los manifestantes.

Cabe mencionar que esto no hubiera sido posible sin la coordinación entre las diferentes agencias gubernamentales. El tejido institucional ligado al ciberespacio que se construyó a partir de 2009 fue complejo. Se trata de un sistema en constante evolución donde cada parte tiene competencias específicas y al mismo tiempo se interrelaciona con las demás.

La creación del Comando de Defensa del Ciberespacio fue de las medidas más relevantes tomadas por el gobierno de Ahmadineyad para controlar Internet y garantizar la seguridad del régimen (Karimi, 2009). Este estableció un departamento especial conocido como el Centro de Inspección de Delitos Organizados (CIDO) para supervisar e investigar el crimen organizado, el terrorismo, el espionaje y los delitos económicos en el espacio virtual (Golkar, 2011). El CIDO utiliza métodos extensivos para identificar a los usuarios de Internet. La identificación de los usuarios a través de su dirección IP fue el más utilizado en protestas recientes.

El funcionamiento de este método implica una compleja coordinación entre agencias gubernamentales. Todos los *weblogs* iraníes como por ejemplo Persianblog, Blogsky, Blogfa, Mihanblog y Parsiblog tienen que registrar la datos del usuario - especialmente su dirección IP

y tipo de conexión -, brindando así fácilmente información sensible a los organismos de inteligencia.

Además, al enviar mensajes de correo electrónico con virus principalmente a través de anuncios, el CIDO puede infectar miles de computadoras a la vez, y robar datos de una manera más disimulada (Mohseni, 2010). La distribución de software anti-filtro es otro medio empleado por el CIDO para espiar a los activistas. Debido a que la gran mayoría de las plataformas cibernéticas en Irán cuentan con el sistema de filtrado inteligente - el cual desarrollamos en el capítulo I -; los usuarios adquirieron el hábito de utilizar aplicaciones anti-filtro para acceder a muchos sitios.

Hábilmente, los ciberguardias aprovechan esta necesidad diseñando sus propios programas de anti-filtro, y los inmiscuyen con las demás aplicaciones de este tipo. De esta forma, al instalar y hacer uso de los anti-filtros creados por las agencias estatales, los usuarios terminan paradójicamente facilitando el ciberespionaje y el acceso a información sensible por parte del gobierno.

Con un metodología similar, en 2009 agentes de seguridad cibernética habían secuestrado algunos sitios *web* y redes sociales - como *Twitter* - y redirigía a los usuarios a otras páginas para identificarlos (Arrington, 2011). Estos agentes también han diseñado algunos sitios *web* y *weblogs* con nombres y diseños similares a los que critican al gobierno. De esta manera, pueden propagar *fake news* en favor del gobierno e insertar propaganda oficialista.

La hipervigilancia de los organismos estatales también está respaldada por grandes empresas que brindan servicios de Internet que permiten obtener datos de los usuarios y contraseñas de las cuentas. Por ejemplo, si bien Yahoo negó haber provisto información personal de más de 200.000 activistas iraníes al régimen. No obstante, informes que revelan que la compañía brindó datos sensibles sobre opositores al gobierno chino y a otros países alienta tales especulaciones (Golkar, 2011).

La otra institución cibernética que tuvo un rol preponderante en la protección del régimen, fue la Fuerza Paramilitar Basij. Esta se ocupa de diseñar y poner en práctica estrategias que busquen garantizar el apoyo de la población al *establishment* político, mediante la publicación de contenido a favor del gobierno en blogs y redes sociales (BBC Persian, 2018).

Si bien hasta el 2023 este ente no ha sido registrado oficialmente en ninguna agencia gubernamental, la evidencia indica que esta institución también está fuertemente relacionada con la IRGC (BBC Persian, 2018). Con más de cuatro millones de miembros, el Basij es una de las milicias más grandes del mundo. Se ha utilizado para reprimir a los oponentes y disidentes en Irán durante más de dos décadas.

Se tomaron medidas como la implementación de cibercafés y la creación de 10.000 *web*logs cuyos contenidos los monitoreaban los miembros del Basij y deben confrontar la invasión cultural y promover contenido islámico (Rafiehzadeh, 2008). Ambos planes apuntan no sólo a la difusión de propaganda, sino también a desmoralizar a activistas políticos y críticos del régimen dentro y fuera de Irán (Golkar, 2011).

Cabe mencionar que la labor en conjunto de estas instituciones no sólo cometieron el objetivo de actuar como un fuerte del régimen, sino que también se convirtieron en alarmas para otros países del mundo. El hecho de que Irán, un país que se encuentra enfrentado a un importante número de actores del sistema internacional, destine sumas exorbitantes a la construcción de un entramado institucional cibernético como este no es un dato menor.

Evidentemente, da cuenta de que el ciberespacio es cada vez más un dominio que puede tener severas consecuencias en el plano real si no es tomado con cautela. Desde el punto de vista del régimen chiita, la relación entre libertad y estabilidad es inversamente proporcional: a mayor libertad en la *web*, menor estabilidad del *establishment*. Y es aquí donde estas agencias, las instrumentadoras de la política de ciberseguridad persa, tuvieron, tienen y tendrán un rol preponderante.

En síntesis, podemos afirmar que el régimen chiita tuvo éxito a la hora de contener las amenazas al régimen y resistir la volatilidad propia de la era digital. Si bien es cierto que perdió el monopolio absoluto de la información y de los medios de comunicación; también es cierto que logró mantener la estabilidad del gobierno en momentos de gran turbulencia política y social - como por ejemplo durante la Primavera Arabe, los levantamientos de 2009, 2017/18 y 2019, y la pandemia.

Arribamos a la conclusión de que las organizaciones más relevantes en lo que respecta a la protección del régimen son la IRGC – dentro de esta, fundamentalmente el Basij – y el Comando de Defensa del Ciberespacio.

Esto se debe a que son instituciones cuyas tareas se resumen en: por un lado, difundir propaganda a favor del régimen, intentando así aumentar el apoyo de la opinión pública. Por otro lado, buscar reducir la injerencia de ideas occidentales por medio del bloqueo o del lanzamiento de ciberataques.

Observamos que la política de ciberseguridad aplicada en el ámbito doméstico tuvo fundamentalmente dos resultados: una clara pérdida de libertad en la *web* para los ciudadanos; y la construcción de un Estado hipervigilante que operó por medio del entramado institucional vinculado al ciberespacio.

2. Posicionamiento como potencia cibernética regional: guerra asimétrica e incremento de las cibercapacidades

Siguiendo a Wajsman (2022), *Stuxnet* no solo fue la primera ciber arma de la historia, sino que marcó un antes y un después en la historia de la guerra. Son muchos los autores que afirman que la ciberguerra es la nueva forma de guerra del siglo XXI.

Esto no significa que la conflagración convencional vaya a desaparecer, sino que implica un nuevo estilo - más barato y menos sangriento - que puede combinarse y/o transformarse en guerra física (Wajsman, 2022). En este marco, podemos decir que la información se está convirtiendo en el recurso más valioso en los enfrentamientos (Vertuli y Loudon, 2018).

Además de los ciberataques directos que un actor pueda lanzar - donde un solo cibersoldado puede por ejemplo apagar una ciudad entera, dejarla sin transporte o golpear el sector financiero de un país -; existen otras metodologías más *soft* que también pueden tener grandes repercusiones en las luchas de poder.

Poseyendo la infraestructura, el *know how* y los recursos humanos pertinentes, las operaciones de información pueden influir en las percepciones de una sociedad (Stel, 2005). Este tipo de enfrentamiento pretendía generar un alto impacto psicológico, que obstaculice la iniciativa, libertad de acción y los deseos del enemigo (Bartolomé, 2006). Con el ciberespacio como epicentro de las confrontación, Teherán instrumentalizó las capacidades cibernéticas con fines políticos y se aferró a las ventajas que proporciona la guerra asimétrica en el quinto dominio.

Desde la revolución iraní de 1979 que puso fin al gobierno del Sha Reza Pahlevi e instauró una teocracia en su lugar, la política exterior regional de la República Islámica estuvo orientada a exportar la revolución. Caracterizada por una política de alto perfil, el nuevo régimen intentó

primeramente sumar a sus filas a los Estados con los cuales tiene mayor afinidad religiosa - Irak, Siria y el Líbano –; para luego aspirar a convertirse en una potencia regional. Pese a que los gobiernos de turno han ido variando con el correr del tiempo, estos aspectos de la política internacional persa se mantuvieron constantes.

Inevitablemente esas ambiciones, sumadas a las diferencias de fondo existentes, generaron - y generan - rispideces con Arabia Saudita, Israel y EE.UU. (con el cual hasta 1979 mantenía una relación más que cordial). Si bien, como desarrollamos en el capítulo anterior, con Arabia Saudita prevalece una rivalidad tal que derivó en el desencadenamiento de enfrentamientos por medio de actores *proxies* en otros países de la región – como Irak, Siria, Yemen y Líbano -; lo cierto es que en materia de ciberseguridad la competencia es más feroz con Israel.

Con estos lineamientos en claro, Irán desarrolló una política de seguridad cibernética ajustada a cada uno de estos tres actores. En este sentido, observamos que la estrategia de ciberseguridad aplicada hacia Washington fue la de utilizar al ciberespacio para poner un freno a las influencias del mundo occidental - del cual EE.UU es referente -.

Como ya desarrollamos, desde el punto de vista de Teherán, EE.UU es un hereje con quien se enfrenta desde la perspectiva ideológica y política; y sus intereses son irreconciliables. Si bien materialmente EE.UU supera con crecer a Irán, las cibercapacidades permiten a la República Islámica acortar distancias y contener el accionar de este actor.

Con Arabia Saudita, la política de ciberseguridad se resume en dos frentes: por un lado, se hace uso de los recursos cibernéticos para atacar directamente infraestructuras vitales para la economía nacional - lo cual se vio reflejado en los numerosos ciberataques a Aramco -. Al mismo tiempo, capacita y brinda recursos cibernéticos a grupos afines para potenciar sus ventajas y vencer a Riad en las distintas guerras *proxies*, buscando reducir su poder en la zona.

Israel por su parte, es su mayor competidor en este rubro. De hecho, existen sólidos argumentos para considerar al Estado judío como el país más desarrolado en la Medio Oriente en lo que respecta a cibserguridad[26]. Desde hace al menos una década, Irán desafía a Israel en el terreno cibernético - como vimos en la cantidad de ciberataques lanzados entre estos actores en el

[26] Por ejemplo la Unidad 8200 del ejército de Israel - responsable de las operaciones cibernéticas vinculadas a la esfera militar-, es la unidad más grande de las Fuerza de Defensa de Israel (LatamIsrael, 2019).

capítulo anterior -. Con este Estado, el foco está puesto en utilizar las cibercapacidades como una herramienta disuasiva, a los fines de paliar el retraso en el programa nuclear.

No obstante, para alcanzar estos fines Irán también se benefició del apoyo brindado por dos estados que con quienes comparte algunos principios de su política internacional: China y Rusia. Con el primero ha forjado una relación fuerte en lo que hace al traspaso de tecnología. El *software* chino - experimentado muchas veces en la misma población del gigante asiático - ha permitido a Irán ejercer una hipervigilancia sobre la población, e incorporar sistemas como el filtrado inteligente (Daricili, 2019).

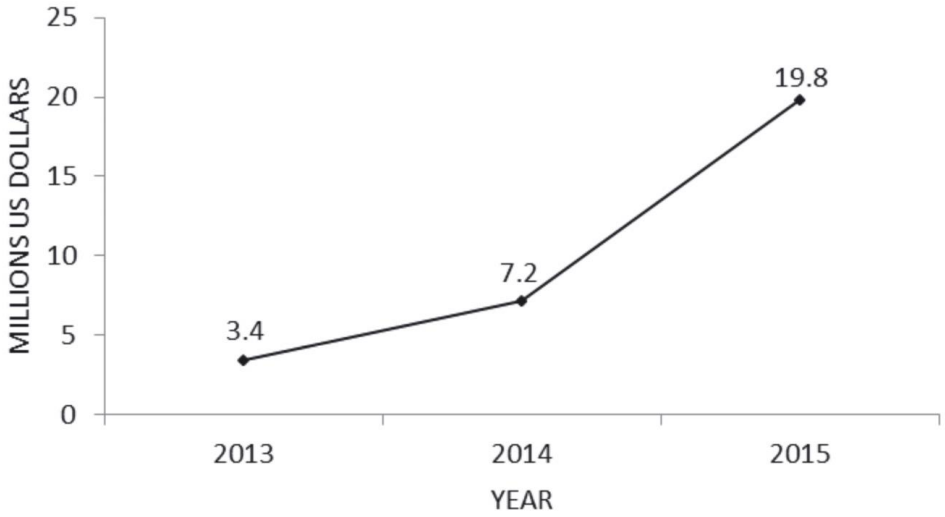
Con Rusia, el vínculo no ha madurado tanto en esta materia, pero sí tenemos indicios de que esa sea la meta. Como se hizo alusión en el capítulo II, la cooperación con el Kremlin fue poco a poco incorporando la seguridad cibernética en las conversaciones bilaterales.

Por ejemplo, a inicios de 2021 Moscú y Teherán firmaron un acuerdo de cooperación en materia de ciberseguridad y tecnologías de la información y las comunicaciones (TIC).El mismo alude a la transferencia de tecnología, la capacitación combinada y la coordinación en foros multilaterales, como las Naciones Unidas (Council Foreign Relations, 2021).

Ambos actores se constituyeron como sostenes del régimen, colaborando no sólo en la perpetuidad del mismo, sino también apostando a su liderazgo regional. El asunto es que los otros países con mayor poder e influencia en el MENA, son principalmente Arabia Saudita e Israel - históricos aliados de EE.UU -. El ciberespacio se convirtió en un espacio más donde tiene lugar el balance de poder, y donde los Estados compiten - y competirán - por ganar terreno.

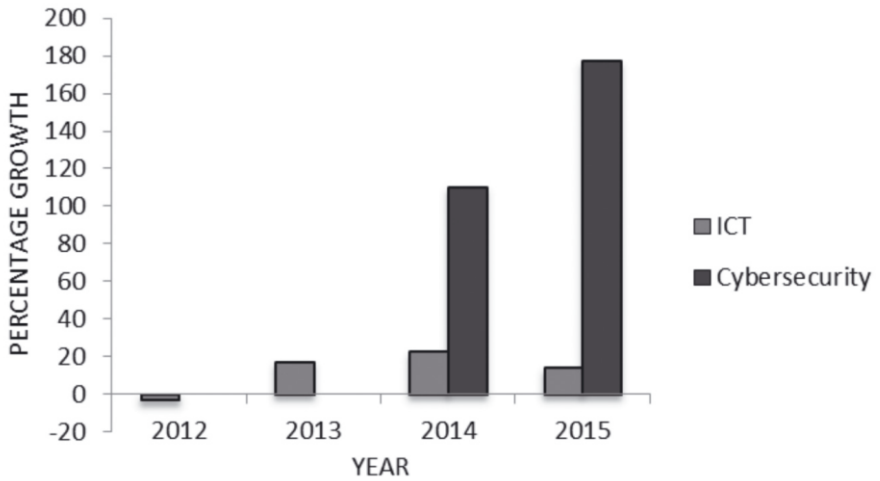
Tal fue la importancia que adquirió la ciberseguridad para Irán, que desde la llegada al poder de Rouhani en agosto de 2013, se observa que el gasto destinado en ciberseguridad ha incrementado notablemente. En el cuadro a continuación (3), elaborado por Small Media (2015), se vislumbra una curva en alza representativa de este aumento en la inversión cibernética.

CUADRO 3: PRESUPUESTO DE SEGURIDAD CIBERNÉTICA DE IRÁN, 2013-2015 (SMALL MEDIA, 2015)



Vemos que en tan sólo dos años, el gasto aumenta un 582%, pasando de $3,4 millones en 2013 a $19,8 millones en 2015 (Small Media, 2015). Para contextualizar este crecimiento, el cuadro 4 compara el presupuesto anual de seguridad cibernética contra el presupuesto destinado a IT en general.

CUADRO 4: CRECIMIENTO ANUAL EN LOS PRESUPUESTOS DE SEGURIDAD CIBERNÉTICA Y TIC DE IRÁN, 2012-2015 (fuente: Pequeños Medios, 2015)



Del cuadro anterior, analizamos que, si bien el gasto en IT de Irán también se vio incrementado desde el año 2013, en el año 2014 y más aún en 2015 el mismo se vio altamente superado por el presupuesto de ciberseguridad puntualmente. Esto da cuenta de los grandes esfuerzos por parte de la República Islámica para mejorar específicamente su capacidades cibernéticas.

Dentro de este gasto en cibercapacidades, también se contempla el monto destinado a las capacitaciones de los recursos humanos (Craig y Valeriano, 2016). En este sentido, para el año 2016 la Guardia Revolucionaria Iraní había capacitado a un ejército cibernético de 120,000 personas, conformado principalmente por profesores universitarios, estudiantes y clérigos (Craig y Valeriano, 2016).

Otras de las herramientas contempladas dentro de las cibercapacidades es el ciberespionaje. De acuerdo a Sexton y Campbell (2020), muchas veces previo a un accionar mayor y más concreto, los Estados destinan grandes recursos al ciberespionaje, para estudiar los blancos y determinar qué tipo de operación es la más idónea. En otras palabras, el ciberespionaje a menudo sienta las bases para futuros ataques cibernéticos.

Un ejemplo donde se grafica la utilización del ciberespionaje como un recurso esencial para planificar futuras acciones fue el ataque a las instituciones financieras estadounidenses en septiembre de 2012. De acuerdo a un informe emitido en EE.UU., varias instituciones financieras norteamericanas fueron atacadas al mismo tiempo - entre las que se encontraban Bank of America, Morgan Chase, y Citigroup - (Siboni y Kronenfeld, 2012); lo que da cuenta de una ardua labor de ciberespionaje previa.

Las evaluaciones de este informe concluyeron que los ataques cibernéticos contra estas organizaciones no se originaron por hackers informáticos al azar movilizados - únicamente - por intereses económicos; sino que fueron financiados por Irán y llevados a cabo como represalia a las sanciones impuestas por EE. UU a este país (Siboni y Kronenfeld, 2012).

No obstante, cabe aclarar que este foco puesto en el desarrollo de cibercapacidades, no implicó que el gasto en defensa convencional se viera reducido. De hecho, se estima que incluso para el año 2021 – en contexto de pandemia -, el mismo aumentó 12.488,6 millones (Datosmacro.com, 2022). Esta cifra supone que el gasto público en defensa en 2021 alcanzó el 2,3% del PIB, una subida 0,14 puntos respecto a 2020 (Datosmacro.com, 2022). En suma, comparativamente, observamos que desde 2009 a 2021 – es decir, durante nuestro período de estudio – el presupuesto destinado a defensa aumentó en más de un 200%, como lo indica el cuadro a continuación confeccionado por Datosmacro.com (2022):

Irán - Gasto Público Defensa				
Fecha	Gasto Defensa (M.€)	Gasto Defensa (%Gto Pub)	Gasto Defensa (%PIB)	Gasto Defensa Per Capita
2021	30.885,3	12,96%	2,30%	364 €
2020	18.396,7	13,00%	2,16%	219 €
2019	12.223,8	13,92%	2,10%	147 €
2018	10.731,9	13,92%	2,46%	131 €
2017	13.386,3	16,05%	3,11%	165 €
2016	12.305,0	15,41%	2,97%	154 €
2015	10.156,6	15,55%	2,76%	129 €
2014	7.910,2	14,80%	2,28%	101 €
2013	7.238,6	15,61%	2,24%	94 €
2012	9.047,5	19,32%	2,76%	119 €
2011	10.703,0	13,01%	2,38%	142 €
2010	10.876,9	15,97%	2,79%	147 €
2009	9.633,7	15,69%	3,05%	132 €

Lo que sí es cierto, es que las cibercapacidades permitieron achicar la brecha con actores materialmente más poderosos. Es decir, posibilitaron lo que muchos autores denominan como "guerra asimétrica", donde actores con menor poder convencional pueden hacer frente e incluso superar a rivales con mayor recursos materiales. Y es allí precisamente donde Irán encuentra sus mayores ventajas.

Podemos operacionalizar el concepto de Rodríguez Peña (2001) de ***guerra asimétrica,*** dividiéndolo en dos: son procedimientos no convencionales que buscan reducir las capacidades militares del enemigo; y al mismo tiempo aprovechar sus vulnerabilidades mediante tecnologías o medios inéditos" (p. 61). En términos prácticos, con el programa nuclear ralentizado, la República Islámica apostó a desarrollar y ejecutar ciberataques - es decir, procedimientos no convencionales -, para acortar la brecha militar con sus rivales; aprovechando el hecho de gran parte de las infraestructuras de los mismos se sostienen a partir del ciberespacio - esto es, identificando la debilidad que les genera la gran dependencia de las tecnología digitales -.

A modo de ejemplo, aunque desde la óptica militar la República Islámica es convencionalmente menos poderosa que EE.UU., esto no implica que el primero sea necesariamente más débil. Es aquí donde el quinto dominio juega un papel esencial. (Daricili, 2019).

Irán ve la guerra en el ciberespacio de manera similar que las tácticas asimétricas empleadas por grupos terroristas, dado que se convierte en una ecualizador eficaz para infligir un daño significativo en el frente interno de un enemigo con superioridad militar y/o geoestratégica (Daricili, 2019). Es por esa razón que expertos estiman que en caso de una escalada en la confrontación entre Irán y Occidente por el programa nuclear iraní, la República Islámica intentaría lanzar un ataque cibernético contra las principales infraestructuras - como centrales eléctricas, instituciones financieras y sistemas de transporte - en suelo estadounidense (Siboni y Kronenfeld, 2012), lo cual la historia reciente ha comprobado.

Irán ha sido muy consciente de los efectos dañinos que pueden tener los ataques directos contra objetivos norteamericanos en la economía global; y entiende que una respuesta titubeante y amortiguada de EE.UU. dotaría a Teherán de tiempo y margen de maniobra para disuadir efectivamente a Washington y sus aliados (Kausch, 2017).

Para Teherán, los ataques cibernéticos acompañan perfectamente su ambición regional expansiva. La guerra tradicional en territorios como el sirio y el yemení suponen por su propia naturaleza un gran costo financiero y humano; y los réditos lejos están de ser garantizados (Kausch, 2017).

Además, como se adelantó en la introducción de este trabajo, el hecho de que gran parte de la infraestructura crítica de Irán todavía esté controlada por sistemas de control mecánico, supone una ventaja en términos de ciberdefensa. Esto, sumado a lo anterior, proporciona una disminución de los riesgos a los que se enfrenta Irán en caso de una represalia en el quinto dominio como respuesta a ciberataques lanzados por este Estado.

3. Conclusiones parciales del capítulo III

El advenimiento del ciberespacio vino a alterar para siempre la forma en la cual los individuos interactúan y se involucran con los asuntos políticos. El vínculo tecnología-política supuso nuevos desafíos para los gobiernos - especialmente para aquellos cuya volición de controlar a la población es mayor -. Con este propósito en mente, los resultados de la política de ciberseguridad en la dimensión doméstica pueden resumirse en un incremento de la intervención gubernamental en el ciberespacio y en la construcción de un Estado hipervigilante.

A nivel internacional, observamos que la política de ciberseguridad implicó una instrumentalización de las capacidades cibernéticas - defensivas y ofensivas -; y el empleo de

una táctica de guerra asimétrica. Esto lo vemos reflejado en la escalada de ciberataques entre Teherán y sus rivales; y en las estrategias escogidas para competir con EE.UU, Arabia Saudita e Israel. Es por ello que sostenemos que, tal como lo plantea John Sheldon - director ejecutivo del Instituto George C. Marshall. -: "el ciberespacio mapea los contornos de geopolítica contemporánea más de lo que podríamos pensar" (Sexton y Campbell, 2020, p. 8).

Entendiendo al ciberespacio como un ecualizador en los términos de Venables, Shaikh y Shuttleworth (2015), Irán supo aprovechar esta condición del quinto espacio, al haber logrado competir con rivales más poderosos en términos relativos y materiales mediante el desarrollo de sus propias armas cibernéticas; y posicionar a la República Islámica como una potencia cibernética regional en los términos de Bebber (2017). Según este autor, para ser considerado como tal, era necesario no sólo poseer los recursos cibernéticos, sino también saber emplearlos y ejercer poder a través de los mismos. Sin lugar a dudas, Irán logró tener un impacto considerable en los Estados de la región - como se observa en el incremento de las interacciones cibernéticas con estos países -; al punto tal de que muchos lo consideran como una amenaza a su seguridad. Esto derivó en que los vecinos colocaran también el tema de la ciberseguridad en agenda, entendiendo que un ciberataque a sus infraestructuras - económicas, de salud, educativas, etcétera -puede tener costos excesivamente altos.

En el siguiente apartado, procederemos a esbozar las conclusiones arribadas en base a los objetivos propuestos.

Conclusión

La evolución tecnológica y la interconexión alcanzada en la última década, moldearon un contexto internacional donde tanto la oportunidades como las amenazas se vieron multiplicadas. Por un lado, la tecnología permitió que los procesos sean efectivos y rápidos, generalmente a un menor costo y con un margen de error más reducido. Por el otro, trajo aparejado un conjunto de amenazas nuevas para las que en muchos casos existen lagunas legales y grises respecto a las regulaciones.

En este - relativamente - nuevo contexto, las agendas estatales intentaron poco a poco maximizar la protección ante los ataques ocurridos en el ciberespacio, a sabiendas de que un golpe en este dominio podría tener severas repercusiones en el plano físico, y en el sistema político, económico y social.

A raíz de lo mencionado, en este trabajo nos propusimos como objetivo general analizar la política de ciberseguridad iraní en su dimensión doméstica e internacional, en el período que va de 2009 a 2021; y los resultados de la misma. Para ello, realizamos una investigación de tipo cualitativa, y empleamos un marco teórico-conceptual amplio que nos permitió abordar nuestro objeto de estudio desde distintas perspectivas.

A los fines de mantener un orden metodológico, desglosamos el objetivo general en tres objetivos específicos, y dedicamos un capítulo a cada uno de ellos. De esa forma, luego de haber esbozado las nociones preliminares, desarrollamos el primer capítulo del trabajo, en el cual examinamos los principales objetivos, *targets* y herramientas de la política de ciberseguridad iraní a nivel doméstico.

Observamos que la misma ha ido evolucionando con mayor ímpetu desde 2009, adaptándose con rapidez a los nuevos contextos. A modo gráfico, podemos decir que la estrategia gubernamental en el ciberespacio fue tomando una forma de espiral, abarcando cada vez más aristas e incluyendo recursos de última generación. Esta adaptación constante al nuevo paradigma, se convirtió en un requisito vital para la propia integridad del gobierno. Para comprender la importancia de esto, nos resultó sumamente útil el aporte de Venables, Shaikh y Shuttleworth (2015), quienes categorizan al ciberespacio como un ***ecualizador***. El régimen comprendió que la red permite que actores con mayor o menor poder relativo puedan competir en términos relativamente iguales, movilizarse, lanzar campañas propagandísticas, opinar con mayor libertad, entre otros.

Teniendo como hitos las revueltas de finales de 2017 e inicios de 2018, los levantamientos de 2019, y la pandemia de COVID-19; notamos que la política de seguridad cibernética fue evolucionando hacia una estrategia cada vez más asertiva y más rigurosa, dirigida - entre otras cuestiones - a proteger la integridad del régimen iraní. Debido a la capacidad de acción que tienen en el ciberespacio, los principales apuntados por el gobierno fueron blancos son minorías religiosas y étnicas; opositores al gobierno; e *influencers*. En otras palabras, el régimen persa realizó grandes esfuerzos para evitar lo que Siboni y Kronenfeld (2012) denominan como *soft revolution*, una revolución pacífica por medio de las redes sociales, que puede estar fomentada por la injerencia de información de occidente.

El tejido institucional vinculado a la ciberseguridad también se fue complejizando al compás del cambio de era. Durante las manifestaciones posteriores a las elecciones de 2009 y luego del advenimiento de la Primavera Árabe, el foco de esta política estuvo puesto en el control y la restricción de las redes sociales - luego de notar que la censura a los medios tradicionales no era suficiente -.

Con las protestas de 2017/2018, la plataforma que se destacó fue *Telegram*, no sólo a la hora de difundir, sino también como un medio para organizar las manifestaciones en diferentes ciudades. En el año 2019 se decidió directamente bloquear el acceso a internet durante los horarios picos de la represión en las calles. En esta oportunidad, la corriente realista del ciberespacio propuesta por Paredes Roibas (2018) fue muy enriquecedora; ya que nos permitió entender estos casos como ejemplos en los cuales los Estados - en este caso Irán – son capaces de ejercer su soberanía en el plano físico del ciberespacio – esto es, en la infraestructura y las computadoras que se encuentren bajo su jurisdicción -; y de tomar medidas que pongan frenos al supuesto libertinaje de la red.

Por su parte la pandemia de COVID-19 - y la aceleración digital que se trajo consigo - supuso enormes desafíos para el gobierno iraní. Esto se debió a que a la vez que la estrategia de ciberseguridad se afinaba, fueron apareciendo nuevas tecnologías y actores en el ciberespacio con capacidades cibernéticas que dificultaban el control en el mismo.

A posteriori, dedicamos el segundo apartado de este trabajo a estudiar la política de ciberseguridad de la República Islámica en el plano internacional; en el marco de la rivalidad con Estados Unidos, Arabia Saudita e Israel. Luego del ciberataque de *Stuxnet* en el año 2010, la política de ciberseguridad persa escaló aún más en la agenda de seguridad y defensa nacional - y perduró como un tema de alta política hasta el momento de escribir esta tesina -. Fue así

que en el plano internacional, Irán se apoyó en aliados gubernamentales - principalmente China y Rusia - y no gubernamentales - como el Ejército Cibernético Yemení, el Ejército Electrónico Sirio y Hezbolá - para el intercambio y desarrollo de ciber capacidades. Esa red de aliados, junto con inversiones de altísimas sumas en ciberseguridad, permitieron que Irán se convierta en un potencia cibernética regional - a la par de Israel -; .

Para poder catalogar a la República Islámica como tal, nos basamos en la definición de potencia cibernética desarrollada por Bebber (2017). Observamos que Teherán logró aumentar sus recursos cibernéticos y transformarlos en herramientas para ejercer poder sobre otros actores, al punto de que muchos lo consideren como una seria amenaza a su seguridad - especialmente Israel, EE.UU y Arabia Saudita -. Si bien en comparación con otras potencias cibernéticas - como EE.UU, China y Rusia - Irán aún está un paso atrás, lo cierto es que su crecimiento exponencial en los últimos años dan cuenta de que la brecha tecnológica se fue reduciendo poco a poco.

Finalmente, en el tercer capítulo, nos dedicamos a analizar cuáles fueron los resultados de la política de ciberseguridad iraní en la dimensión doméstica e internacional que permitieron proteger la integridad del régimen y posicionar a Irán como una potencia cibernética regional de los durante el periodo de estudio seleccionado.

En el ámbito interno, observamos que las ramas cibernéticas de la IRGC – principalmente el Basij – y el Comando de Defensa del Ciberespacio tuvieron los roles de mayor preponderancia para proteger la seguridad del régimen desde el punto de vista cibernético. A su vez, si bien se utilizaron incontables herramientas para la ejecución de la política de ciberseguridad, podemos decir que la estrategia del gobierno tuvo cuatro grandes ejes que nos ayudan a categorizar el resto de las medidas: el ciberespionaje, la censura, el bloqueo de plataformas y sitios web y la propaganda.

Tras haber abordado la rivalidad EE.UU., Arabia Saudita e Israel; y la ejecución de la política de ciberseguridad de la República Islámica hacia esos actores, consideramos que Irán ha sabido aprovechar las ventajas que proporciona el ciberespacio, para reducir la asimetría existente con estos países.

De esta forma, acortó las distancias respecto a rivales con un gran poder militar tradicional - como EE.UU. - aplicando una estrategia típica de guerra asimétrica. Con Arabia Saudita, utilizó sus capacidades de ciberataque para golpear infraestructuras esenciales de su economía

nacional. Al mismo tiempo, proveyó de recursos cibernéticos a facciones *proxies* para potenciar sus ventajas y vencer a Riad en las distintas guerras en terceros estados.

Más allá de la rivalidad existente entre Irán y Arabia Saudita, observamos que el mayor competidor de Teherán en esta materia ha sido Israel, el país más desarrollado en Medio Oriente en lo que respecta a ciberseguridad. Como pudimos ver en el período estudiado, la República Islámica desafía a Israel en el terreno cibernético, utilizando las cibercapacidades como una herramienta disuasiva - paliando así el retraso del programa nuclear -.

En síntesis, podemos decir que la política de ciberseguridad persa efectivamente se intensificó desde 2009 en adelante, y consiguió cumplir con los dos objetivos macro propuestos: proteger la integridad del gobierno y posicionar a Irán como una potencia cibernética regional. La noción amplia de "ciberseguridad" esbozada por Stevens (2018), nos permitió tender un vínculo entre la política de seguridad cibernética, y los objetivos políticos del régimen; ya que desde el punto de vista del autor, la misma no debe entenderse sólo desde un punto de vista defensivo, sino también como una forma de hacer política nacional e internacional, y de perseguir intereses concretos.

Asimismo, observamos que tal como lo reivindica la teoría realista, el Estado continúa siendo el actor más importante del sistema internacional. Más allá del poder que puedan haber adquirido los individuos gracias los avances tecnológicos y a la aparición de Internet, lo cierto es que los Estados tienen la facultad de controlar a la sociedad civil mediante el ejercicio de la plena soberanía sobre sus territorios - como fue el caso del corte masivo de internet en 2019 o el bloqueo de las aplicaciones que conectan a los iraníes con el resto del mundo -. En este sentido, el concepto de ciberpoder de Venables, Shaikh y Shuttleworth (2015) - es decir, los recursos utilizados para vigilar y alterar el comportamiento de otro por medio del ciberespacio - permitió que pudiéramos identificar cómo el mismo se fue incrementando en el período de estudio, para perseguir intereses políticos concretos.

A su vez, cabe mencionar que retomamos algunos aportes de la teoría de la interdependencia compleja, la cual nos permitió entender al ciberespacio como un dominio más donde una gran diversidad de actores del sistema internacional interactúan y dependen unos de otros. Si bien esta teoría nace en un contexto de globalización incipiente, notamos que la revolución digital ha reforzado la interconexión entre los actores que releva esta corriente; así como también ha elevado el grado de vulnerabilidades a las cuales estos se exponen.

Dado que los cambios tecnológicos y socioculturales ocurren con mayor celeridad, resulta cada vez más complejo analizar el acontecer nacional e internacional. En lo que hace al objeto de estudio de esta tesina, queda pendiente para futuras investigaciones estudiar el flujo de la política de ciberseguridad iraní en el contexto post pandémico, donde la realidad tal cual la conocíamos dio paso a un mar de nuevas incertidumbres.

Bibliografía

Alimardani, M. (12 de septiembre de 2016), *Irán declara «inaugurada» su intranet nacional*, Global Voices. https://es.globalvoices.org/2016/09/12/iran-declara-inaugurada-su-intranet-nacional/

Amnistía Internacional (2019), *Irán*, https://www.amnesty.org/es/location/middle-east-and-north-africa/iran/report-iran/

Arrington, M. (18 de febrero de 2011), *Twitter hacked, defaced By "Iranian cyber army"*, http://techcrunch.com/2009/12/17/twitter-reportedlyhacked-by-iranian-cyber-army/

Aryan, S.Aryan, H y Halderman, A. (2013), *Internet Censorship in Iran: A First Look*, Aryan Censorship Project y Universidad de Málaga.

Azali, M. (2017), *Infographic: Instagram Usage Statistics in Iran*, Techrasa, https://techrasa.com/2017/06/21/infographic-instagram-usage-statistics-iran/
Baezner, M. y Robin, P. (2017), *Hotspot Analysis: Stuxnet*, Center for Security Studies (CSS), ETH Zürich.

Bahais Of Iran, *Una religión mundial originaria de Irán*, https://www.bahaisofiran.org/

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.

BBC Mundo (18 de diciembre de 2009), *Un "ciber ejército" iraní golpea a Twitter*, https://www.bbc.com/mundo/cultura_sociedad/2009/12/091218_1147_twitter_iran_gtg.

BBC Persian (2018), *Structure of Iran's Cyber Warfare*.

Bebber, R (2017), *Cyber Power and Cyber Effectiveness: An Analytic Framework*, 36(5): 426, doi 10.1080/01495933.2017.1379833

Berman, I. (20 de marzo 2013), *The Iranian Cyber Threat, Revisited*, Consejo de Política Exterior Estadounidense.

Bowen, K. y Marchant, J. (2018), *Internet Censorship in Iran: preventative, interceptive, and reactive*, Small Media, 14.

Castro Torres, J.I. (2019), *Diez años del Movimiento Verde en Irán*, Instituto Español de Estudios Estratégicos (IEEE), 14.

Cavelty, M. y Egloff, F. (2019). *The politics of cybersecurity: Balancing different roles of the state*, St Antony's International Review, 15, pp. 37-57.

Cyber Law Toolkit (2012), *Shamoon (2012)*, https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012)#:~:text=A%20group%20called%20'Cutting%20Sword,evidence%20to%20support%20that%20claim.

Chen, T.M. y Abu-Nimeh, S. (2011), *Lessons from Stuxnet,* Computer 44 (4), pp 91–93, DOI 10.1109/MC.2011.115

Council Foreign Relations (15 de marzo de 2021), *The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East*, https://www.cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east

Craig, A. y Valeriano, B. (2016), *Conceptualising cyber arms races*, 8th International Conference on Cyber Conflict Cyber Power, NATO CCD COE Publications, Tallinn.

Daricili, A.B. (2019), *Analysis of Iran's cyber security strategy with regard to the attack and the defense capacity,* Turkish Studies-Social Sciences.

Datosmacro.com (2022), *Irán - Gasto público Defensa*, https://acortar.link/NR1lir.

De Falco, M. (2012), *Stuxnet Facts Report: A Technical and Strategic Analysis*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Deutsch, K. (1964), *External Involvement in Internal War,* New York, NY: Free Press of Glencoe, 100.

Doffman. Z. (6 de julio de 2019), *Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S.*, Forbes, https://n9.cl/wsxz5.

Dubowitz, M. y Ghasseminejad, S. (2020), *Iran's COVID-19 Disinformation Campaign*, Combating Terrorism Center, 13 (6).

El Economista.es, *Dow Jones Industrial Average Editorial,* Ecoprensa, S.A., https://www.eleconomista.es/diccionario-de-economia/dow-jones-industrial-average

El Mundo.es (16 de junio de 2009), *Los manifestantes iraníes utilizan Twitter para hacerse* oír, https://www.elmundo.es/elmundo/2009/06/16/navegante/1245137105.html

Financial Tribune (4 de febrero de 2018), *Iran Ranked World's 7th Instagram User*, https://financialtribune.com/articles/economy-sci-tech/81384/iran-ranked-world-s-7th-instagram-user

Finkle, J. y Wagstaff, J. (1 de diciembre de 2016), *Nuevo ataque informático con el virus Shamoon en países del Golfo*, Reuters, https://www.reuters.com/article/ciberataques-orienteproximo-shamoon-idESL8N1DW1NQ

Farwell, J.P. y Rohozinski, R. (2011), *Stuxnet and the Future of Cyber War. Survival,* 53 (1), pp. 23–40, DOI https://doi.org/10.1080/00396338.2011.555586

García Orta, M.J., Alonso González, M. y Carreras Álvarez, M. V. (2010), Redes Sociales y Herramientas 2.0 en las Elecciones Presidenciales de Irán, ISBN 978-84-693-2361-8.

Goertz, G. y Diehl, P. (2003), *(Enduring) Rivalries,* M. Midlarsky (Ed.), Handbook of War Studies II, The University of Michigan Press, pp. 222-270.

Golkar, S. (2011), *Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran*, Australian Journal of Emerging Technologies and Society, 9 (1).

Górka, M. (2021), *Cybersecurity Politics – Conceptualization of the Idea*, Polish Political Science Yearbook, 50 (1), pp. 71–89, DOI https://doi.org/10.15804/ppsy202112.

Green, D. (8 de mayo de 2018), *From Friends to Foes: How Israel and Iran Turned Into Arch-enemies*, Haaretz, https://n9.cl/nrczu.

Hafezi, P (18 de septiembre de 2009), *Ahmadinejad dice el Holocausto fue una "mentira"*, Reuters, https://www.reuters.com/article/internacional-iran-israel-ahmadinejad-idLTASIE58H03N20090918

Hassan, H. (2007), *Iran: Ethnic and Religious Minorities*, Library of Congress Washington DC Congressional Research Service, 14.

Human Right Watch (2019), World Report 2019, ISBN-13: 978-1-60980-884-6, pp 288 - 297.

Ilyas, A. (2020), COVID-19 Pandemic: Emergence of a new geopolitical perspective, Sustainable Development `policy Institute, DOI http://hdl.handle.net/11540/11906.

Jerez, L. (19 de agosto de 2016), *Los Bahá'ís de Irán, una comunidad perseguida,* Pressenza International Press Agency. https://www.pressenza.com/es/2016/08/los-bahais-iran-una-comunidad-perseguida/

Jones, S. (26 de abril de 2016). *Cyber warfare: Iran opens a new front*, Financial Times. https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3

Journalism Is Not a Crime, https://journalismisnotacrime.com/en/wall/.

Karimi, S. (7 de agosto de 2009) *Ejército cibernético al servicio de la pureza y la juventud,* Keyan Newspaper, Tehran.

Kausch (2017), Cheap Havoc: *How Cyber-Geopolitics Will Destabilize the Middle East*, The German Marshall Fund of the United States, (35).

Kelly, S. y Cook, S. (2011), *A Global Assessment of Internet and Digital Media*, Freedom on the net, Freedom House.

Kuehl, D. T. (2009), *From cyberspace to cyberpower: Defining the problem,* DC: Center for Technology and National Security, National Defense University, 30.

La Vanguardia (14 de junio de 2009), *Violencia y censura contra los periodistas que informan desde Irán*, Madrid, https://n9.cl/8h2xy

Labio Bernal, A. y García Orta, M. J. (2010). *Libertad de expresión en Irán. El desarrollo de la web 2.0 para luchar contra la censura*, Mercado y políticas de cultura y comunicación en la convergencia global, Actas del 3er Congreso Nacional de ULEPICC, pp. 236-245.

Langner, R. (2013), *To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve,* The Langner Group.

LatamIsrael, (24 de abril de 2019), *La mejor escuela sobre el planeta es la unidad 8200 del ejército de Israel*, https://latamisrael.com/la-mejor-escuela-sobre-el-planeta-es-la-unidad-8200-del-ejercito-de-israel/

Lubin, A. (2020), *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, Middle East Institute.

MacGregor, M. (22 de septiembre de 2020), *GMF digital session: The power of influencers*, Made for Minds. https://n9.cl/y024u

Manjikian, M.M. (2010), *From global village to virtual battlespace: the colonization of the internet and the extension of realpolitik*, International Studies Quarterly, 54 (2), pp. 381-401.

Naciones Unidas, Consejo de Seguridad, *Resolución 2231 (2015) relativa a la cuestión nuclear de Irán,* (18 de octubre 2015), https://n9.cl/x5hxl.

Mehran, K. (2008), *The United States and Iran: A Dangerous but Contained Rivalry*, The Middle East Institute Policy Briefs, Georgetown University Institutional Repository, 9.

Newmeyer, K., Cubeiro, E., y Sánchez, M. (2015), *Ciberespacio, Ciberseguridad y Ciberguerra*, Escuela Superior de Guerra Naval, ISBN 978-612-47941-0-0.

Mirghaderi, L. (2021), *Social Media Users Free Labor in Iran Influencers, Ethical Conduct and Labor Exploitation*, Illinois Institute of Technology, 7, DOI https://doi.org/10.3389/fsoc.2022.1006146

Núñez Villaverde, J. (2015); *Irán vuelve al redil, ¿y ahora qué?*, Real Instituto Elcano.

Matrosov, A., Rodionov, E., Harley, D., Malcho, J., (2010), *Stuxnet Under the Microscope*, ESET LLC, 6.

Mohseni, M. (10 de septiembre de 2010), *Iranian cyber army or hired hackerd*, DW World Website, http://www.dw-world.de/dw/article/0,,5992646,00.html

Paredes Roibás, I. (2018). Ataques en el ciberespacio bajo el derecho humanitario y políticas de ciberseguridad como forma de defensa, XIII Edición Máster en Protección Internacional de los Derechos Humanos, Universidad de Alcalá de Henares.

Parsa, S (2008), *Weblogistan: a new path to self-expression in Iran*, Publics, Politics and participation - Location the public sphere in the Middle East and North Africa, SSRC, pp. 325-355.

Peña, R. (2001), *Guerra asimétrica*, Boletín de Información, 270, (4).

Rafiehzadeh, S. (25 de febrero de 2010), *IRGC warn about internet velvet revolution*, Roozonline, http://www.roozonline.com/persian/new s/newsitem/article/////-c1c9eb2e2d.html

Red Nacional de Información (2020). https://hmong.es/wiki/National_Information_Network#title

Reporteros sin Fronteras (11 de marzo de 2013), *The Enemies of Internet - Special Edition: Surveillance*, https://www.jadaliyya.com/Details/28276

Reporteros sin Fronteras (3 de enero de 2018), *Irán - La libertad de información, víctima de la represión de las protestas*, https://acortar.link/sP3nIJ

Roozbeh (2018), *The Politics of Cyberspace in Iran: State-society and International Relations in the Information Age*, Department of Political Science University of Alberta.

Ruiz San Miguel, F.J. y Blanco, S. (2005). *Los contenidos televisivos y el control social de su calidad: los weblogs, una nueva herramienta interactiva*, Universidad de Málaga, España.

Sánchiz, S. (14 de febrero de 2019), *Evolución de Shamoon – Parte 1*, Security Art Work, https://www.securityartwork.es/

Sexton, M. y Campbell, E. (2020), *Cyber War & Cyber Peace in the Middle East: Digital*

Conflict in the Cradle of Civilization, Middle East Institute.

Shalal-Esa, A. (17 de enero de 2013), *Iran strengthened cyber capabilities after Stuxnet: US General*, Reuters, http://www.reuters.com/article/2013/01/18/us-iran-usa-cyber-idUSBRE90G1C420130118

Siboni, G. y Kronenfeld, S. (2012), *Iran and Cyberspace Warfare*, Military and Strategic Affairs, 4 (3), pp. 86-91.

Small Media (2015), *Iranian Internet Infrastructure and Policy Report*, smallmedia.org.uk

Stel, E. (2005), *Guerra cibernética*, Circulo Militar, ISBN: 9789509822696

Steven, S. (2010), *Iran and Israel*, The Iran Premier, United States Institute of Peace, https://iranprimer.usip.org/resource/iran-and-israel

Stevens, T. (2015), *Security and surveillance in virtual worlds: who is watching the warlocks and why?*, International Political Sociology, 9 (3), pp. 230-247.

Stevens, T. (2018), *Global cybersecurity: new directions in theory and methods,* Politics and Governance (ISSN: 2183–2463), 6 (2), pp. 1–4, DOI 10.17645/pag.v6i2.1569

Strum, C. (23 de abril de 2013), *Hackearon el Twitter de Associated Press anunciando falsa explosión en la Casa Blanca*, Fayer Wayer, https://n9.cl/4dlvg

Talbot, D. (6 de marzo de 2009), *La mejor manera de evitar el gran 'firewall' de China*, MIT Technology Review. https://www.technologyreview.es/s/284/la-mejor-manera-de-evitar-el-gran-firewall-de-china

Tanios, S. (2015), *Iran, Israel, the Persian Gulf, and the United States: A Conflict Resolution Perspective,* Asian Politics and Policy, 7 (3), DOI 10.1111/aspp.12199

Tasnim News Agency (18 de agosto de 2016), *Iran Unveils National Information Network*, https://www.tasnimnews.com/en/news/2016/08/28/1170368/iran-unveils-national-information-network

Castro Torres, J. (2019), *Diez años del movimiento verde en Irán*, Boletín IEEE, (14), pp. 64-75.

Torres Soriano, M (2017), *Guerras por delegación en el ciberespacio,* Revista del Instituto Español de Estudios Estratégicos (IEEE), 9.

Tratado de No Proliferación Nuclear,, Artículo. 4, 5 de marzo de 1970)

Tsagourias, N. (2012), *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, 17 (2), pp. 229-244, DOI 10.1093/jcsl/krs019.

Urueña Centeno, F. (2015), *Ciberataques, la mayor amenaza actual*, Instituto Español de Estudios Estratégicos, (1), 42.

Venables, A., Shaikh, S. A., y Shuttleworth, J. (2015), *A Model for Characterizing Cyberpower*, International Conference on Critical Infrastructure Protection, pp. 3-16, Springer, Cham.

Vertuli, M. y Loudon, B.(2018), *percepciones son realidades*, Circulo Militar.

Waltz, K. (2012), *Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability*, Foreign Affairs, Council on Foreign Relations, 91 (4), pp. 2-5.

Wajsman, G. (2022), *Ciberguerra entre Israel e Irán: desde Stuxnet hasta los ciberataques actuales*, Anuario en Relaciones Internacionales, Instituto de Relaciones Internacionales, UNP, ISSN: 1668-639X

West, D. (3 de octubre de 2010), '*The two faces of Twitter: Revolution in a digital age*, The Huffington Post, http://www.huffingtonpost. com/darrellwest/thetwo-faces-of-twitter_b_218734.html

World Trade Energy (12 de septiembre de 2012), *Los ciberataques son un gran riesgo para Saudi Aramco, la mayor petrolera del mundo*, https://www.worldenergytrade.com/oil-gas/general/ciberataques-saudi-aramco-mayor-petrolera-del-mundo

Wajsman, G. (2022), *Ciberguerra entre Israel e Irán: desde Stuxnet hasta los ciberataques actuales*, Anuario en Relaciones Internacionales, Instituto de Relaciones Internacionales, UNP, ISSN: 1668-639X

Zetter, K. (2011), *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/