TRABAJO DE INVESTIGACION FINAL

La distribución de poder en el ciberespacio : Anonymus y las capacidades de ciberpoder 2010-2012

Autor/es:

Thompson, Juan Carlos - LU: 135061

Carrera:

Lic. en Gobierno y Relaciones Internacionales

Tutor:

Dr. Maioli, Esteban

Año: 2012

Fundación Universidad Argentina de la Empresa
Facultad de Ciencias Jurídicas y Sociales

FUNDACIÓN UADE

Trabajo de Investigación Final

La distribución de poder en el ciberespacio: Anonymous y las capacidades de ciberpoder 2010-2012

Lic. en Gobierno y Relaciones Internacionales

Juan Carlos Thompson LU 135061

Universidad Argentina de la Empresa (UADE)

Facultad de Ciencias Juridicas y Sociales

Año 2012

Índice

Resumen

En los últimos años el ciberespacio se ha consolidado como un nuevo ámbito para el desarrollo de las relaciones internacionales. La posibilidad de desempeñar roles protagónicos a muy bajos costos ha facilitado la aparición de nuevos actores no estatales que representan intereses públicos transnacionales y que han contribuido a la difusión del poder. En este contexto, el hacktivismo se ha desarrollado como la nueva forma de ciberactivismo intentando por medio de herramientas virtuales la concreción de sus objetivos.

Anonymous se ha posicionado como un actor relevante en el ciberespacio a través de la utilización de recursos de ciberpoder para la obtención de sus principales objetivos, como la liberalización del flujo de la información y la descentralización del poder. El presente trabajo busca examinar aquellas capacidades de ciberpoder que el grupo ha adquirido en el ciberespacio entre los años 2010-2012, identificándolas a partir de los ciberataques dirigidos en este periodo a organizaciones públicas y privadas con relevancia internacional.

Palabras clave: Anonymous, ciberespacio, ciberpoder, información, hacktivismo.

In recent years the cyberspace has become a new field for the development of international relations. The ability to play leading roles at very low costs has facilitated the emergence of new non-state actors which representing transnational public interests have contributed to the power diffusion. In this context, hacktivism has been developed as a new form of cyberactivism trying, through the use of virtual tools, the achievement of its objectives.

Anonymous has positioned itself as a major player in cyberspace through the use of cyberpower resources for obtaining its main objectives, such as the liberalization of information and decentralization of power. This paper tries to examine the cyberpower capabilities that the group has acquired in cyberspace between the years 2010-2012, identifying them from cyberattacks performed to public and private organizations with international relevance.

Key words: Anonymous, cyberspace, cyberpower, information, hacktivism.

Introducción

Desde comienzos del siglo XXI nuevas amenazas, dirigidas desde el ciberespacio, hacia los individuos, economías y sociedades en su conjunto han agregado una nueva dimensión de análisis al estudio de la distribución de poder (Choucri & Goldsmith, 2012). Para Choucri y Goldsmith (2012) por primera vez en la historia los avances en las tecnologías de la información y la comunicación son potencialmente accesibles a la mayoría de la población mundial. Internet ha transformado varios aspectos en las relaciones entre los diferentes actores internacionales y ha creado un nuevo espacio permitiendo la participación de grupos no gubernamentales en las relaciones internacionales en un nivel no oficial (Hearn, Williams, & Mahncke, 2010). En este sentido, Joseph Nye (2011) explica que el problema de todos los Estados, en la era de la información en la que vivimos, es que cada vez más cosas están sucediendo por fuera del control de los Estados más poderosos y, por tal motivo, la velocidad de Internet implica que estos Estados tengan menos control sobre sus agendas.

Las características de internet, es decir, su velocidad, su bajo costo de transmisión de información y la relativa capacidad de anonimato para sus usuarios parecen ser puntos clave para el surgimiento de "nuevos actores transnacionales quienes reclaman actuar como una "conciencia global" representando intereses públicos generales mas allá de la esfera de competencia de cada Estado" (Traducción propia, Nye, 2011 p.120). En este contexto, los grupos hacktivistas han tenido su origen y han comenzado a cobrar relevancia en el plano internacional. Como define Dorothy Denning (Traducción propia, 2001, p. 263): "los hacktivistas son la convergencia entre el hacking y el activismo, donde "hacking" es usado para referirse a operaciones que utilizan herramientas informáticas de formas inusuales y a veces ilegales. El hacktivismo incluye desobediencia civil electrónica la cual lleva métodos de desobediencia civil al ciberespacio." La libertad en el flujo de información en Internet es su bandera de batalla y sus principales ciberataques, entendidos como los ataques que se llevan a cabo en el "reino de la información" (Nye, 2011), es decir, en el ciberespacio, se dirigen a quienes buscan regular o limitar este tipo de principio cibernético mediante el cual "toda la información debe ser libre, uno debe desconfiar de la autoridad y promover la descentralización de poder" (Traduccion Propia. Saunders, 2011).

Para Nye (2011) el poder basado en la información no es nuevo, pero el Ciberpoder si lo es. Define el Ciberpoder como "la capacidad de obtener resultados esperados mediante el uso de los recursos de información electrónicamente interconectados en el ciberespacio" (Traducción propia, Nye, 2011). Desde esta perspectiva, los grupos hacktivistas como Anonymous utilizan los recursos del ciberespacio como medio para transmitir sus mensajes políticos y, de esta forma, lograr obtener resultados en cuanto a la libertad en el flujo de información.

En diciembre de 2010 el grupo Anonymous cobró relevancia pública global apoyando a Wikileaks, y pidiendo por la libertad de información en Internet, ante la decisión de organizaciones privadas como Visa y MasterCard de quitar el servicio mediante el cual se realizaban transferencias de dinero a la página web de Julián Assange (Busschers, 2010). Mediante una serie de ciberataques denominados "Operación Payback", este grupo hacktivistas se dirigió a organismos financieros y a otras organizaciones que protegían los derechos de copia de música y software.

Las capacidades materiales de los Estados no deben dejarse de lado al momento de analizar esta distribución de poder, pero esta nueva variable, y particularmente, el papel que cumplen los grupos hacktivistas como Anonymous en la misma, implica un nuevo análisis en función a como se distribuye el poder entre los diversos actores que participan del ciberespacio. Algunos Estados como Estados Unidos, Rusia, Reino Unido, Francia y China tienen mayores capacidades terrestres,

marítimas o aéreas que el resto de los actores en el sistema internacional. Sin embargo, si trasladamos esta distribución de poder al ciberespacio, carece de validez.

Como plantea Clay Shirky (Shirky, 2011), algunos Estados como Estados Unidos buscan promover el concepto de libertad en el uso de Internet en el extranjero a través de la libertad de acceso a la información, la libertad de los ciudadanos comunes para producir sus propios medios de comunicación pública y la libertad para conversar unos con otros mediante estos medios. Sin embargo, desde la aparición en Wikileaks (2010) de cables diplomáticos estadounidenses, una serie de hechos, orientados a la limitación y al control de la información en el ciberespacio se han sucedido hasta la fecha. En este contexto, Anonymous se ha posicionado como fiel representante de la libertad de información y ha lanzado una serie de ciberataques a quienes, mediante nuevas legislaciones o persecuciones, buscan limitar el libre flujo de la información en internet. La distribución de poder en el ciberespacio parece no seguir los mismos parámetros que en el resto de los espacios, de forma tal que los actores no estatales pueden actuar con el objeto de que sus resultados sean más notorios, o por lo menos, logren mayor relevancia.

La relevancia del presente trabajo se enmarca en la necesidad proporcionar un análisis de las capacidades y la distribución de poder en un espacio que no ha sido explorado en detalle con anterioridad, es decir, el ciberespacio. Puntualmente, en el surgimiento de nuevos actores que se identifican con intereses por fuera de la esfera estatal y que no han sido tenidos en cuenta para explicar la lógica del poder en este tipo de espacios.

El objetivo principal de este trabajo es examinar las principales capacidades de ciberpoder que el grupo Anonymous ha adquirido en el ciberespacio en el periodo 2010-2012. La delimitación temporal responde a dos hechos que permiten observar los principales objetivos de este grupo hacktivista. En primer lugar el año 2010, y particularmente el caso Wikileaks, representan un punto de inflexión en la participación del grupo Anonymous en el ciberespacio como un actor relevante defendiendo el libre flujo de la información en Internet. Desde que se publicaron los cables diplomáticos y a partir de todos los hechos que se sucedieron con el objeto de limitar la información de la política exterior secreta de varias de las potencias del sistema internacional, el grupo Anonymous ha comenzado a responder mediante ciberataques intentando que la información continúe siendo libre. En Octubre de 2012 un cambio en la postura de Anonymous en relación a Wikileaks permite poner fin a una etapa en la que la página web de Julián Assange representaba de alguna forma el objetivo de este grupo. Según el diario inglés *The Guardian* las declaraciones en redes sociales realizadas en nombre de Anonymous establecían que “la idea detrás de Wikileaks era proporcionar al público información que de otro modo sería mantenida en secreto por gobierno e industrias, información que creemos firmemente el público tiene el derecho de saber” (Halliday J. , 2012). Declaraciones que eran respuesta al hecho de que Wikileaks comenzara a limitar el acceso a la información mediante una suscripción paga.

Los objetivos específicos de este trabajo son: en primer lugar, caracterizar los métodos utilizados por Anonymous para llevar a cabo sus ciberataques en el periodo indicado para de esta forma, en segundo lugar, identificar las capacidades de ciberpoder que este grupo ha desarrollado con el propósito de llevar a cabo sus objetivos. En tercer lugar, mediante este análisis se intentará examinar los resultados que estos ciberataques han tenido en el ciberespacio, en relación a los objetivos del grupo Anonymous, teniendo en cuenta el uso de las capacidades de ciberpoder anteriormente identificadas.

La unidad de análisis del presente trabajo de investigación está representada por los ciberataques llevados a cabo por el grupo hacktivista Anonymous en el periodo 2010-2012. La muestra será no probabilística y solo se tomarán en cuenta los ciberataques realizados desde el 2010 al 2012 dirigidos a organizaciones públicas y privadas y reconocidos como propios por el grupo Anonymous a nivel mundial. La selección de la muestra responde al objetivo de examinar las capacidades de

ciberpoder adquiridas por este grupo en el periodo indicado, por lo que el resto de los ciberataques hacia otros actores y fuera de este periodo no resultan relevantes para la investigación. No se tendrán en cuenta los ciberataques llevados a cabo por las partes del grupo Anonymous que actúan a nivel local ya que lo que se intenta examinar son las capacidades de poder a nivel global.

La técnica de recolección de datos será de relevamiento documental. La misma comprenderá la revisión de bibliografía de diversa índole con el objeto de contar con la información necesaria para llevar a cabo la investigación. En primer lugar su utilizarán revistas especializadas, diarios, artículos y páginas web para recolectar la información referente a los ciberataques realizados por el grupo Anonymous ya que, dada su actualidad, no se han desarrollado elaboraciones teóricas sobre este tema en particular. Mediante esta información se identificarán los métodos utilizados por este grupo para llevar a cabo sus ciberataques y los principales objetivos que se buscan obtener. Esta primera recolección de datos permitirá también examinar los resultados que, durante el periodo indicado, ha logrado el grupo Anonymous.

En segundo lugar se utilizarán libros, *papers* y documentos electrónicos recolectados tanto de bibliotecas como de las bases de datos electrónicas para obtener la teoría necesaria que permita el análisis de la información recolectada en la primera etapa.

La técnica de análisis de la información será el análisis de contenido de los documentos recolectados anteriormente. Las dimensiones de análisis en las que se va a concentrar este trabajo son los métodos utilizados para llevar a cabo los ciberataques, los resultados de los ciberataques en relación a los objetivos del grupo Anonymous y las capacidades de ciberpoder que permiten la ejecución de los mismos. Dentro de las capacidades de ciberpoder solo se tendrán en cuenta los instrumentos virtuales que se desarrollan dentro del ciberespacio, dado que los instrumentos físicos que se dan fuera de este espacio como las manifestaciones y las protestas en las calles no resultan relevantes como un indicador para medir el poder de Anonymous en el mundo virtual sino que hacen referencia a los efectos que este poder causa en el mundo físico.

La hipótesis del presente trabajo es que la combinación entre la utilización de ataques de Denegación de Servicios o Web Hacking y la habilidad de imponer temas en la agenda internacional ha permitido que el grupo Anonymous se posicione como uno de los principales actores en el ciberespacio. Con el objeto de explicar de qué forma Anonymous se posiciona como un actor protagónico en el ciberespacio se recurrirá a una hipótesis subsidiaria: el grupo Anonymous ha logrado, mediante la utilización de capacidades cibernéticas en la ejecución de sus ciberataques, la concreción de sus objetivos en el periodo indicado.

Para cumplir con los propósitos planteados anteriormente, en el primer capítulo se mostrarán los trabajos más recientes sobre la temática en cuestión y luego se desarrollarán las diferentes perspectivas teóricas necesarias para enmarcar la investigación del caso de estudio elegido. En primer lugar se enunciarán los principios Realistas que permiten explicar la distribución de poder en el sistema internacional, en segundo lugar se acudirán a ciertos aspectos de la Interdependencia Compleja con el objeto de evidenciar los cambios a partir de la Revolución de la Información y la aparición de los nuevos actores no estatales y, por último, se establecerán las principales diferencias entre las capacidades materiales y las capacidades cibernéticas disponibles en el ciberespacio.

En el segundo capítulo se introducirá la particularidad del caso de estudio explicando en primer lugar la aparición de nuevos actores en el ciberespacio y la lógica de una nueva forma de activismo denominada hacktivismo. En segundo lugar se identificarán y describirán los principales ciberataques llevados a cabo por Anonymous en el periodo estudiado para poder, más tarde, caracterizar la metodología utilizada en los mismos. En tercer lugar, y a partir del análisis efectuado sobre los ciberataques, se describirán los principales objetivos de Anonymous en el ciberespacio.

En el tercer capítulo, se examinarán las capacidades de poder adquiridas por Anonymous intentando determinar cuál es la posición que este grupo ocupa en el ciberespacio. Por último, se observarán las estrategias desarrolladas por Anonymous al momento de realizar sus ciberataques para evaluar si ha concretado sus objetivos y si el poder que ha utilizado en definitiva puede ser definido como un poder inteligente, es decir, una combinación entre capacidades de hard y soft power.

Capítulo 1

Poder + Ciberespacio = Ciberpoder

Los estudios referidos al ciberpoder son muy recientes y hasta el momento no se han orientado a explicar el papel de los grupos hacktivistas en relación a la distribución de poder en el ciberespacio. Sin embargo, a partir de la aparición de estos grupos en los últimos años, se han desarrollado varios estudios sobre las lógicas hacktivistas. También se han desarrollado, paralelamente, estudios sobre el ciberpoder y las capacidades requeridas por un actor para ejercerlo.

De las indagaciones preliminares realizadas Tim Jordan en su libro "*Cyberpower: The Culture and Politics of Cyberspace and the Internet"* realiza un análisis del ciberespacio describiendo tres regiones interconectadas, que él considera como perspectivas de la naturaleza del ciberespacio, en donde se manifiesta el ciberpoder: desde el punto de vista del individuo, desde el punto de vista de lo social y desde el punto de vista del imaginario colectivo (Jordan, 1999). Desde el punto de vista del individuo el ciberpoder permite, según Jordan, la aparición de la ciberpolítica que genera un mayor acceso a la defensa de los derechos en contra de las opresiones y las instituciones. Desde el punto de vista de lo social, el ciberpoder permite la construcción de estructuras sociales en el ciberespacio en donde los individuos se consideran miembros y hasta en algún punto ciudadanos. Por último, desde el punto de vista del imaginario colectivo el ciberpoder permite el desarrollo de una ciudadanía cibernética por sobre las primeras dos regiones. Esta ciudadanía, en tanto, es reconocida por el resto de los miembros del ciberespacio (Jordan, 1999).

Continuando con su análisis, en el libro "*Hacktivism and Cyberwars: Rebels with a cause"* Tim Jordan explora la lógica hacktivista desde sus orígenes hasta la actualidad basándose en la variable vulnerabilidad. Desde esta perspectiva, Jordan observa como el ciberespacio se ha vuelto más vulnerable ante una gran cantidad de amenazas capaces de transgredir la seguridad y causar daños al bienestar de la sociedad (Jordan, 2004). Si bien Jordan posiciona a los grupos hacktivistas como actores relevantes en el ciberespacio, ya que los considera como "el primer movimiento social de la virtualidad" (Jordan, 2004), sus trabajos carecen de una descripción de los elementos reales de ciberpoder que le permiten a estos grupos ocupar la posición que ocupan.

Por otra parte, Joseph Nye en su libro "*The Future of Power"* realiza una descripción de las dimensiones de ciberpoder que permiten medir la capacidad de poder de un actor determinado en el ciberespacio. En primer lugar diferencia a los instrumentos de la información, o virtuales y luego a los instrumentos físicos. A su vez, ambos instrumentos pueden actuar dentro o fuera del ciberespacio. En segundo lugar, clasifica a los instrumentos en hard o soft power, en función a como son utilizados (Nye, 2011). Como resultado obtiene instrumentos virtuales que pueden ser utilizados como hard power en el ciberespacio, por ejemplo los ataques de denegación de servicio; o instrumentos virtuales que pueden ser utilizados como soft power como por ejemplo establecer normas y estándares en el ciberespacio. Por otro lado, pueden ser utilizados fuera del ciberespacio como hard power, por ejemplo afectando informáticamente con un virus la producción de algún producto estratégico para un Estado, o mediante soft power realizando una campaña para afectar la opinión del resto (Nye, 2011).

En el artículo de Barney Warf y John Grimes "*Counterhegemonic Discurses and the Internet"* el tema de la difusión de poder es el eje fundamental para explicar la aparición de una contrahegemonía. Según los autores, el poder difuso es poder

"nómade", es decir, que en el ciberespacio el poder no tiene un lugar determinado, sino que mantiene su autonomía a través del movimiento (Traducción propia. Warf & Grimes, 1997). El poder es desafiado por formas nómades de resistencia electrónica en el ciberespacio, a partir de las cuales surgen grupos que, no necesariamente organizados, se oponen al poder de la elite (Warf & Grimes, 1997). Estas formas de resistencia electrónica son caracterizadas por Julie Thomas en su artículo *"Ethics of Hacktivism"* como la "caja de herramientas" de los llamados grupos hacktivistas (Thomas, 2001). Según Thomas, los grupos hacktivistas poseen varias técnicas de ataque para obtener sus objetivos. Entre ellas se destacan las infecciones mediante virus informáticos, los ataques de denegación de servicios a páginas webs, las sentadas a las páginas webs y los bombardeos de correos electrónicos a direcciones de e-mail. En este sentido, los hacktivistas plantean que ellos están siguiendo ni más ni menos que la tradición de Gandhi o Martin Luther King, reconocidos activistas, con el objeto de traer cambios sociales mediante medios no violentos (Thomas, 2001).

Los medios utilizados por los grupos hacktivistas para llevar a cabo sus ataques han sido estudiados por Rik Busschers (2010) en su artículo *"Effectiveness of Defence Methods Against DDoS Attacks by Anonymous"*. Para el autor, el grupo Anonymous ha sido uno de los principales representantes del hacktivismo atacando a quienes han intentado derogar la libertad de información en el ciberespacio. El grupo se las ha arreglado para atacar a grandes compañías y a organismos públicos denegando el servicio de sus páginas webs, por lo tanto Busschers asume que las herramientas que este grupo ha utilizado son poderosas (Busschers, 2010). Sin embargo, el autor no tiene en cuenta, a los objetivos finales del grupo Anonymous, como una variable importante a la hora de explicar si las herramientas que utiliza son poderosas o no.

En este sentido, Peter Ludlow analiza en su artículo *"Wikileaks and Hacktivist Culture"* la cultura del movimiento hacktivista. Define al hacktivismo como "la aplicación de las tecnologías de la información y el hacking a la acción política" (Ludlow, 2010). Para Ludlow, la acción política del Hacktivismo se ha extendido en contra de todo tipo de estructuras de poder con el objeto de que la información se encuentre en las manos del público en general (Ludlow, 2010). En su artículo realiza una reseña histórica de los diferentes grupos hacktivistas partiendo del grupo denominado "El culto de la vaca muerta" hasta el grupo Anonymous en la actualidad. Si bien analiza alguno de sus ataques, no hace referencia a capacidades de poder ni analiza la posición de estos grupos en el ciberespacio.

Dorothy Denning realiza un análisis del hacktivismo en su investigación *"Activism, Hacktivism and Cyberterrorism: The internet as a tool for influencing foreign policy"*. Además de explicar y ejemplificar los diferentes métodos de ciberataques indicados anteriormente, Denning observa el poder de estos grupos a partir de ciertas capacidades. Señala que los hacktivistas se sienten poderosos en la medida en que pueden controlar las computadoras del gobierno y obtener de esta forma la atención de los medios, pero que, sin embargo, esto no significa que tendrán éxito en cambiar las reglas ya establecidas (Denning, 2001).

1.1 La era de la Información: nuevo espacio, nuevos actores, nuevas relaciones.

Los Estados, que son las unidades de los sistemas políticos internacionales, no están formalmente diferenciados por medio de las funciones que desempeñan. Dado que se desarrollan en un ambiente anárquico, sus relaciones son de coordinación y esto, por lo tanto, determina su paridad (Waltz, 1988). Para Waltz los Estados no son los únicos actores del sistema internacional. Pero, puesto que las estructuras no están definidas por todos los actores sino por los más importantes, los Estados establecen los términos de sus relaciones permitiendo la creación de reglas o interviniendo

activamente para cambiarlas. En este sentido, “el hecho de afirmar que los Estados conservan el rol principal en el sistema internacional no implica restar importancia o existencia a otros actores” (Waltz, 1988). Los Estados son semejantes con respecto a las tareas con las que se enfrentan pero no en sus capacidades para desarrollar esas tareas, es decir, que las diferencias entre las unidades radican en la menor o mayor capacidad para desempeñar tareas similares. La estructura de un sistema cambia con las variaciones en la distribución de las capacidades entre las unidades del mismo. Estos cambios en la estructura generan variaciones en las expectativas acerca del comportamiento de las unidades y acerca de los resultados que sus interacciones producirán (Waltz, 1988).

El realismo asume que en las condiciones anárquicas del sistema internacional, donde no hay una autoridad de gobierno internacional por sobre los Estados, éstos deben confiar en sus propias capacidades para preservar su independencia y en última instancia, recurrir al uso de la fuerza para mantenerla. El realismo enmarca al mundo en términos de la soberanía de los Estados con el objeto de preservar su seguridad, con fuerza militar como instrumento ultimo. Esta perspectiva representa una buena primera delimitación para enmarcar algunos aspectos de las relaciones internacionales. Pero en la actualidad, los Estados no son el único actor importante en las relaciones globales y la fuerza no es el único ni el mejor instrumento disponible para obtener ciertos resultados (Nye, 2011).

La teoría de la Interdependencia Compleja elaborada por Robert Keohane y Joseph Nye resulta útil en este punto para explicar los cambios de la Revolución de la Información. Durante el siglo XX los modernistas han estado proclamando que la tecnología transformaría el mundo político. Corporaciones multinacionales, ONGs y los mercados financieros globales han cobrado mucha mayor relevancia. En la era de la información, el ciberespacio es un lugar en sí mismo. Los clásicos problemas de la política, es decir, quien gobierna y en qué términos, son tan relevantes para el ciberespacio como para el mundo real (Keohane & Nye, 1998).

La revolución de la información ha incrementado el número de canales de contacto entre sociedades, uno de las tres dimensiones de la interdependencia compleja. Sin embargo, la revolución de la información no ha generado cambios dramáticos en las otras dos condiciones de la interdependencia compleja. Las fuerzas militares aun juegan un significante rol en la relación entre estados y la seguridad aun supera a otros problemas en la relación entre los Estados. En muchas áreas, las suposiciones realistas a cerca del dominio de la fuerza militar y los temas de seguridad se mantienen validos (Keohane & Nye, 1998).

La cantidad de información disponible en el ciberespacio significa poco por sí misma. La calidad de la información y la distinción entre los diferentes tipos de información disponible son cuestiones probablemente más importantes. La información no solo existe, es creada. Tres diferentes tipos de información que son recursos de poder:

- Información libre: es la información que los actores están dispuestos a crear y distribuir sin retribución financiera.
- Información comercial: es la información que la gente está dispuesta a crear y enviar a un determinado precio.
- Información estratégica: confiere grandes ventajas a un actor solo si su competidor no la posee (Keohane & Nye, 1998).

La Revolución de la Información altera los patrones de la interdependencia compleja mediante el incremento exponencial de los canales de comunicación. Pero el movimiento de la información varía según la estructura política existente. La información libre se moverá rápidamente sin regulaciones, la información estratégica será protegida lo mayormente posible y la información comercial dependerá de los derechos de propiedad establecidos en el ciberespacio (Keohane & Nye, 1998). En

este sentido, los actores no gubernamentales tienen muchas más oportunidades para organizarse y propagar sus ideas.

La Revolución de la Información ha permitido el desarrollo de avances tecnológicos orientados a reducir los costos de transmisión de la información, principalmente mediante las computadoras. De esta forma, el poder se enfrenta en la actualidad a la difusión, particularmente en espacios como el cibernético. Los bajos costos de comunicación en Internet han abierto el campo a la aparición de organizaciones poco estructuradas que en los últimos años se han posicionado como actores relevantes en el ciberespacio. El ciberespacio es un régimen híbrido de propiedades físicas y virtuales. Las primeras son controladas por las leyes políticas de la jurisdicción soberana mientras que el control de las segundas es mucho más difícil dadas sus características espaciales (Nye, 2011). "La geografía del ciberespacio es mucho mas mutables que la de otros ambientes, montañas y océanos son difíciles de mover, pero porciones de ciberespacio pueden prenderse o apagarse con un solo click" (Traducción propia. Nye, 2011). Por tal motivo, explica Nye, las barreras para ingresar al ciberespacio son tan bajas que los actores no estatales pueden jugar roles importantes a bajos costos. "En el mundo virtual los actores son diversos, algunas veces anónimos; la distancia física es inmaterial y una ofensa virtual puede ser producida casi a costo cero" (Traducción propia. Nye, 2011).

Sin embargo no todos los aspectos de la Revolución de la Información ayudan a los Estados más pequeños o a los grupos no estatales: Si bien hoy en día la distribución de la información existente es de bajo costo, la producción de información sigue requiriendo costos de inversión; la creación de estándares y arquitectura de los sistemas de la información sigue siendo centralizada en pocas manos; el poder militar continúa siendo importante en algunos aspectos críticos de las relaciones internacionales.

Los Estados territoriales continuarán estructurando políticas en la era de la información, pero confiarán menos en los recursos materiales y más en su habilidad para mantenerse creíbles ante un público con diversos recursos de información en continuo incremento (Keohane & Nye, 1998).

1.2 El poder en el Ciberespacio: Capacidades Materiales vs. Capacidades Cibernéticas.

La concepción más común del poder en las ciencias sociales trata las relaciones de poder como un tipo de relación causal en la cual el poder afecta el comportamiento, las actitudes, las creencias y la propensión de actuar de otro actor. Waltz es uno de los que propone la vieja y simple noción de que un agente es poderoso en tanto que él afecta a otros más de lo que ellos lo afectan a él (Baldwin, 1993). El término capacidades, o recursos de poder, es el que permite especificar el alcance y el dominio del poder en sí. Esto es, quien está involucrado en la relación de poder (alcance) y que tópicos están involucrados (dominio) (Nye, 2011).

El poder está compuesto por elementos tangibles e intangibles (Amstutz, 1982). Un recurso tangible significante es el territorio. Según Morgenthau, la ubicación de una nación es el factor de poder más estable del que depende. La ubicación territorial afecta el desarrollo industrial, la productividad agrícola y la estrategia de defensa del Estado. El tamaño es también relevante a la hora de evaluar recursos materiales y defensa militar (Morgenthau, 1986). Otro factor importante es la población ya que determina el grado de cohesión de una nación y sus capacidades económicas y militares. Sin embargo el tamaño de la población no garantiza poder (Amstutz, 1982). Otros recursos tangibles relevantes son: los recursos nacionales, que permiten el desarrollo económico y aseguran una mayor independencia del sistema internacional; el nivel de desarrollo económico y la fuerza militar. Los recursos intangibles que

permiten afectar el comportamiento del otro son: la cohesión y moral de un país y el liderazgo.

Desde la perspectiva neorrealista de Kenneth Waltz la estructura define la disposición o el ordenamiento de las partes de un sistema a partir del éxito que han tenido para acumular poder, medido en capacidades materiales. Mientras que las partes de los sistemas políticos domésticos se encuentran centralizadas y ordenadas jerárquicamente, las partes de los sistemas políticos internacionales se hallan en relación de coordinación. Formalmente, cada una de ellas es igual a todas las demás, ninguna está autorizada a mandar y ninguna está autorizada a obedecer. La situación mutua de las unidades no está completamente definida por el principio ordenador del sistema ni por la diferenciación formal de sus partes (Waltz, 1988).

Joseph Nye desarrolla una concepción de poder más acorde al propósito de este trabajo. Según Nye, el poder siempre depende del contexto en el que se desarrolla. En el contexto del siglo XXI, dice, la distribución de poder en el mundo se asemeja a un juego de ajedrez en tres dimensiones. En el tablero superior el poder militar es ampliamente unipolar, ya que responde a un único polo de poder que por el momento son los Estados Unidos; en el tablero del medio, el poder económico se ha transformado en multipolar, es decir, que responde a varios polos de poder económico a lo largo del mundo. Por último, el tablero inferior es el ámbito de las relaciones transnacionales que cruzan los límites del control gubernamental e incluye actores no estatales como los hackers que amenazan la seguridad en el ciberespacio (Nye, 2011).

En este sentido, “dos grandes cambios de poder están ocurriendo en este siglo: una transición de poder entre los Estados y una difusión del poder desde todos los Estados hacia los actores no estatales” (Traducción propia. Nye, 2011). La disminución en los costos de comunicación, como consecuencia de la revolución de la información, hace más probable que hackers y criminales cibernéticos causen billones de dólares en daños a gobiernos y compañías.

Desde esta perspectiva, Nye define al poder como “la capacidad de hacer cosas y, en situaciones sociales, de afectar a otros para obtener los resultados que queremos” (Traducción propia. Nye, 2011). La teoría realista presenta una falencia al definir al poder en términos de recursos, dejando de lado al poder definido en términos de dominio y alcance. Por tal motivo, si lo que se buscan son resultados, es necesario prestar más atención al contexto y a las estrategias que se van a utilizar y no solamente a los recursos (Nye, 2011).

El poder que surge de las relaciones también presenta tres diferentes aspectos: en primer lugar, la habilidad de cambiar el comportamiento de otros en contra de sus preferencias iniciales; en segundo lugar la capacidad de controlar agendas para moldear las preferencias de los otros afectando las expectativas de lo que es legitimo o factible; por último la capacidad para establecer preferencias para el resto de los actores. En síntesis las tres caras del poder relacional se pueden esquematizar de la siguiente manera (Nye, 2011):

- Primera cara: A utiliza amenazas o recompensas para cambiar el comportamiento de B en contra de las preferencias iniciales y las estrategias. B lo sabe y siente el efecto del poder de A.
- Segunda cara: A controla la agenda de las acciones de forma que limite las opciones de la estrategia de B. B puede o no saber esto y estar al tanto del poder de A.
- Tercera cara: A ayuda a crear y moldear las creencias básicas, percepciones y preferencias de B. B es poco probable que sea consciente de esto o de darse cuenta del efecto del poder de A.

Además de las tres caras del poder, Nye define dos clases de poder en relación a los recursos y al comportamiento de los actores. En primer lugar define al

Hard Power como la fuerza militar o económica que coacciona a otros a seguir un curso de acción particular. Por otro lado, Soft Power es la habilidad para afectar a otros mediante medios de cooptación, determinando su agenda, persuadiendo y generando una atracción positiva con el objeto de obtener los resultados deseados. Generalmente se piensa que lo recursos tangibles se relacionan con el hard power y los intangibles con el soft power, sin embargo "los recursos usualmente asociados con comportamientos de hard power pueden producir también un comportamiento relacionado a soft power dependiendo del contexto y de cómo son usados" (Traducción propia. Nye, 2011).

La revolución de la información afecta al poder medido en términos de recursos en lugar de comportamientos. En el siglo XVIII el balance de poder Europeo, el territorio, la población y la agricultura proveía la base para la infantería y Francia fue el principal beneficiario. En el siglo XIX las capacidades industriales proveían los recursos para que Gran Bretaña y luego Alemania se posicionaran como dominantes. Para mitades del siglo XX, la ciencia y en particular la física nuclear contribuyeron como recursos cruciales de poder para los Estados Unidos y la Unión soviética. En el siglo XXI la tecnología de la información es probable que sea el recurso de poder más importante (Keohane & Nye, 1998).

El poder en el ciberespacio es entendido como Ciberpoder. Ciberpoder puede ser definido en términos de Nye como "la capacidad de obtener resultados esperados mediante el uso de los recursos de información electrónicamente interconectados en el ciberespacio" (Traducción propia. Nye, 2011). El ciberpoder implica un conjunto de recursos que refieren a la creación, control y comunicación de información electrónica computarizada, infraestructura, redes, software y habilidades humanas.

Dentro del ciberespacio, los instrumentos de la información pueden ser utilizados para producir soft power a través del establecimiento de la agenda, la atracción y la persuasión pero también los ciberrecursos pueden ser utilizados para producir hard power a través de un ataque de denegación de servicios, es decir, utilizando cientos de miles de computadoras para hundir el sistema de internet o la pagina web de una compañía o un país impidiendo su funcionalidad (Nye, 2011).

En el contexto del ciberespacio, es difícil poder encontrar actores que solamente utilicen capacidades de poder en términos de soft o hard power de forma independiente. El concepto "Smart Power" de J. Nye (2011) permite explicar que el poder en la actualidad se desarrolla a través de una combinación de capacidades soft y capacidades hard. Las capacidades de poder de un actor en términos de hard power no siempre garantizan la obtención de los resultados esperados. Son necesarias las capacidades y habilidades para llevar a cabo estrategias que permitan las conversión del poder en resultados. En este sentido, el smart power o poder inteligente "radica en encontrar las maneras de combinar recursos en estrategias exitosas en un nuevo contexto de difusión de poder y del ascenso del resto" (Nye, 2011). Las principales dimensiones del poder inteligente se basan en determinar en primer lugar cuáles son los objetivos esperados por el actor en cuestión, en segundo lugar cuáles son los recursos disponibles y en qué contexto, en tercer lugar cuáles son las formas de poder más adecuadas y en tercer lugar, cuál es la posibilidad de éxito.

Capítulo 2

Anónimos en el Ciberespacio

2.1 Nuevos Actores: Anonymous y la Lógica Hacktivista.

A medida que el sector de las comunicaciones se vuelve más denso, más complejo y más participativo, la población conectada en red logra un mayor acceso a la información, más oportunidades de participar en el discurso público y una mayor capacidad para emprender una acción colectiva (Shirky, 2011). En este contexto, el ciberespacio se posiciona como un espacio estratégico para el desarrollo de las relaciones a nivel internacional dando lugar a una serie de nuevos actores, predominantemente de carácter no estatal, que con el objeto de defender el libre acceso a la información utilizan recursos y capacidades propias de este espacio de acción.

En los últimos años, el activismo también ha incursionado en el ciberespacio. Éste puede ser definido en palabras de Dorothy Denning (2001) como el uso normal y sin interrupciones de internet con el objeto de apoyar una causa o una agenda de temas particulares. Pero lo que verdaderamente interesa a los efectos de esta investigación es una forma específica de activismo que se ha desarrollado en el ciberespacio. El hacktivismo, es decir, la convergencia entre el hacking y el activismo, donde "hacking" es usado para referirse a operaciones en el ciberespacio que utilizan herramientas informáticas de formas inusuales y a veces ilegales con el objeto de obtener algún resultado (Denning, 2001) se ha desarrollado como una de las formas más llamativas de participación en el ciberespacio.

El hacktivismo es muchas veces confundido con el activismo online o con el Ciberterrorismo. El activismo online puede ser definido como legal y no disruptivo, mientras que el hacktivismo tiene intenciones de ser disruptivo y puede ser o no ser legal. Por su parte, el Ciberterrorismo además de intentar ser disruptivo e ilegal busca causar daño intencionalmente o amenazar con acciones violentas con propósitos políticos (Thomas, 2001).

Como una herramienta de poder, Internet beneficia con sus recursos tanto a los individuos y pequeños grupos como a las grandes organizaciones. Facilita actividades como la educación, la colecta de dinero, la formación de coaliciones por sobre las fronteras geográficas, la distribución de peticiones y alertas de acción y la coordinación y el planeamiento de eventos a nivel regional e internacional. Esto permite a los activistas y puntualmente a los hacktivistas evadir los monitoreos estatales (Denning, 2001).

El hacktivismo se ha extendido a la acción política en contra de todo tipo de estructuras de poder (Ludlow, 2010). Sus raíces se remontan a finales de la década de los 1990s con uno de los grupos pioneros de la lógica hacktivista llamado "Teatro de la perturbación electrónica"[1] el cual se caracterizaba por contrarrestar las políticas del gobierno Mexicano mediante "sentadas" virtuales que fueron tomando la forma de ataques de denegación de servicio con el objeto de afectar el correcto funcionamiento de sus páginas webs (Sembrat, 2011). Otro de los grupos precursores en los años 90s fue el denominado "Hong Kong Blondes" quien tomó relevancia pública interrumpiendo ciertas redes electrónicas en China para que las personas pudieran acceder a sitios webs que habían sido bloqueados por el gobierno. The Hong Kong Blondes no fueron los únicos participes de estos hechos, recibieron la ayuda de un grupo estadounidense denominado "El culto de la vaca muerta"[2]. Durante el 2006 este grupo comenzó una

[1] Traducción propia de las siglas en ingles "EDT" (Electronic Disturbance Theater).
[2] Traducción propia de las siglas en ingles "cDc" (Cult of the Dead Cow).

campaña en contra de “Google” cuando éstos cedieron ante las demandas de censura del gobierno Chino (Ludlow, 2010).

En el transcurso del año 2008 una serie de eventos que afectaron a la Iglesia de la Cientología[3] en todo el mundo pusieron el foco en un nuevo grupo anónimo que se oponía moral y éticamente a los principios y doctrinas de esta religión y mediante el uso de herramientas cibernéticas se proponía reducir su influencia (Anderson N. , 2012). En este contexto, el denominado grupo Anonymous hacia su ingreso desde el ciberespacio a la escena internacional y comenzaba a cobrar relevancia. En una carta publicada por el diario “El País” de España, Anonymous expresaba que su mensaje era simple “Anonymous quiere ser un movimiento pacífico a favor de la libertad de expresión en todas partes y en todas sus formas. Libertad de expresión en internet, para el periodismo y los periodistas y los ciudadanos del mundo en general. Independientemente de lo que usted piense o tenga que decir, Anonymous está haciendo campaña a favor de usted.” (Cuéllar, 2010). La particularidad de este grupo es que en realidad no es un grupo en sí mismo. No existen líderes, no existen miembros y no hay que pagar membrecía para participar en él (Anderson N. , 2012).

Si bien Anonymous participó activamente en varios ataques con anterioridad al año 2010, no fue sino a partir de ese momento que su posición en el ciberespacio tomó una postura claramente definida con el objeto de defender la libertad de la información a partir de la defensa de una de las páginas webs más polémicas creadas hasta el momento. Lanzada en 2006, Wikileaks era una organización global sin fines de lucro dedicada a la transparencia a través de la publicación de información clasificada, secreta y privada (Saunders, 2011). Estructurada inicialmente como una página abierta a sus usuarios en donde cualquiera podía anónimamente filtrar documentos de significancia ética, política y diplomática, el sitio fue mutando hasta convertirse en una plataforma de publicaciones de internet más estandarizada con la posibilidad de dar acceso a más de un millón de documentos en línea (Saunders, 2011). De esta forma, Wikileaks representaba una nueva generación para la cultura hacktivista reafirmando el principio de que toda la información debía ser libre y promoviendo la descentralización de poder. Para su creador y quienes lo apoyaban, “la abolición de la diplomacia secreta era la condición primaria para una política exterior honesta, popular, verdadera y democrática” (Saunders, 2011).

Las consecuencias no tardaron de llegar, influenciados por la presión que ejercieron los principales gobiernos de los países afectados por la liberalización de esta información encabezados por Estados Unidos, varios organismos financieros privados que actuaban como intermediarios para que se pudieran realizar donaciones a Wikileaks a través de internet, cancelaron sus servicios e impidieron que los lectores dieran su apoyo económico a quienes publicaban este tipo de información estratégica. Además, una serie de nuevas legislaciones sobre seguridad cibernética y copyright, como la denominada ley SOPA[4], comenzaron a intentar cubrir los vacios legales que hasta el momento dominaban el ciberespacio. A partir de estos hechos, el grupo Anonymous comenzó su llamada operación “Payback” cuyo objetivo principal fue atacar a estos organismos financieros que habían dejado de dar servicio a Wikileaks.

El año 2010 fue un punto de inflexión a nivel mundial para el grupo Anonymous: logró en poco tiempo una visibilidad mayor en relación con sus ciberataques anteriores y expreso de forma más clara cuáles eran sus principales objetivos en el ciberespacio. Las intenciones de Anonymous estaban claras, “residen en cambiar las forma en la que los gobiernos del mundo y la gente en general ven en la actualidad la libertad de expresión en internet. El objetivo es simple: ganar el derecho a mantener Internet libre de cualquier control de cualquier entidad, corporación o gobierno” (Cuéllar, 2010).

[3] Para más información sobre los objetivos y características de la Cientología recurrir a su web oficial. En: www.scientology.org

[4] “Stop Online Piracy Act”.

Muchos de los integrantes del grupo Anonymous representan valores respaldados por varias democracias modernas, como la libertad de expresión, una Internet más libre y un gobierno más transparente. Son, de alguna forma, la canalización de las demandas de una generación que se desarrolla en un nuevo espacio como lo es el ciberespacio (Anderson N. , 2012).

2.2 Los principales Ciberataques y su metodología.

Durante el periodo 2010-2012, el grupo Anonymous llevó a cabo una serie de ciberataques hacia diferentes organismos estatales y privados que se oponían a la libertad de información o apoyaban a quienes buscaban restringir el acceso de la población a ciertos contenidos en Internet. Con el objeto de facilitar el análisis de estos casos, los mismos serán clasificados en tres grupos que corresponden a:

- *Ciberataques a organismos privados*: cuando los ciberataques han sido en contra de empresas u organizaciones con fines de lucro.
- *Ciberataques a Estados*: cuando los ciberataques han sido dirigidos a páginas webs de organismos estatales y/o del propio gobierno de turno.
- *Ciberataques a organizaciones con participación internacional*: cuando los ciberataques han sido dirigidos a organizaciones internacionales, o a organizaciones locales pero con relevancia internacional.

Para analizar la metodología mediante la cual se llevaron a cabo estos ciberataques, es necesario identificar las diferentes formas de ciberataques que desarrollan los grupos hacktivistas. Para Dorothy Denning (2001) el primer método para efectuar un ciberataque se denomina “Sentada Virtual o bloqueo”. Mediante una sentada virtual, miles de activistas visitan simultáneamente un sitio web e intentan generar el tráfico suficiente para que otros usuarios no puedan acceder al mismo. Este método es también denominado por otros autores como Denegación de Servicios o “Distributed Denial of Service” en relación a sus siglas en ingles DDoS. Para Eric Sembrat (2011), un ataque de denegación de servicios es una técnica en la cual varias computadoras funcionan sincronizadas para transmitir el tráfico suficiente para que los servidores del sitio web atacado colapsen y no puedan responder a la demanda de usuarios. El segundo método de ciberataque se denomina “email bombs” o bombas de correo electrónico. Consiste en bombardear al objetivo del ataque con miles de correos electrónicos a la vez mediante herramientas automatizadas (Denning, 2001). El tercer método es el “web hack” o hackeo de la página web, el cual consiste en un grupo de hackers que logran tener acceso a determinado sitio web y reemplazar o extraer cierta información de dicha página. El último de los métodos que los hacktivistas utilizan para realizar sus ciberataques es el uso de virus informáticos con el objeto de difundir un mensaje de protesta y dañando el sistema informático del objetivo a atacar (Denning, 2001).

Ciberataques a Organismos Privados

El conjunto de ciberataques llevado a cabo por el grupo Anonymous en 2010 en contra de tres grandes compañías financieras que proveían el servicio para realizar donaciones a la página web de Julián Assange Wikileaks fue una de las primeras operaciones coordinadas a nivel global. Luego de la publicación de cables diplomáticos e información sensible de varios Estados, las compañías que brindaban servicios a Wikileaks para que sus lectores pudieran realizar donaciones monetarias, cancelaron sus servicios e intentaron apartarse de la imagen que representaba esta nueva manifestación de la libertad de información en internet.

Ante estos hechos, el grupo Anonymous coordinó la llamada “Operación Payback”, la cual consistió en una serie de ataques de denegación de servicios (DDoS) a las páginas web de Visa, MasterCard y Paypal. Los ciberataques también fueron dirigidos en contra de la web del banco Suizo Post Finance, el cual había congelado la cuenta bancaria del creador de Wikileaks, Julián Assange (Fernandez & Caroe, 2010). Entre las declaraciones de los integrantes de la operación, el mensaje que se repetía indicaba que el grupo estaba en contra de cualquier forma de censura en internet y que, por tal motivo, quien intentara llevarla a cabo o quien apoyara a la censura, se vería afectado por estos ciberataques (Halliday & Arthur, 2010).

Mediante estos ataques cientos de miles de transacciones financieras fueron suspendidas y gran parte de los clientes de estas compañías fueron afectados (Halliday & Arthur, 2010).

A partir de la Operación Payback, Anonymous dejo de ser visto como un simple grupo de hacktivistas y comenzó a ser tenido en cuenta por varios Estados y organismos de seguridad como un actor potencialmente peligroso. En este sentido, el gobierno de los Estados Unidos contrato los servicios de la compañía HBGary Federal con el objeto de identificar a los principales participes de la operación Payback.

La compañía de seguridad informática HBGary Federal fue durante un tiempo proveedora de servicios de información del gobierno Estadounidense y participe importante en la búsqueda de quienes durante 2010 habían participado en los ataques a compañías como Visa, MasterCard y Paypal en relación al caso Wikileaks.

A principios del 2011 el CEO de HBGary, Aaron Barr, anunciaba en sus redes sociales que ya tenía en su poder los datos de varios de los protagonistas de los ciberataques llevados a cabo por Anonymous en 2010 y que los mismos iban a ser presentados al FBI y al gobierno de los EEUU si es que éstos se lo solicitaban. Ante el anuncio, Anonymous no se hizo esperar: en enero de 2011 encabezó varios ciberataques contra la página oficial de HBGary Federal mediante el método de DDoS, y hackeó las cuentas de twitter y facebook de Aaron Barr. Pero la ofensiva se extendió mucho más y Anonymous ganó control de los correos electrónicos de la compañía, se infiltró en sus documentos, dio de baja sus teléfonos y publicó varios documentos internos en Internet (BBC, 2011). En este caso, el resultado más obvio para Anonymous fue la publicidad. Los ciberataques fueron cubiertos por varios de los medios más importantes del mundo y le permitieron al grupo mostrar, más allá de sus objetivos de defenderse ante la amenaza de ser descubiertos, los documentos de este tipo de compañías que ayudaban a los gobiernos a mantener el control sobre la administración de la información estratégica (Anderson N. , 2011).

Ciberataques a Estados

Luego de los ciberataques expuestos anteriormente, el grupo Anonymous comenzó a diversificar sus objetivos de ataque. El tópico de la seguridad informática fue puesto en la agenda de los Estados, tanto para la defensa pública como para la defensa de los organismos privados nacionales y, en este contexto, nuevas legislaciones comenzaron a aparecer en diferentes países con el objeto de reglamentar el ciberespacio. De la misma forma, los Estados que bajo un régimen autoritario impedían la libertar de expresión o controlaban los contenidos en Internet, también se convirtieron en un blanco para los ciberataques de Anonymous.

Durante enero del 2011 se llevo a cabo la llamada Operación Egipto. Esta operación dirigida por el grupo Anonymous y con participantes de todo el mundo era una de las respuestas ante las declaraciones, del por entonces gobierno egipcio de Mubarak, que buscaba limitar las protestas públicas a través del bloqueo de las redes sociales que facilitaban su organización. Los objetivos de ataque fueron las páginas web del gobierno Egipcio, principalmente la del Primer Ministro, la del Gabinete, la del Ministerio de Interior y la del Ministerio de Comunicación y Defensa. En todos los casos el método utilizado fue el de denegación de servicio o DDoS (El Tahawy, 2012).

En una de sus publicaciones, Anonymous expresó su objetivo al atacar al gobierno Egipcio, “Anonymous quiere que ofrezcan libre acceso a los medios de comunicación sin censura en todo el país. Cuando ignoran este mensaje, no solo atacamos a las páginas de su gobierno, también nos aseguramos de que los medios internacionales puedan ver la horrible realidad que imponen a su pueblo” (El Tahawy, 2012).

Simultáneamente, en Túnez se sucedían hechos similares a los de Egipto. Las protestas que a comienzos del 2011 sacudían a Túnez no habían cobrado la suficiente relevancia pública para el grupo Anonymous por lo que en ese contexto decidieron lanzar la “Operación Túnez”. Mediante la declaración de que “es responsabilidad de la prensa libre y abierta denunciar lo que la prensa censurada no puede” el grupo Anonymous llevo a cabo una serie de ataques de DDoS contra varios sitios web del gobierno de Túnez los cuales habían alcanzado un alto nivel de censura bloqueando sitios y redes sociales de activistas disidentes, además de cualquier fuente de noticias que mencionara a Wikileaks. El gobierno de Túnez también había llevado a cabo una serie de ataques a las redes sociales y páginas web de quienes llevaran a cabo actividades denominadas como activistas (El Mundo, 2011).

Los ciberataques fueron bajo la metodología de DDoS y se dirigieron principalmente a la página web del Primer Ministro, su gobierno y el mercado de valores. Para el grupo Anonymous la violación de la libertad de expresión e información de los ciudadanos no podía ser tolerada, por lo que proponían continuar los ataques hasta que el Gobierno de Túnez respetara el derecho a la libertad de expresión de todos los habitantes y dejara de censurar internet (El Mundo, 2011).

Como uno de los países precursores de la legislación en contra del cibercrimen a través del proyecto de ley SOPA[5] que fue presentada al congreso y espera su aprobación, Estados Unidos se posiciono rápidamente como un blanco para los ciberataques de Anonymous. Mediante este tipo de legislación se busca una mayor injerencia del gobierno en la administración de los contenidos disponibles en Internet a través de la posibilidad de bloquear al sitio considerado como “infractor”.

Dentro de esta situación, el grupo Anonymous ha dirigido varios ciberataques a diferentes organizaciones estatales y no estatales que se han pronunciado a favor de este tipo de proyectos. Entre los ataques puntuales al gobierno de los Estados Unidos se destacan el realizado al departamento de justicia de los Estados Unidos. El ataque consistió en hackear la página web del Consejo de Estadísticas del departamento de justicia, que se encarga de recabar y analizar datos sobre los crímenes cometidos en Estados Unidos. El robo fue de unos aproximadamente 1700 gigas de datos (El País, 2012).

El motivo de los ciberataques al departamento de justicia se corresponde con el cierre de la página web Megaupload acusada de violar Copyright. “Si ha sucedido esto sin la ley Sopa aprobada, imagínense que ocurrirá cuando entre en vigor. Será el fin de la Internet que conocemos” (Delclós, 2012), declaraba Anonymous en sus redes sociales. La campaña de Anonymous sirvió como venganza por la pérdida de Megaupload y una demostración de la futilidad de los intentos por controlar el ciberespacio (Delclós, 2012).

Algo similar ocurrió en India. A partir de una legislación denominada Information Technology Act, el gobierno Indio paso a tener la capacidad de bloquear, interceptar, monitorear y decodificar cualquier información sobre cualquier dispositivo informático que le resultara sospechosa. En este contexto, el grupo Anonymous lanzó una serie de ciberataques de DDoS en contra de servidores de internet privados, departamentos gubernamentales, la corte suprema de india y dos partidos políticos, quienes fueron en gran medida los que apoyaron la aprobación de la legislación y permitieron que la misma fuera aplicada (Mackinnon, 2012).

[5] Para mas informacion sobre el proyecto de Ley : http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf

En marzo de 2012, Anonymous comenzó a captar la atención en China mediante la publicación de una frase en las páginas webs atacadas, dirigida al gobierno chino "no infalible, hoy las webs son hackeadas, mañana será su vil régimen el que caerá" (Segal, 2012).

Una de las características fundamentales de estos ciberataques en relación a los anteriores, es que la mayoría de los integrantes de Anonymous que participan no se encuentran en China sino en el exterior y utilizan la red china para atacar al régimen popular chino. Los objetivos de estos ataques de DDoS fueron principalmente los sitios del Gobierno y sus agencias Oficiales. El objetivo radica en el estricto control que existe por parte del gobierno Chino a la libertad de expresión y difusión de información en Internet (BBC, 2012).

China tiene uno de los más estrictos sistemas de control social a través de internet en el mundo, llamado The Great Firewall of China. Este sistema le permite al gobierno chino controlar donde las personas pueden ir en el ciberespacio y restringir sobre lo que pueden hablar.

El más reciente ciberataque que Anonymous realizó hacia un Estado fue dirigido al Reino Unido. La llamada "Operación Free Assange" llevo a que varios sitios web del gobierno inglés fueran atacados mediante DDoS durante el mes de agosto de 2012. Los objetivos fueron las páginas web del departamento de justicia de Reino unido y el departamento de trabajo y pensiones. Pero el principal ataque se realizó a la denominada Home Office de UK, el departamento encargado de la inmigración, pasaportes, la política antidrogas, crimen y anti-terrorismo (Halliday J. , 2012). Con el objeto de protestar en contra del pedido de extradición que el gobierno Suizo pide al Reino Unido por Julián Assange que se encuentra refugiado en la embajada de Ecuador en Londres, varios sitios del gobierno británico fueron atacados mediante la denegación de sus servicios, ante declaraciones de que en caso de que saliera de la embajada de Ecuador, Assange seria automáticamente extraditado a Suiza.

Ciberataques a Organizaciones con participación internacional

A mediados del 2011, la Organización del Tratado del Atlántico Norte lanzó un comunicado mediante el cual establecía que el hacktivismo seria detectado y perseguido si sus acciones ilegales continuaban. El grupo Anonymous respondió partiendo de que su mensaje era simple, "si no le mienten a la gente no tendrán que preocuparse de que sus mentiras sean expuestas" (Keating, 2011). Según Anonymous, el principal temor de este tipo de organizaciones no radica en que sean una amenaza para la sociedad, sino en son una amenaza la jerarquía establecida. "Anonymous ha probado en los últimos años que el orden jerárquico no es necesario para obtener buenos resultados" (Keating, 2011), dicen haciendo referencia a la organización de su propio grupo el cual no responder a jerarquías, nadie lidera y el comportamiento del grupo se coordina entre todos sus integrantes.

A partir de este enfrentamiento, el grupo Anonymous lanzó sus ataques contra la OTAN y logró infiltrarse denegando el servicio de la pagina web y robando aproximadamente 1 gigabyte de información sensible para la organización (Nakashima, 2011). La información publicada refiere en gran medida a las operaciones en Afganistán y Kosovo, poniendo de manifiesto algunos de los hechos clasificados sobre el desarrollo de la participación de la OTAN en estos acontecimientos (Daily Mail, 2011).

El FBI también fue sujeto de ciberataques por el grupo Anonymous. En este caso, el grupo intercepto información estratégica de la organización y la publicó en Internet. En primer lugar, pudo tener acceso a información clasificada sobre el juicio de uno de los soldados que lidero la masacre Haditha[6] en Irak, en la cual murieron 24

[6] Para mas detalles sobre la masacre de Haditha visitar la página web de la organización: http://haditha.org/

civiles. El sargento que llevo a cabo la masacre, fue degradado en cargo por la justicia norteamericana pero no fue condenado a prisión por la masacre. El objeto de la publicación de estos documentos fue "poner en evidencia la corrupción del sistema de justicia norteamericano y la brutalidad del imperialismo de Estados Unidos" (El País, 2012). En segundo lugar, durante principios de 2012, Anonymous llevó a cabo una serie de ataques de DDoS contra la página web del FBI en respuesta al arresto de los líderes de la web Megaupload, la cual permitía el intercambio de información gratuita en Internet a través de documentos de diversa índole (Harkinson, 2012).

La Scotland Yard también resulto afectada por los ciberataques de Anonymous. En agosto de 2012 su página web fue atacada mediante un DDoS en la llamada "Operación Free Assange". También fue interceptada una llamada con el FBI en la cual hablaban sobre el grupo Anonymous y la misma fue publicada en youtube (Keating, 2012).

Finalmente, la CIA también fue blanco de los ciberataques de Anonymous en febrero de 2012. Su página web fue atacada a través de DDoS y respondía también a que desde el enero de 2012 el departamento de justicia de EEUU había bloqueado las páginas web de intercambio y visualización de archivos como Megaupload y había acusado de delitos a varios de sus creadores (AFP, 2012).

En síntesis, los métodos utilizados por Anonymous para llevar a cabo sus ciberataques fueron predominantemente de Denegación de Servicios. Si bien en algunos casos estos se articularon con métodos de " web hacking" para la obtención de información sensible que permitiera causar un mayor daño al blanco atacado, los ataques de Denegación de Servicios le permitieron a Anonymous causar daños materiales y al mismo tiempo lograr relevancia pública en los medios de comunicación. De esta forma es posible establecer que las principales características de los métodos utilizados por Anonymous para llevar a cabo sus ciberataques son:

- La utilización de Denegaciones de Servicio o hacking para causar daños materiales a sus objetivos en el ciberespacio.
- La relevancia en los medios de comunicación que logran a partir de los ciberataques.
- La participación de individuos anónimos de todas partes del mundo en los diferentes ciberataques.
- La publicación de sus objetivos y resultados en las redes sociales de forma anónima.

La metodología de ataque desarrollada por Anonymous en el ciberespacio puede también ser caracterizada mediante la conceptualización que realiza Singer (2009) en su libro sobre la revolución de los robots y los conflictos del siglo XXI. Para el autor, ciertas metodologías de ataque en la actualidad pueden ser relacionadas con un enjambre de abejas. Los enjambres se caracterizan por tener un control descentralizado con el objeto de concentrarse en la potencia de su ataque y se componen de una multitud de unidades que actúan de forma paralela por lo que no hay una cadena de mando jerárquicamente establecida. Los enjambres actúan de forma constante con gran intensidad, reaccionando y adaptándose a la situación (Singer, 2009). Esta descripción concuerda ampliamente con la forma en que Anonymous lleva a cabo sus ciberataques. Los ataques de DDoS se distinguen por la amplia participación de unidades que actúan de forma paralela con el objeto de colapsar los servidores de la página web a la cual se intenta afectar. Además, estos ataques también se diferencian porque no existe una cadena de mando ni una jerarquía previamente establecida, todos los hacktivistas participantes se encuentran en el mismo nivel y son igual de importantes para lograr el objetivo final.

2.3 Los objetivos de Anonymous.

Los ciberataques analizados permiten identificar los principales objetivos que el grupo Anonymous ha tenido en el periodo 2010-2012. En este sentido, la relación entre todos los casos observados radica en un objetivo fundamental para el grupo que es la libertad en el ciberespacio. En un espacio en donde lo que predomina es la información, la libertad implica el amplio acceso de los actores a los diferentes tipos de información disponible.

Los diferentes actores que se han opuesto a la libertad en el ciberespacio, es decir las organizaciones privadas, los Estados y las organizaciones internacionales, han sido en su mayoría objetivos de ataque por parte de Anonymous. De esta forma, es posible identificar tres objetivos que explican el desarrollo del grupo Anonymous en los ciberataques analizados.

En primer lugar, y como se indicó anteriormente, el objetivo prioritario que el grupo expone explícitamente, tanto en sus declaraciones como en los destinos a los que se dirige con sus ciberataques, es la libertad de información. Los actores que han resultado víctimas de estos ataques fueron de forma directa o indirecta participes de acciones en contra del libre flujo de información en el ciberespacio. Los organismos privados como Visa, MasterCard y Paypal se mostraron contrarios al propósito de Wikileaks, que representaba también el propósito de Anonymous, en el momento que cancelaron sus servicios. Del mismo modo, HBGary y puntualmente su CEO resultaron una amenaza al desarrollo de la organización hacktivista y dieron lugar a que los mecanismos de recolección de la información, por parte de gobiernos como el estadounidense, salieran a la luz. Los Estados también se posicionaron como opositores al ideal de Anonymous, principalmente regímenes como el egipcio y el tunecino en donde la censura y el bloqueo de información para la organización de los ciudadanos eran algo habitual. Por otro lado, ciertas organizaciones con participación internacional, como la OTAN o el FBI, fueron objeto de ciberataques a partir de la capitalización de información clave sobre el desarrollo de las actividades de Anonymous. Estas organizaciones representaban una fuerte amenaza a la libertad de la información en el ciberespacio, principalmente por el manejo de información estratégica.

En segundo lugar, podemos identificar como objetivo la descentralización del poder. En el análisis de sus ciberataques se evidencia la intención de Anonymous de demostrar como un grupo sin una estructura formal y jerárquica establecida, es capaz de causar daños tangibles e intangibles a ciertos actores que durante mucho tiempo han sido quienes concentraron el poder en los diferentes espacios de la política internacional. El poder de los Estados, las grandes corporaciones privadas y los organismos internacionales parece no tener el mismo efecto en el ciberespacio, lo que permite a grupos como Anonymous llevar a cabo represalias en pos de la descentralización de poder en términos de acceso a la información.

En tercer lugar, la relevancia mediática que el grupo logra a partir de sus ciberataques resulta también un objetivo implícito de la organización. En este sentido, una mayor relevancia mediática es fundamental a la hora de causar daños a sus oponentes. Más allá de las consecuencias materiales que un ataque de denegación de servicio o hacking pueden causar, la cobertura del caso por los diferentes medios del mundo le permiten a Anonymous hacer público su reclamo. En definitiva, una mayor liberalización del flujo de la información en internet, la búsqueda de una descentralización del poder en el ciberespacio y la relevancia pública de sus ciberataques resultan como los objetivos fundamentales del grupo Anonymous en los ciberataques observados.

Capítulo 3

¿Quién es poderoso en el Ciberespacio?

3.1 Las capacidades de ciberpoder adquiridas por Anonymous

Partiendo de la premisa realista que indica que la posición de un actor en el sistema se basa en el éxito que éste ha tenido para acumular poder, medido en capacidades materiales, (Waltz, 1988) es posible examinar cómo se distribuye el poder en los diferentes espacios que conforman el sistema internacional. En primer lugar, es necesario definir al sistema internacional como un extenso conglomerado de unidades independientes e interactuantes las cuales no tienen ningún otro nivel sistémico por sobre ellas (Buzan & Little, 2000). Este conglomerado de unidades interactuantes se encuentra, desde la perspectiva realista, integrado por los actores más importantes que son los Estados (Waltz, 1988). Pero dado que la estructura del sistema cambia a medida que se generan variaciones en la distribución de las capacidades entre las unidades los Estados ya no son las únicas unidades del sistema internacional. Nuevos actores han tenido la posibilidad de comenzar a acumular poder en término de capacidades y por tal motivo se han posicionado como agentes de influencia en el sistema internacional. La teoría realista no es capaz de explicar el surgimiento de los nuevos actores que en la actualidad juegan un papel importante en la distribución de poder en el sistema internacional.

Un nuevo espacio para el desarrollo de las relaciones internacionales ha cobrado mayor relevancia a partir de la Revolución de la Información. El ciberespacio resulta tan importante como el resto de los espacios de interacción para las unidades del sistema internacional. Pero las características del poderoso parecen no seguir los mismos parámetros en el mundo virtual que en el resto de los espacios. Como establece Nye (2011) el poder siempre depende del contexto en el que se desarrolla. En este sentido, las capacidades materiales que asignan poder a los Estados, es decir, las capacidades militares, económicas, de territorio y de población no poseen la misma relevancia en el ciberespacio.

Desde la teoría de la interdependencia compleja, Keohane y Nye (1998) explican como la tecnología ha comenzado a cambiar el sistema y ha permitido el ingreso de nuevos actores como Anonymous a la arena internacional. Internet es un factor clave para entender como Anonymous es capaz de obtener poder en el ciberespacio. El avance de Internet en los últimos años ha permitido incrementar exponencialmente los canales de comunicación y ha decrementado los costos y los tiempos para su transmisión. De esta forma, la información se ha consolidado como un recurso estratégico para los actores que participan de las relaciones internacionales.

La información es un recurso que se encuentra en disputa entre los diferentes actores del ciberespacio. En este punto es necesario aclarar que si bien la información no es un recurso escaso como los recursos materiales, la información estratégica y comercial no se encuentra disponible para todos los usuarios de Internet, o no por lo menos de forma gratuita. Este es el principal problema al que se enfrentan grupos como Anonymous al intentar liberalizar el flujo de información en el ciberespacio independientemente de su origen.

Partiendo de la definición que Nye (2011) elabora sobre el ciberpoder, es decir, la habilidad para obtener resultados esperados a partir del uso de recursos de la información electrónicamente interconectados en el ciberespacio, es posible evaluar cuan poderoso es un actor en este contexto. Los principales recursos de poder en el ciberespacio se traducen en la creación, el control y la comunicación-transmisión de la información (Nye, 2011). Mediante los ciberataques observados, los recursos de poder que Anonymous ha adquirido en el periodo 2010-2012 se traduce en:

- *Creación de la información:*

La creación de información en Internet es un recurso fundamental para cualquiera de los actores que interactúan en el ciberespacio. De esta forma sería correcto pensar que quien produce información estratégica o comercial, la cual luego implica cierto costo de intercambio, posee mayor poder que quien produce información de libre acceso. Sin embargo, Anonymous ha creado y perfeccionado información de libre acceso pero con relevancia estratégica, es decir, la forma de llevar a cabo sus ciberataques.

Los ataques de DDoS fueron perfeccionados por Anonymous durante este periodo y, como se evidencia en los casos observados, fueron una herramienta fundamental para intentar conseguir sus objetivos. La información necesaria para llevar a cabo este tipo de procedimientos fue de libre acceso para todos los que quisieron participar en los mismos, pero al mismo tiempo resultó información estratégica para el resto de los actores del ciberespacio.

En definitiva, la información que Anonymous domina durante este periodo es básicamente el *know how* para la realización de ciberataques, principalmente de DDoS pero también de web hacking, es decir, sobre cómo extraer información sensible de otros actores, como es posible ver en los ataques a la OTAN y al FBI. Si bien podría decirse que la información para llevar a cabo los ciberataques no resulta estratégica para el resto de los actores, ya que en definitiva el acceso a ésta es libre, si resulta estratégica la información necesaria por el resto de los actores para prevenir este tipo de ciberataques. Anonymous se encuentra, durante este periodo, en ventaja ya que domina la ofensiva, mientras que el resto de los actores no poseen la información necesaria para prevenir los ciberataques o desarrollar una defensa efectiva ante los mismos.

- *Control de la información:*

Este recurso es, sin ninguna duda, en el que Anonymous mejor se ha podido concentrar. Partiendo de que uno de sus principales objetivos es la libertad en el flujo de la información, ha unificado sus esfuerzos para garantizar la libertad de la información ante quienes intentaron limitarla. En este sentido la utilización del web hacking como medio para obtener información, que de otra forma no hubiese sido posible conseguir, le permitió a Anonymous tener el control de este recurso en el ciberespacio.

En los ciberataques observados, Anonymous fue capaz de lograr el control de la información que le resultaba necesaria para poder obtener sus objetivos. Cuando su oponente fue una organización privada, pudo controlar información estratégica para causar un daño importante a sus clientes, como en el caso de Visa, MasterCard y Paypal, o para causar un daño a la imagen de la misma organización, como el caso de HBGary Federal. Por otro lado, cuando su objetivo fue un Estado, Anonymous pudo exponer públicamente ciertos aspectos sobre el régimen político que no se querían dar a conocer, como el caso de Egipto, Túnez, India y China y la censura que ejercían sobre el flujo de la información, o sobre información que intentaba mantenerse reservada como en Estados Unidos y los cables diplomáticos o el Departamento de Justicia y los crímenes de guerra. También, cuando el blanco fueron organizaciones internacionales, Anonymous pudo lograr el control de la información que venían recolectando sobre el comportamiento hacktivista, como en el caso de la OTAN y el FBI exponiendo información confidencial de estas organizaciones en el ciberespacio.

Ser capaz de controlar información no siendo el actor que originalmente la creo es una de las habilidades que Anonymous ha podido desarrollar a lo largo del periodo analizado, esto le ha permitido posicionarse por sobre quienes concentran la mayor parte de la información estratégica en el ciberespacio.

- *Comunicación y transmisión de la información:*

La comunicación y transmisión de la información puede ser entendida como un recurso de ciberpoder ya que permite o restringe el acceso de los individuos a la información en el ciberespacio. En este sentido, Anonymous ha buscado mediante sus ciberataques que el acceso a la información sea libre, es decir, que quienes producen y controlan la información puedan transmitirla también libremente.

Anonymous ha logrado que todos sus ciberataques tengan, en mayor o menor medida, relevancia mundial a partir de los medios de comunicación. La habilidad que este grupo ha desarrollado para que sus ataques puedan ser noticia en gran cantidad de medios de comunicación y que, de esta forma, sus demandas sean puestas en agenda, demuestra su dominio sobre el recurso de la transmisión de información.

El ciberespacio facilita en gran medida la transmisión de la información de forma rápida y a bajo costo, por tal motivo Anonymous ha tenido cierta ventaja en relación al resto de los actores que se oponen al libre flujo de información. Una vez logrado el control de la información, como en el caso del Departamento de Justicia o de la OTAN, su transmisión resultó bastante sencilla. Del mismo modo, la organización de un ciberataque y la transmisión de la información necesaria para desarrollarlo fueron posibles gracias a la existencia de canales de comunicación como las redes sociales o los foros de Internet.

El dominio de las herramientas necesarias para la comunicación y la transmisión de la información le han permitido a Anonymous expandir sus demandas en el ciberespacio y ganar relevancia internacional a partir de la cobertura que los medios de comunicación le han dado a sus ciberataques.

De los recursos de ciberpoder identificados anteriormente se desprenden dos capacidades básicas que el grupo Anonymous ha podido desarrollar. En primer lugar, y entendida en términos de hard power, una de las principales capacidades es el desarrollo de ataques de denegación de servicio y de web hacking. Según Nye (2011) los ciberrecursos pueden producir hard power en el ciberespacio ya que pueden causar daños materiales y de esta forma modificar el curso de acción de otro actor. Mediante los ciberataques de DDoS y hacking Anonymous ha causado daños materiales a sus oponentes y ha logrado modificar el curso de acción de aquellos actores que se oponían a sus objetivos.

En segundo lugar, y entendida en términos de soft power, otra de las capacidades de poder que Anonymous ha logrado desarrollar es la habilidad para poner en agenda los principales temas del ciberespacio. Los Estados han comenzado a prestar más atención a este tipo de grupos y se han orientado a intentar reglamentar los espacios legales del ciberespacio, mientras que los medios de comunicación le han dado más relevancia a Anonymous y le han permitido sumar más integrantes alrededor del mundo con el objeto de lograr aquella “conciencia global” que el grupo propone.

Identificadas las capacidades de ciberpoder que Anonymous ha adquirido en el periodo 2010-2012, es necesario a continuación examinar los resultados que han tenido los ciberataques realizados para poder determinar la posición de este grupo en el ciberespacio.

3.2 La posición de Anonymous en el Ciberespacio

Es evidente que la posición de Anonymous en el ciberespacio ha variado desde sus primeros ciberataques, como se puede observar en los casos analizados. Pero para examinar cuál es su verdadera posición en términos de poder, es necesario en primer lugar observar sí mediante la utilización de los recursos anteriormente identificados ha sido capaz de concretar sus objetivos.

Como se detalló en el capítulo anterior, el principal objetivo del grupo Anonymous es la libertad de información en el ciberespacio. En este contexto sus ciberataques se orientaron a aquellos actores que se oponían con acciones concretas a esta especie de principio hacktivista.

En los ciberataques dirigidos a organismos privados, Anonymous demostró que los recursos del ciberespacio eran una herramienta clave para obtener su objetivo. En la "Operación Payback" logró afectar materialmente a las compañías que se habían hecho a un lado a partir del fenómeno Wikileaks y defendió la información que se encontraba publicada en dicha página web. Por otro lado, en su ataque a HBGary logró afectar considerablemente la imagen de esta compañía puesto que resultaba una amenaza para los individuos que participaban en las ofensivas.

Por otro lado, en los ciberataques en contra de Estados, el grupo Anonymous se posicionó como un fiel defensor de la libertad y atacó a quienes optaban por la censura en el ciberespacio. De esta forma Anonymous logró que la información se transmita a pesar de los intentos estatales de restringir el acceso de los individuos a ella mediante leyes o la amenaza de sanciones. En países como Egipto y Túnez Anonymous cumplió un papel clave para proporcionar información sobre los procedimientos para poder sortear la censura impuesta por el gobierno. Mientras tanto, en otros países como India, China y Estados Unidos orientó sus ataques a todas las instituciones que promovieran la necesidad de sancionar una legislación que permitiera la censura estatal en el ciberespacio. Pero a medida que el acceso a la información comenzó a restringirse, este grupo se encargó de aumentar la magnitud de sus ciberataques y de dar a conocer información estratégica de estos actores. Por su parte, y manteniéndose en línea con los ataques que había llevado a cabo anteriormente en defensa de Wikileaks, Anonymous atacó a varias instituciones del Reino Unido con el objeto de apoyar a Julián Assange y en definitiva continuar dando soporte al periodo de libre información que este fenómeno había inaugurado en 2010.

En cuanto a los ciberataques a organizaciones internacionales, Anonymous se encargó de que la información estratégica que dichas organizaciones mantenían bajo su poder, se diera a conocer en el ciberespacio y estuviera accesible a todo aquel que quisiera acceder. En este contexto, aquellas organizaciones que intentaron dar información que afectara la legitimidad de Anonymous en el ciberespacio sufrieron las mismas consecuencias. Información estratégica fue extraída de sus bases de datos y publicada en Internet para mostrar algunas de las operaciones más polémicas llevadas a cabo por estos actores. En el caso de la OTAN Anonymous publicó información sensible sobre las operaciones en Afganistán y Kosovo; en cuanto al FBI publicó información sobre una de las masacres más importantes en Irak en donde varios civiles resultaron muertos en manos del ejército estadounidense.

En definitiva, la utilización de los recursos del ciberespacio le permitió a Anonymous transmitir información de creación propia, principalmente para la organización y realización de sus ciberataques. En cuanto a la información que se encontraba censurada o a la información estratégica que estaba en poder de algún actor relevante en el ciberespacio, los recursos del ciberespacio le permitieron a Anonymous obtener dicha información y transmitirla a la comunidad internacional exponiendo públicamente el accionar de aquellos actores que condenaban el comportamiento de este grupo hacktivista.

En relación al segundo objetivo de Anonymous, los ciberataques le permitieron accionar en contra de la concentración de poder en el ciberespacio. Partiendo del hecho de que las bajas barreras de ingreso al ciberespacio contribuyen a la difusión de poder (Nye, 2011), es posible explicar cómo este tipo de actores no estatales han contribuido a la descentralización del ciberpoder, entendido en términos de recursos de la información.

En los ciberataques a organizaciones privadas Anonymous demostró que, mediante los recursos de ciberpoder disponibles, era capaz de reaccionar ante quienes intentaran monopolizar la información y utilizarla en su contra. Cuando el CEO

de HBGary realizó declaraciones a raíz de la información que había adquirido sobre los participantes de la Operación Payback, automáticamente Anonymous desarrolló una serie de ciberataques que terminaron con la destrucción material y social de la compañía. La imagen de la compañía sufrió grandes consecuencias a partir de que se revelaron datos sobre sus actividades con el gobierno estadounidense.

Del mismo modo, los ciberataques a Estados respondieron a la concreción de este objetivo. La búsqueda de libertad de expresión y transmisión de la información en el ciberespacio llevó a Anonymous a atacar a aquellos Estados que intentaban mediante la coerción, como en Egipto y Túnez, o mediante la implementación de normas legales, como en Estados Unidos, India y China, tener mayor control sobre la distribución de la información y de tal forma concentrar más ciberpoder. Pero Anonymous se opuso firmemente a que concentraran más capacidades de ciberpoder y por tal motivo dirigió sus ciberataques para causar daños materiales a las páginas web de estos actores y a transmitir la información estratégica que, mediante el web hacking, recolectaba de dichos ataques.

Por otro lado, los ciberataques que Anonymous llevó a cabo en contra de organizaciones internacionales también respondieron de alguna manera a cumplir este objetivo. En varias de sus declaraciones en las redes sociales, Anonymous indicaba que la mayor amenaza que representaban para este tipo de organizaciones era su forma de organización. Este grupo desafiaba al orden establecido ya que no necesitaba una estructura jerárquica para coordinar sus acciones en el ciberespacio como el resto de las organizaciones. De esta forma demostró mediante sus ciberataques que un orden jerárquico no es necesario para obtener buenos resultados. A través de los recursos de ciberpoder logró enfrentarse a organizaciones como la OTAN y el FBI afectando materialmente sus páginas webs mediante los ataques de DDoS y perjudicando su imagen a través de la publicación de información sensible. En este sentido, la descentralización del poder, facilitada por el contexto de difusión de poder presente en el ciberespacio, fue un objetivo concretado por Anonymous. Su dominio sobre los métodos de ciberataque y los recursos de ciberpoder necesarios para enfrentarse a cualquier actor que se le opusiera le permitieron combatir la centralización de poder del resto de los actores en el ciberespacio.

Por último, el tercer objetivo del grupo Anonymous, es decir, el lograr relevancia pública internacional mediante sus ciberataques también fue obtenido en el periodo observado. La magnitud de las consecuencias que se desprenden de los ciberataques realizados fueron disparadores para que el grupo Anonymous lograra relevancia mundial a través de los diferentes medios de comunicación.

Más allá de los daños materiales causados a partir de los ataques de denegación de servicios y hacking, la utilización de los medios de comunicación también resultó fundamental para causar daños a la imagen de los actores involucrados. En el caso de los organismos privados, Anonymous pudo capitalizar el recurso de la comunicación para dañar la imagen de las compañías que, como HBGary, Visa, MasterCard y Paypal se opusieron a su primer objetivo. La utilización del ciberespacio como espacio de acción es, sin ninguna duda, la clave para entender la relevancia que estos hechos luego tuvieron en los medios de comunicación.

En cuanto a los Estados, Anonymous pudo utilizar la relevancia mediática para mostrar aquellos aspectos que condenaba de regímenes como el egipcio o el tunecino en relación a la censura y a la falta de libertad de expresión. Sus ciberataques fueron rápidamente cubiertos por varios medios en el mundo, y por tal motivo, su mensaje fue ampliamente difundido.

En relación a las organizaciones internacionales, los ciberataques cobraron importancia en los medios del mundo principalmente a partir de la difusión de información estratégica que Anonymous pudo extraer de estos actores y publicar en Internet. Así, pudo exponer mediáticamente el accionar de organizaciones como el FBI, la CIA, la Scotland Yard y la OTAN y de esta forma, más allá del daño material causado por los ataques de DDoS, logró afectar la imagen de estas organizaciones

para el público general. En la mayoría de estos casos la concepción de seguridad interna de todas estas organizaciones quedó en discusión a partir de que Anonymous lograra derribar sus páginas webs y extraer información sensible permitiéndole mostrar al mundo el verdadero accionar interno de dichos actores.

La utilización de los recursos de ciberpoder que el grupo Anonymous pudo adquirir en el periodo 2010-2012 fue un factor clave para que pudiera obtener sus objetivos en el ciberespacio. Como se evidencia en el análisis realizado anteriormente, Anonymous fue capaz de obtener resultados mediante la creación, el control y la transmisión de la información en el ciberespacio. El desarrollo de capacidades de poder y su articulación a partir de los recursos de la información presentes en el ciberespacio le han permitido posicionarse como un actor poderoso.

3.3 ¿Poder Inteligente?

Como se ha analizado a lo largo de esta investigación, la distribución de poder en el ciberespacio y las capacidades disponibles para los diferentes actores intervinientes no siguen las mismas características que en el resto de los espacios. La información es, en este contexto, el recurso estratégico más importante y la habilidad de los actores para crearla, controlarla y comunicarla es lo que determina la diferencia de la estructura del sistema internacional en el ciberespacio.

Siguiendo el argumento de Nye (2011) en la actualidad y más específicamente en el ciberespacio, las capacidades de ciberpoder en términos de hard power no son suficientes para convertir el poder en resultados. Los ataques de DDoS y web hacking llevados a cabo por este grupo han sido efectivos para causar daños materiales en términos económicos, ya que en la mayoría de los casos afectaron a clientes y/o individuos que quedaron sin servicio o dieron a conocer información de valor estratégico. Sin embargo, no es correcto decir que el ciberpoder desarrollado por Anonymous solamente responde a elementos de hard power. La capacidad de poner en agenda internacional los diferentes ciberataques realizados y de persuadir y atraer más individuos a la lógica hacktivista resulta también relevante para entender la posición de Anonymous en el sistema internacional.

Anonymous ha tenido éxito en articular sus capacidades de hard power (ataques DDoS y hacking) con sus capacidades de soft power (Poner temas en agenda y persuadir otros actores) y, en este contexto, supo estructurar un poder Inteligente que le permitió llevar a cabo estrategias para convertir sus recursos de poder en resultados. La habilidad para organizar sus ciberataques a través de métodos virtuales, de elegir a sus blancos en el ciberespacio y de dar a conocer información estratégica a través del uso de los medios de comunicación, le permitieron aumentar considerablemente la eficacia y eficiencia en la concreción de sus objetivos. Según Nye (2011), las principales dimensiones de una estrategia de “Smart Power” o Poder Inteligente son: determinar los objetivos que se desean obtener, identificar cuáles son los recursos de los que se dispone y en qué contexto, examinar que formas de poder son más adecuadas y finalmente evaluar la posibilidad de éxito.

En primer lugar, Anonymous fue capaz de establecer cuáles eran sus prioridades en el ciberespacio. Si bien en un principio el grupo se enfrentó con una serie de instituciones, como la Iglesia de la Cientologia por una pura contradicción ideológica, es a partir de la Operación Payback que logra firmemente establecer sus objetivos y estructurar sus ciberataques contra quienes se oponían a éstos. Queda claro a partir de las declaraciones analizadas luego de los ciberataques que Anonymous tiene como prioridad en este periodo la liberalización de la información y descentralización del poder en el ciberespacio. Como consecuencia, todos sus ciberataques se estructuraron a partir de estos objetivos y los mismos cumplieron el rol de líneas directrices en todas las acciones que este grupo desarrolló en el ciberespacio. En ningún momento Anonymous se distanció de estos fines lo que le

permitió consolidarse como un actor con fines claros en el espectro de participación del ciberespacio.

En segundo lugar, Anonymous también fue capaz de identificar cuáles eran los recursos más importantes del ciberespacio para ejercer poder y de esta forma los fue adquiriendo y articulando con sus objetivos. Creó información estratégica para llevar a cabo los ciberataques y controló y transmitió información estratégica de otros actores con el objeto de descentralizar el poder de quienes ejercían mayor influencia en el ciberespacio.

En tercer lugar, Anonymous fue capaz de combinar en sus ciberataques capacidades de hard y soft power. De esta forma no solo se orientó a intentar influenciar el comportamiento del resto de los actores a través de la fuerza y de los daños materiales, sino que también utilizó sus capacidades de ciberpoder para poner en agenda sus demandas más importantes en relación a la defensa de la libertad de expresión e información en el ciberespacio. Esta combinación entre las diferentes formas de ciberpoder en un espacio en donde el mismo se encuentra difuso le permitió rápidamente posicionarse como un actor relevante ya que pudo concretar sus objetivos mediante el uso de recursos cibernéticos. En definitiva, Anonymous supo reconocer que la verdadera eficiencia de sus ciberataques no resultaría solo del uso de recursos de ciberpoder para causar daños materiales y coaccionar a otros actores, sino de la combinación de éstos con elementos de soft power para que sus demandas sean conocidas a través del ciberespacio y puestas en agenda.

Por último, Anonymous tuvo éxito al evaluar la ventaja de su estrategia en el ciberespacio. Su habilidad en términos técnicos y humanos para llevar a cabo los ciberataques mediante métodos novedosos y anónimos sumada a su capacidad para lograr que sus objetivos se expandan por el ciberespacio y ganen cada vez más adeptos resulto una ventaja estratégica en relación al resto de los actores. Desde un principio la posibilidad de éxito de este grupo fue alta ya que el ciberespacio le garantizaba anonimato en sus acciones, sus capacidades técnicas les permitían coaccionar al resto de los actores mediante ciberataques y sus habilidades de transmisión y manejo de las redes de comunicación les permitían dar a conocer sus demandas.

Como es posible observar, la articulación de los diferentes recursos de poder presentes en el ciberespacio con los objetivos de Anonymous resultaron factores clave para que este grupo desarrollara capacidades de poder Inteligente y de esta forma se posicionara en el ciberespacio como un actor importante. Las características del ciberespacio configuran un espacio completamente diferente al resto en términos de distribución de poder y, en este sentido, aquellos actores que son capaces de coordinar las mejores estrategias de creación, control y distribución de la información son capaces de establecer las reglas de comportamiento.

Conclusiones

El ciberespacio ofrece una nueva dimensión para el análisis de la distribución de poder que aún no ha sido abordada en detalle. La aparición de nuevos actores que participan activamente del desarrollo de la política internacional mediante el uso de herramientas cibernéticas es un fenómeno reciente que se ha desarrollado a partir de los cambios que Internet ha sufrido en los últimos años. La considerable reducción en los costos de comunicación y transmisión de la información ha permitido una difusión de poder desde los actores clásicos del sistema internacional, los Estados, hacia nuevos actores no estatales con novedosas formas de organización y nuevos objetivos de carácter transnacional.

El nivel de conexión que ha logrado la humanidad a través de internet ha acrecentado también los niveles de interdependencia, principalmente en términos de información. En este contexto, los Estados y sus sociedades se han vuelto más vulnerables ante las acciones de los nuevos grupos que participan del ciberespacio. Las características de este ambiente en donde las fronteras no existen y las barreras de ingreso son sumamente bajas, permiten a los diferentes actores desempeñar grandes roles a muy bajo costo. Particularmente, aquellos grupos no estatales que carecen de una estructura jerárquicamente organizada, poseen ventajas al desempeñar de forma anónima sus acciones en el ciberespacio.

La participación política en Internet se ha incrementado a medida que el acceso de los individuos a este ambiente se fue extendiendo por el mundo. A pesar de que aún muchas zonas del planeta se encuentran fuera de este tipo de tecnología, la increíble cantidad de participantes que interactúan en el ciberespacio permiten comenzar a hablar de una “ciudadanía cibernética”. De esta forma los individuos se identifican más con ciertos grupos que defienden un objetivo global y participan fuera de la esfera estatal que con su propia ciudadanía en términos territoriales. El activismo, y puntualmente su manifestación a través del hacktivismo, es un fenómeno novedoso que permite observar hasta qué punto Internet funciona como un ámbito para articular las demandas de diferentes individuos que, a pesar de su anonimato, buscan participar activamente en la conformación de un nuevo orden internacional a través del ciberespacio.

Si bien muchos de los regímenes democráticos se pronuncian a favor de la libertar en Internet condenando a aquellos que promueven la censura de la información, al mismo tiempo desarrollaron una serie de nuevas normas con el objeto de ampliar la injerencia estatal en la reglamentación del ciberespacio. Es en este ámbito en el que Anonymous ha estructurado sus objetivos y ha desarrollado sus capacidades de poder para consolidarse como uno de los actores más importantes del ciberespacio, representando valores como la libertad de expresión, una internet más libre y un gobierno más transparente, valores que en definitiva coinciden con muchas de las democracias modernas a las que atacan.

Los ciberataques que el grupo Anonymous ha llevado a cabo en el periodo 2010-2012 se dirigieron a tres clases de actores diferentes. En primer lugar, el grupo atacó a las organizaciones privadas que atentaban con los propósitos de la libertad de información en el ciberespacio. En segundo lugar dirigió sus ofensivas a los Estados y organizaciones estatales que o bien aplicaban la censura en cuanto a la información y a la libertad de expresión, o bien desarrollaron normas con el objeto de ampliar la capacidad estatal para reglamentar el ciberespacio. En tercer lugar, Anonymous ejerció su poder en contra de organizaciones internacionales, o locales pero con relevancia internacional, las cuales intentaron desarticular su funcionamiento localizando a los individuos que realizaban materialmente los ciberataques.

La metodología característica en todos los ciberataques observados fue la de Denegación de Servicio o DDoS, combinada otras veces con el web hacking para la obtención de información estratégica. De esta forma, todos los ciberataques cobraron

relevancia mediática internacional y las publicaciones en redes sociales realizadas por miembros de Anonymous para explicar los motivos de sus ataques y dejar en claro sus objetivos, tuvieron la posibilidad de expandirse dentro y fuera del ciberespacio. La participación de individuos de todo el mundo le permitió a Anonymous aumentar su efectividad en los ciberataques ya que cada vez resultó más difícil para las autoridades lograr rastrear quienes ejecutaban estas ofensivas y al mismo tiempo le brindó una mayor constancia en el desarrollo de los ataques de DDoS. Así, es posible afirmar que el hecho de que la participación fuera ejercida desde todo el mundo, refuerza la idea de una conciencia global y de demandas que se articulan por sobre los límites físicos de los Estados.

A medida que se fueron analizando los diferentes ciberataques en este periodo, fue posible también identificar los principales objetivos que Anonymous buscaba de su participación en el ciberespacio. El objetivo más importante que se desprende de todas las declaraciones realizadas por este grupo, es una mayor liberalización del flujo de la información en Internet. Por otro lado, y respondiendo a la lógica en la que se estructuró el grupo -sin miembros, sin lideres y sin jerarquías- el segundo de los objetivos es la descentralización del poder en el ciberespacio. Por último, y con la necesidad de extender su poder de influencia hacia el resto de los actores, Anonymous buscó que los ciberataques desarrollados tuvieran relevancia pública en la mayor cantidad de medios que fuera posible.

Para poder concretar sus objetivos, Anonymous tuvo que dominar una serie de recursos de ciberpoder presentes en el ciberespacio y consolidar una estrategia efectiva para poder transformarlos en las capacidades que le permitieran obtener los resultados deseados. En este sentido, Anonymous se orientó a la creación, el control y la transmisión de la información. En primer lugar pudo crear y transmitir correctamente la información necesaria para que los integrantes del grupo que se encontraban dispersos por todo el mundo tuvieran el know how suficiente para llevar a cabo las ofensivas en el ciberespacio. También supo cómo controlar información estratégica de otros actores y transmitirla para causarles un daño mayor. Por último, desarrolló la habilidad necesaria para comunicar y transmitir la información que le resultaba útil para afectar la imagen de ciertas organizaciones estatales y privadas. De esta forma, pudo en cada ciberataque reafirmar sus objetivos y posicionarse como un legítimo defensor de la libertad.

A medida que Anonymous fue logrando el dominio de los diferentes recursos de poder, pudo desarrollar y articular diferentes formas de ciberpoder con el propósito de asegurar el éxito de sus ciberataques. En primer lugar perfeccionó los métodos de DDoS y los combinó con el web hacking con el objeto de aumentar el daño a quienes se oponían en la obtención de sus resultados. De esta forma, no solo causo daños económicos mediante la suspensión de los servicios web, sino también pudo acceder a información estratégica que luego le resultó útil para afectar la imagen de sus adversarios. En segundo lugar, desarrollo hábilmente capacidades de soft power para afectar el comportamiento de otros miembros poniendo el tema de la libertad en el ciberespacio en la agenda de varios de los actores, principalmente de los Estatales ,que comenzaron a ocuparse intentando revertir esta situación con la reglamentación del ciberespacio. La capacidad de poner el tema en la agenda internacional le permitió extender sus demandas por todo el mundo a través de diferentes medios de comunicación en el ciberespacio y fuera de éste. Así, la lógica hacktivista fue ganando cada vez más adeptos que participaron activamente de los siguientes ciberataques.

Como se demostró mediante esta investigación, Anonymous fue capaz de asegurar el acceso a la información en el ciberespacio a través de los diferentes ciberataques realizados. La habilidad de comunicación y transmisión de la información le permitió asegurar el acceso a todo aquel individuo que quisiera obtenerla, y al mismo tiempo, la habilidad para controlarla le permitió conseguir toda aquella información estratégica que desde su perspectiva, necesitaba darse a conocer. Pero no fue solamente el uso de hard power mediante los ataques de DDoS y web hacking

el que le permitió concretar sus objetivos. Para poder ejercer mayor influencia y lograr una posición más relevante en el ciberespacio Anonymous necesitó de una combinación de capacidades de soft y hard power.

Resulta correcto afirmar en este punto que, como se estableció en la hipótesis principal de esta investigación, la combinación entre la utilización de ataques de Denegación de Servicios o Web Hacking y la habilidad de imponer temas en la agenda internacional ha permitido que el grupo Anonymous se posicione como uno de los principales actores en el ciberespacio. El desarrollo de ataques de Denegación de Servicio y la obtención de información mediante el web hacking fueron métodos claves para poder causar daños en el ciberespacio e intentar coaccionar al resto de los actores. De esta forma Anonymous pudo impedir el acceso de usuarios a los servicios que brindaban las diferentes páginas webs, generando pérdidas económicas para las organizaciones atacadas y también publicando información sensible de clientes o de las propias actividades de la organización. También pudo impedir mediante estos ataques que en casos como el de HBGary o el de la OTAN se revelaran datos clave sobre los participantes de la Operación Payback o que normas de censura sobre la información en el caso de India, Estados Unidos, China, Túnez y Egipto fueran aplicadas efectivamente por el Estado en el ciberespacio.

Las capacidades de ciberpoder en términos hard resultaron validas para que Anonymous pudiera afectar el comportamiento del resto de los actores en el ciberespacio, pero en este sentido, también fue clave el uso de sus capacidades de soft power. La habilidad para poner en agenda temas como la liberalización de la información en el ciberespacio o la descentralización del poder le permitieron maximizar los efectos de sus ciberataques. Controlada cierta información sensible de los principales actores que se oponían a que Anonymous concretara sus objetivos, su capacidad de hacerse conocer y de que la publicación esa información fuera cubierta por gran cantidad de medios internacionales resultó estratégica para que los efectos causados por el uso de hard power fueran mayores. No solo las organizaciones privadas, los Estados y las organizaciones internacionales, sufrieron consecuencias materiales por los ataques de DDoS y web hacking, sino también que muchos de ellos se vieron afectados por la relevancia que cobró la publicación de cierta información clave como en el caso del FBI y las operaciones en Irak o la OTAN y las operaciones en Afganistán y Kosovo. La publicación y transmisión de dicha información muchas veces resulto más efectiva para causar daños a la organización atacada que el propio ataque de DDoS, como por ejemplo en el caso de HBGary.

En definitiva, la habilidad de desarrollar este tipo de estrategias de ataque le permitió a Anonymous lograr los diferentes objetivos que fueron analizados. En primer lugar pudo garantizar la libertad en el flujo de la información a través del control y transmisión de la misma. En segundo lugar fue capaz de influir en la descentralización del ciberpoder a través del uso de los recursos presentes en el ciberespacio, controlando información de los actores más relevantes y transmitiéndola al resto de los individuos. Por último, logró relevancia mediática en el desarrollo de los ciberataques y de esta forma pudo aumentar las posibilidades de éxito en el resto de sus objetivos y expandir sus demandas en el ciberespacio. Lo expuesto anteriormente permite demostrar que, como se indicó en la hipótesis subsidiaria de esta investigación, la utilización de capacidades cibernéticas en la ejecución de los ciberataques le ha permitido a Anonymous lograr la concreción de sus objetivos en el periodo estudiado.

Volviendo a la primera definición de ciberpoder expuesta por Nye (2011) en donde un actor es poderoso si es capaz de obtener los resultados esperados a través del uso de los recursos de la información electrónicamente interconectados en el ciberespacio, y luego de la investigación desarrollada, es factible concluir que Anonymous se ha posicionado en el periodo 2010-2012 como un actor relevante en términos de poder. En este sentido, ha sido capaz de desarrollar capacidades de ciberpoder, tanto en términos de hard como de soft power, y de articular estrategias

efectivas con el propósito de cumplir sus objetivos, los cuales finalmente ha podido lograr y mantener.

La distribución de poder en el ciberespacio y el papel que cumplen los nuevos actores en él es un campo de investigación que todavía necesita una mayor precisión conceptual. Muchas veces las líneas entre el ciberactivismo y el cibercrimen no se encuentran teóricamente delimitadas por lo que no es posible clasificar los métodos de ciertos grupos que participan en el ciberespacio. La falta de legislación y regulación en el ciberespacio es un factor importante a tener en cuenta para poder precisar que métodos están permitidos y que métodos no. En este contexto, definir el papel de los Estados para reglamentar un espacio que no responde a límites territoriales también resulta interesante con el objeto de explicar de forma global las relaciones internacionales que se dan entre actores estatales y actores no estatales en el ciberespacio.

El mundo se ha vuelto cada vez más dependiente del ciberespacio y gran parte de las relaciones internacionales utilizan este medio como plataforma para articular sus intereses. Futuras investigaciones deberán concentrarse más en las características de este espacio e identificar cuáles son los patrones sobre los que se constituyen las lógicas de poder y de qué forma se estructura el orden internacional en el ciberespacio.

Bibliografía

- *Publicaciones:*

Amstutz, M. (1982). Conflict in the International System. En M. Amstutz, *An Introduction to Political Science. The Management of Conflict* (págs. 379-385). Illinois: Scott, Foresman and Company.

Anderson, N. (2012). Who was that masked Man? *Foreign Policy* , 1-4.

Baldwin, D. (1993). Neoliberalism, Neorealism and World Politics. En D. Baldwin, *Neorealism and Neoliberalism: The Contemporary Debate* (págs. 3-25). New York: Columbia University Press.

Buzan, B., & Little, R. (2000). The theoretical toolkit of this book. En B. Buzan, & R. Little, *International System in World History* (págs. 69-89). Oxford: Oxford University Press.

Denning, D. (2001). Activism, Hacktivism and Cyberterrorism: The internet as a tool for influencing foreign policy. En J. Arquilla, & D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy* (págs. 239-288). California: RAND.

Hearn, K., Williams, P., & Mahncke, R. (2010). International Relations and Cyber Attacks: Official and Unofficial Discourse. *Australian Information Warfare and Security Conference.* Australia.

Jordan, T. (1999). *Cyberpower: The Culture and Politics of Cyberspace and the Internet.* Londres: Routledge.

Jordan, T. (2004). *Hacktivism and Cyberwar: Rebels with a Cause.* Londres: Routledge.

Keohane, R., & Nye, J. (1998). Power and Interdependence in the Information Age. *Foreign Affairs , 77* (5), 81-94.

Morgenthau, H. (1986). La Esencia del Poder Nacional. En H. Morgenthau, *Política entre las Naciones. La Lucha por el Poder y la Paz.* Buenos Aires: Grupo Editor Latinoamericano.

Nye, J. (2011). Diffusion and Cyberpower. En J. Nye, *The Future of Power* (págs. 122-147). New York: PublicAffairs.

Nye, J. (2011). Preface. En J. Nye, *The Future of Power* (págs. 14-18). New York: PublicAffairs.

Nye, J. (2011). What is Power in Global Affairs? En J. Nye, *The Future of Power* (págs. 6-23). New York: PublicAffairs.

Singer, P. (2009). *Wired for War: The Robotics Revolution and Conflict in the XXI Century.* New York: Penguin Books.

Waltz, K. (1988). Estructuras Politicas. En K. Waltz, *Teoria de la Política Internacional.* Buenos Aires: Grupo Editor Latinoamericano.

Warf, B., & Grimes, J. (1997). Counterhegemonic Discurses and the Internet. *Geographical Review , 87* (2), 259-274.

- *Documentos electrónicos en línea:*

AFP. (10 de Febrero de 2012). *Anonymous 'ataca' a la CIA*. Recuperado el 11 de Noviembre de 2012, de Diario El Mundo: http://www.elmundo.es/america/2012/02/10/estados_unidos/1328908490.html

Anderson, N. (25 de Febrero de 2011). *Anonymous vs. HBGary: the aftermath*. Recuperado el 3 de Noviembre de 2012, de ArsTechnica: http://arstechnica.com/tech-policy/2011/02/anonymous-vs-hbgary-the-aftermath/2/

BBC. (7 de Febrero de 2011). *Anonymous hackers attack US security firm HBGary*. Recuperado el 3 de Noviembre de 2012, de BBC UK News: http://www.bbc.co.uk/news/technology-12380987

BBC. (5 de Abril de 2012). *Chinese websites 'defaced in Anonymous attack'*. Recuperado el 11 de Noviembre de 2012, de BBC UK : http://www.bbc.co.uk/news/technology-17623939

Busschers, R. (2010). *University of Twente The Netherlands.* Recuperado el 13 de 10 de 2012, de http://referaat.cs.utwente.nl/TSConIT/download.php?id=1085

Choucri, N., & Goldsmith, D. (2012). *Lost in cyberspace: Harnessing the Internet, Internacional Relations and Global Security*. Recuperado el 23 de Agosto de 2012, de Bulletin of the Atomic Scientist: http://globality.cc.stonybrook.edu/?p=195

Cuéllar, M. (9 de Diciembre de 2010). *El ideario político de los "ciberactivistas" anonimos.* Recuperado el 1 de Noviembre de 2012, de El Pais: http://internacional.elpais.com/internacional/2010/12/09/actualidad/1291849216_850215.html

Daily Mail, O. (22 de Julio de 2011). *Anonymous claims to have hacked one gigabyte of classified information from Nato and says 'wait for some interesting data'*. Recuperado el 11 de Noviembre de 2012, de Daily Mail Online: http://www.dailymail.co.uk/news/article-2017584/Anonymous-hacks-Nato-says-wait-interesting-data.html

Delclós, T. (20 de Enero de 2012). *Anonymous replica al cierre de Megaupload atacando webs del Gobierno*. Recuperado el 11 de Noviembre de 2012, de Diario El País: http://tecnologia.elpais.com/tecnologia/2012/01/20/actualidad/1327019245_786013.html

El Mundo, D. (5 de Enero de 2011). *Anonymous ataca varios sitios del Gobierno de Túnez*. Recuperado el 11 de Noviembre de 2012, de Diario El Mundo: http://www.elmundo.es/elmundo/2011/01/05/navegante/1294225836.html

El País, D. (3 de Febrero de 2012). *Anonymous intercepta mensajes del FBI y de los abogados del Ejército de EE UU*. Recuperado el 11 de Noviembre de 2012, de Diario El País: http://tecnologia.elpais.com/tecnologia/2012/02/03/actualidad/1328299419_387178.html

El País, D. (22 de Mayo de 2012). *Anonymous roba 1.700 gigas del departamento de Justicia de EE UU*. Recuperado el 11 de Noviembre de 2012, de El País: http://tecnologia.elpais.com/tecnologia/2012/05/22/actualidad/1337675122_978519.html

El Tahawy, R. (6 de Marzo de 2012). *Anonymous: Operation Egypt*. Recuperado el 11 de Noviembre de 2012, de Egypt Today: http://www.egypttoday.com/news/display/article/artId:567/Anonymous-Operation-Egypt/secId:22

Fernandez, C., & Caroe, L. (9 de Diciembre de 2010). *Army of hackers targets the Swedish government, Sarah Palin and credit card giants in WikiLeaks 'Operation: Payback'*. Recuperado el 3 de Noviembre de 2012, de Daily Mail: http://www.dailymail.co.uk/news/article-1336806/WikiLeaks-hackers-Operation-Payback-cyber-war-targets-Swedish-Government.html

Halliday, J. (12 de Octubre de 2012). *Anonymous distances itself from Wikileaks.* Recuperado el 1 de Noviembre de 2012, de The Guardian: http://www.guardian.co.uk/technology/2012/oct/12/anonymous-distances-itself-wikileaks

Halliday, J. (21 de Agosto de 2012). *Anonymous hits UK government websites over Julian Assange row*. Recuperado el 11 de Noviembre de 2012, de The Guardian: http://www.guardian.co.uk/technology/2012/aug/21/anonymous-hits-government-websites-julian-assange

Halliday, J., & Arthur, C. (8 de Diciembre de 2010). *WikiLeaks: Who are the hackers behind Operation Payback?* Recuperado el 3 de Noviembre de 2012, de The Guardian: http://www.guardian.co.uk/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal

Harkinson, J. (20 de Enero de 2012). *How and Why Anonymous Took Down the FBI's Website*. Recuperado el 11 de Noviembre de 2012, de Mother Jones: http://www.motherjones.com/mojo/2012/01/inside-anonymous-largest-attack-ever-FBI-megaupload-mega-upload

Keating, J. (3 de Febrero de 2012). *Anonymous leaks FBI-Scotland Yard conference call*. Recuperado el 11 de Noviembre de 2012, de Foreign Policy: http://blog.foreignpolicy.com/posts/2012/02/03/anonymous_leaks_fbi_scotland_yard_conference_call

Keating, J. (9 de Junio de 2011). *Anonymous vs. NATO: Get your popcorn ready*. Recuperado el 11 de Noviembre de 2012, de Foreign Policy: http://blog.foreignpolicy.com/posts/2011/06/09/anonymous_vs_nato_get_your_popcorn_ready

Ludlow, P. (4 de Octubre de 2010). *The Nation*. Recuperado el 13 de Octubre de 2012, de http://www.thenation.com/article/154780/wikileaks-and-hacktivist-culture

Mackinnon, R. (6 de Junio de 2012). *The War for India's Internet*. Recuperado el 11 de Noviembre de 2012, de Foreign Policy: http://www.foreignpolicy.com/articles/2012/06/06/the_war_for_india_s_internet

Nakashima, E. (21 de Julio de 2011). *Anonymous claims it hacked NATO Web site, tells FBI 'we're back'*. Recuperado el 11 de Noviembre de 2012, de The Washington Post: http://www.washingtonpost.com/world/national-security/nato-web-site-hacked-by-anonymous/2011/07/21/gIQACLFCSI_story.html

Saunders, R. (2011). *Wikileaks are Not Terrorist - A Critical Assessment of the "Hacktivist" Challenge to the Diplomatic System.* Recuperado el 23 de Agosto de 2012, de Global Studies: http://globality.cc.stonybrook.edu/?p=195

Segal, A. (20 de Abril de 2012). *5 Secrets Anonymous Should Steal from China*. Recuperado el 11 de Noviembre de 2012, de Foreign Policy: http://www.foreignpolicy.com/articles/2012/04/20/5_secrets_anonymous_should_steal_from_china?page=0,0

Sembrat, E. (21 de Octubre de 2011). *Hacktivism: How to respond and build around hacker communities.* Recuperado el 23 de Septiembre de 2012, de Disaster Recovery and Contengency Planning: http://ericsembrat.com/wp-content/uploads/2012/06/is8300-paper.pdf

Shirky, C. (Enero - Febrero de 2011). *The Political Power of Social Media*. Recuperado el 23 de Agosto de 2012, de Foreign Affairs: http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media

Thomas, J. L. (12 de Enero de 2001). *SANS Institute.* Recuperado el 20 de 8 de 2012, de http://www.giac.org/paper/gsec/530/ethics-hacktivism/101266