FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia.

CLARA MARTÍNEZ JIMÉNEZ

Director: Guillem Colom Piella

Madrid, junio de 2015

Índice

"Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional"

Ban Ki-moon

Secretario General de las Naciones Unidas

Introducción e hipótesis

¿Por qué es importante este tema para las relaciones internacionales?

Hoy en día todo parece estar interconectado: los sistemas de defensa, de seguridad, comerciales, energéticos, sanitarios, comunicaciones, transporte, bancarios, alumbramiento, y todo lo que afecta tanto nuestra vida diaria como la seguridad de los estados como tal. Antes, cuando se hablaba de ciberseguridad se enmarcaba en el contexto de las "low politics", ya que no se consideraba como algo vital para la seguridad y la supervivencia del Estado, se trataba como un tema económico o social que no afectaba al bienestar del Estado. (Sánchez Medero, 2013)

Hoy en día, debido a la ya citada interconexión del mundo en el que vivimos, la red es un elemento crucial y vital para las sociedades más avanzadas. Es por esta interconexión que la ciberseguridad ha comenzado a verse como algo vital para la supervivencia del Estado tanto a nivel nacional como a nivel internacional. Es por esto mismo que a día de hoy la ciberseguridad se enmarca dentro de las "high politics". Los ciberataques se han visto como un riesgo potencial para las sociedades, ya que es complicado saber a ciencia cierta cuáles son sus límites.

La posesión de conocimientos para llevar a cabo ataques cibernéticos no entiende de fronteras, y aunque hoy en día las fronteras son muy poco tangibles, los expertos en informática, que a partir de ahora llamaremos *hackers*, tienen grandes facilidades para aprender y una vez que han aprendido, seguir aprendiendo sobre las materias de internet. (Sánchez Medero, 2013)

En 2010, solamente unas décadas después de la creación de internet los expertos de seguridad de la OTAN declararon que el próximo ataque significativo que recibiría la Alianza, poniendo en jaque la polaridad del sistema internacional, seguramente se realizaría a través de internet. (Mshvidobadze, 2013) En la pasada cumbre de Gales del 4

y 5 de septiembre de 2014 la OTAN se centró en realizar una ciberestrategia para la mejor protección del ciberespacio de la alianza. (OTAN, 2014)

La necesidad de una legislación se puso de manifiesto tras los incidentes de Rusia en Ucrania. Sin embargo, parece no haber una conciencia social de la verdadera importancia del mundo ciber, ya que como veremos a lo largo de este trabajo de investigación es muy complicado, por no decir imposible, establecer la autoría de un ciberataque, a lo que hay que sumar la falta de normativas internacionales que definan y/o condenen estos actos.

Los ciberataques son posteriores a las convenciones que hoy en día están vigentes con respecto al Derecho Internacional, por lo que la guerra informática no está recogida dentro del derecho, y no existe norma alguna en el derecho que dicte al respecto de la guerra informática. Sin embargo, desde el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (CCD COE) en el año 2013 publicó el *Manual de Tallín sobre la Ley Internacional aplicable a la Ciberguerra*, (Schmitt, 2013) un documento que analiza las posibilidades existentes para poder aplicar las normas que ya existen en el derecho internacional al ámbito de la ciberguerra. No obstante, este no es un documento oficial, y por tanto no refleja la doctrina o postura de la OTAN o las organizaciones o estados representados en la Alianza, ni siquiera la postura del propio CCD COE. Es simplemente un manual que recoge las opiniones de un grupo de expertos que trabajaron durante años en este tema, debido a la falta de legislación y de iniciativa por parte de los Estados o las organizaciones internacionales más importantes.

Este manual, por un lado, identifica las partes del derecho internacional que pueden ser aplicadas a la ciberguerra. Por otro lado, el manual establece 95 normas que deberían regir estos ciber-conflictos. En esos puntos se abordan temas como la soberanía y la responsabilidad de los Estados. El *ius ad bellum* y el *ius in bello,* así como el derecho humanitario internacional y la ley de neutralidad son, entre otros, las ramas del derecho abordadas por este manual. Cada una de las 95 normas que se definen en este trabajo viene acompañada con una explicación que establece la norma en base a tratados y describe como el grupo de expertos que realizó el informe interpretaría las normas aplicables en el contexto cibernético. (Infodefensa, 2013)

En este trabajo se analizarán las doctrinas de estratégicas tanto de Rusia como de Estados Unidos para respaldar la siguiente tesis: tanto Rusia como Estados Unidos hacen uso de los ciberataques como parte de su estrategia militar en el contexto de las relaciones

internacionales. Para lograr este objetivo se presentarán diversos casos reales que justifican cómo tanto Rusia como Estados Unidos hacen uso de ciberataques como parte de su estrategia militar de defensa. En el caso de Rusia se estudiarán los casos de Estonia en 2007, Georgia en 2008 y más recientemente la situación de Ucrania desde el pasado año 2014, así como se planteará la situación de las *Russian Information Troops* en comparación con el sistema estadounidense de ciberdefensa. Para el caso estadounidense se presentarán los casos de Stuxnet, WikiLeaks, la NSA y el USCYBERCOM.

Metodología

Para conseguir un mejor resultado a la hora de realizar este trabajo de investigación y conseguir un Trabajo de Fin de Grado completo, se han llevado a cabo varios métodos. El primero es delimitado y de investigación en cuanto a la acuñación y definición del término ciberataque y el planteamiento de la relevancia del mundo ciber para la realidad en las relaciones internacionales actuales. Después se procederá a un método descriptivo, para lo que se hará uso de fuentes primarias y secundarias, centrándonos en las Doctrinas de Seguridad y de Estrategia Militar de Rusia como de Estados Unidos, así como toda la documentación específica provista por sendos Estados al respecto. También, se realizará una comparación de ambas doctrinas, así como de las ciber-capacidades de ambos estados, para así comprender mejor los ejemplos y los casos que se expondrán al final del trabajo.

Marco Teórico

Hoy en día la posibilidad de comunicarse es más sencilla, mientras que el mundo de las telecomunicaciones se vuelve más complejo, haciendo que las comunicaciones sean más rápidas y lleguen antes a todo el mundo. Podemos definir el ciberespacio como un espacio de interacción. Su realidad se construye a través del intercambio de información, es decir que el ciberespacio surge en y por la comunicación, de ahí que tenga doble naturaleza, tanto de espacio como de medio. Por tanto el ciberespacio es un «espacio que se genera cuando se producen ciertos tipos de comunicación». (Aguirre Romero, 2004)

Por eso mismo podemos decir que estamos a la merced de los delitos en la red. Los delitos en la red pueden afectar desde lo más mínimo a un usuario privado, hasta la infección de las infraestructuras gubernamentales o de grandes empresas. (Cruzado Reyes, 2011)

¿Por qué es importante el mundo ciber para las relaciones internacionales?

Durante los últimos años ha sido inevitable darse cuenta de que el mundo de Internet o el mundo «ciber» representan un cambio real del paradigma de las dinámicas de la seguridad internacional. Los ciberataques son los encarnadores de la asimetría, ya que son baratos y fáciles de desarrollar, neutralizan la superioridad militar convencional y la posición segura de la que disponían los países occidentales, a la vez que convierten a las sociedades tecnológicamente más avanzadas en las más vulnerables. (Rubio, 2011)

Por norma general, los ciberataques son más baratos que los ataques físicos a la hora de llevarse a cabo. No obstante, si estos son patrocinados por Estados pueden llegar a complicarse y los presupuestos pueden aumentar de manera exponencial. Sin embargo, las herramientas que se necesitan para llevar a cabo un ciberataque están disponibles en todas partes, y las tienen disponibles tanto los estados como los actores no estatales, desde las organizaciones de crimen organizado hasta cualquier hacker independiente. (Fojon Chamorro & Hernandez Lorente, 2014)

La fuente de un ciberataque puede ser bastante complicada de determinar, ya que un ciberataque puede ser *enrutado* (que significa *enviado* en la jerga informática) a través de terceras partes e incluso provenir de otros países, de redes que no estén ni siquiera relacionadas con el ataque o el propio objetivo. No puede hacerse una distinción ente los

que son combatientes y los que no lo son. Los objetivos civiles son tanto objetivos de gran valor como los más fáciles de atacar.

La vulnerabilidad de nuestras sociedades va más allá de un mero riesgo para las infraestructuras críticas. Las sociedades de la información dependen en la confianza y la comunicación abierta. Y, si tenemos esto en cuenta, podemos fácilmente desde difundir mensajes de pánico, desestabilizar gobiernos democráticos hasta destruir grandes cantidades de riqueza.

Siempre se ha hablado de la ciberseguridad y la ciberdefensa como los «nuevos riesgos», junto con la seguridad energética, el cambio climático o los movimientos poblacionales. Sin embargo, el mundo ciber es más que un problema de seguridad y defensa, es un gran cambio en la estructura de nuestras sociedades, economías e incluso de las relaciones globales. En realidad, deberíamos hablar de unas estrategias de seguridad y defensa en un cibermundo en vez de hablar de ciberseguridad o ciberdefensa.

Podemos comparar la situación de la ciberseguridad con la seguridad marítima del siglo XVIII, ya que los ciberatacantes no honran ninguna bandera ni se limitan dentro de las fronteras de ningún país. (Harris, 2014) En realidad los ciberatacantes tienen impunidad legal, ya que esa habilidad de saltarse las fronteras es algo básico en sus estrategias de ataque. Ya que como se ha mencionado anteriormente, los actos de ciberguerra no están regulados actualmente y no pueden aplicarse normas de derecho internacional, ni el derecho de guerra para la regulación o imposición de normas a dichos conflictos.

Hoy en día no hay una cooperación internacional lo suficientemente buena con respecto a este tema; y aunque, existen organizaciones creadas con este fin específico dentro de las organizaciones internacionales responsables de la seguridad internacional, como la OTAN, realmente no hay una legislación internacional que pueda aplicarse y con la que todos los Estados estuviesen de acuerdo, ya que los conceptos, como hemos mencionado anteriormente, se definen de manera muy diferente dependiendo del Estado, porque cada uno tiene sus riesgos y necesidades diferentes a pesar de vivir en un mundo hiperconectado.

Los ciberataques constituyen una revolución profunda en cuanto a la naturaleza de las posibles amenazas que existen para la paz y, por tanto, el buen funcionamiento de las sociedades, estados y economías del siglo XXI. Podría decirse que se sacan tres

conclusiones básicas: la primera es que el desafío que constituye el ciberespacio no es solamente un desafío tecnológico sino más una cuestión de liderazgo, principalmente político. En segundo lugar, para llegar a conseguir un estado de ciberseguridad, se necesita un nuevo enfoque, un enfoque que sea combinado, completo y provenga de diferentes sectores, y que sobre todo esté enfocado a la construcción de unas relaciones civil-militares más fuertes, a la cooperación con las empresas privadas de seguridad y a la educación de los ciudadanos en estas materias. Y, finalmente, la ciberseguridad y la ciberdefensa requieren un aumento en la cooperación internacional tanto a nivel formal como a nivel informal; queriendo decir que deberían crearse nuevas estructuras y políticas o adaptar las ya existentes a las nuevas realidades.

Hay que analizar siempre la importancia de la ciberseguridad para las relaciones internacionales desde el contexto del realismo político. Todo realista político considera que el principal actor de las relaciones internacionales es el Estado. Los Estados están siempre preocupándose por su propia seguridad para perseguir sus intereses nacionales, además de pelear por el poder, que es su principal objetivo. En relación con este trabajo de investigación, analizaremos cómo dos estados llevan a cabo una lucha por la supremacía cibernética y de capacidades del sector.

¿Qué es un ciberataque?

Acuñar el término ciberataque es bastante complejo, ya que diariamente tanto la sociedad como las tecnologías de la información están en continuo cambio, por lo que una definición se quedaría obsoleta en cuestión de poco tiempo. Y, aunque existan muchas definiciones del término, oficiales o no, ninguna abarcará todos los conceptos que desde otro punto del planeta puedan verse como absolutamente necesarios.

Realmente es complicado dar una definición exacta porque depende de muchas variables, y sobre todo si la definición se pretende crear para la aceptación en la comunidad internacional, ya que entre las naciones tienen conceptos diferentes en la mayoría de los sentidos. (Singer & Friedman, 2014) El término de ciberataque se ha usado para todo tipo de actividad «extraña» dentro de los confines del internet, desde las protestas online hasta actos reales de guerra en campos de batalla reales. Incluso los mismos expertos en el tema caen presa a la hora de dar una definición más que valida del concepto, debido a la intangibilidad de los conceptos. Normalmente se llama ciberataque a todo hecho malicioso que conlleve el uso de Internet. Para intentar definirlo bien hay

que comenzar por distinguirlo de un ataque «convencional» (físico). (Singer & Friedman, 2014)

La primera diferencia que encontramos es la fuerza que se usa en los ataques, mientras que en un ataque convencional usamos las fuerzas cinéticas, como puede ser una bomba o el uso de una espada, y que por tanto está ligado a la física y al terreno en el que se encuentren. Mientras que en un ciberataque se usa cualquier tipo de acción informática de cualquier fuerza, y no tiene fronteras y es apolítico, queriendo decir que no proviene de una sola ideología, esto quiere decir que puede estar en múltiples lugares a la misma vez y propagarse en cuestión de segundos. (Singer & Friedman, 2014)

Los objetivos de los dos tipos de ataques son diferentes; los ataques convencionales tienen como objetivo infligir daño físico directo, tangible y específico. Por su parte los ciberataques tienen como objetivo un ordenador o un sistema y la información que contenga, y aunque pueda conllevar en algún momento a daño físico, siempre va a estar centrado en dañar lo informático, como también la información que se encuentra contenida en estos mismos sistemas y redes informáticos. Los ataques convencionales, por ser tangibles, pueden atribuirse más fácilmente que los ciberataques, ya que estos no se puede saber realmente con seguridad a quién atribuírselos.

Normalmente el radio de daños siempre va a ser más predecible en un ataque convencional (a pesar de que existe la posibilidad de que haya errores de cálculo), mientras que cuando creas malware no puedes saber exactamente hasta donde va a propagarse y en el ordenador de qué persona, empresa o entidad va a terminar. Sin embargo, cualquier ciberarma es un sistema bastante complejo y se programa para unos fines muy específicos.

En contraste, los ataques convencionales usan la mayoría de sus recursos en armas y materiales, mientras que en un ciberataque se invierte en la investigación y el desarrollo para poder llevar a cabo el ataque. Otro ejemplo de virus o malware que está destinado a los sistemas industriales son los sistemas SCADA[1].

[1] Es el acrónimo de Supervisory Control And Data Adquisition, en español Supervisión, Control y Adquisición de datos, que es un software para ordenadores que permite el control y la supervisión de procesos industriales a distancia.

En conclusión, podría decirse que la diferencia más clara, obvia y fácil de ver entre los dos tipos de ataque es el uso de la tecnología y los objetivos digitales que se marcan, haciéndolo por tanto mucho menos tangible. Y que un ciberataque es, de manera más general, un ataque de ordenador a ordenador que afecta, inhabilita, destruye o toma el control de un sistema informático; o que daña o roba la información que dicho sistema contiene.

Hay muchas maneras para llevar a cabo un ciberataque, ya sea por ejemplo infectando los ordenadores o las redes con virus y gusanos que controlen, ralenticen o dañen los ordenadores; o bien mediante la explotación de los programas espía para encontrar posibles puntos débiles dentro del sistema, o robar la información; enviando ataques de denegación de servicio (DDoS)[2], con o sin la ayuda de *botnets*[3], para saturar tanto páginas web como redes e infraestructuras críticas. Los ciberataques no causan daño físico a los ordenadores como sucedería si usaramos otro tipo de armas, como por ejemplo destrozándolos con armas o explosivos. Por tanto los ciberataques siempre van a ser llevados a cabo en el ciberespacio. El ciberespacio incluye el internet, las infraestructuras de telecomunicaciones, y los sistemas informáticos.

El objetivo principal de un ciberataque siempre va a ser infligir el daño al ordenador que sea el blanco, robar su información o simplemente observar el sistema para

---

[2] En seguridad informática, se entiende como un ataque de denegación de servicios (DoS por sus siglas en inglés Denial of Service, o DDoS de Distributed Denial of Service) como el ataque a un sistema de ordenadores o a una red que es capaz de causar que un servicio o un recurso sea inaccesible para los usuarios legítimos. Normalmente, lo primero que causa es la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o bien una sobrecarga de los recursos de computación del sistema de la víctima. Este ataque se genera mediante la saturación de los puertos con flujo de información, lo que produce una sobrecarga en el sistema y este por defecto lo "deniega". Los ataques pueden realizarse de muchas formas diferentes, pero todos tienen algo que les une, todos usan la familia de protocolos TCP/IP para llevarse a cabo. Más concretamente, el DDoS, que es una ampliación del DoS, se produce generando grandes flujos de información desde puntos diferentes de conexión, lo que lleva a cabo la sobrecarga y por tanto la denegación del servicio. Esta técnica, gracias a su sencillez tecnológica, es la más usada por los crackers para llevar acabo cualquier tipo de ciberataque.

[3] Microsoft define **Botnet** como: «El término *bot* es el diminutivo de robot. Los delincuentes distribuyen software malintencionado (también conocido como malware) que puede convertir su equipo en un *bot* (también conocido como zombi).Cuando esto sucede, su equipo puede realizar tareas automatizadas a través de Internet sin que lo sepa. Los delincuentes suelen usar *bots* para infectar una gran cantidad de equipos. Estos equipos crean una red, también conocida como *botnet*. Los delincuentes usan *botnets* para enviar mensajes de correo electrónico no deseados, propagar virus, atacar equipos y servidores y cometer otros tipos de delitos y fraudes. Si su equipo forma parte de una *botnet*, el equipo puede volverse más lento y puede estar ayudando a los delincuentes sin darse cuenta.» (Microsoft, 2014)

captar los puntos débiles para un posterior ataque. La clave de un ciberataque es que el atacante siempre lleva a cabo el ataque con intenciones hostiles, y normalmente destructivas, sin el consentimiento o el conocimiento de la víctima. Por su lado el ciberespionaje es la acción de obtener información que la otra parte mantiene en secreto. El ciberespionaje no es el final de la historia, sino que esta información se usa normalmente para obtener algún tipo de ganancia o ventaja estratégica. La información que se obtenga tendrá que tener un valor intrínseco para el lado contrario. Por tanto podemos decir que el ciberespionaje es un ciberataque, pero un ciberataque no es ciberespionaje, ya que un ciberataque conlleva acciones que inflijan daños a la parte que los recibe y el ciberespionaje es el paso previo, el de obtención de información.

En cuanto al perfil de un ciberatacantes, no podemos hablar de uno específico, ya que, como veremos en este trabajo, los perfiles son muy variados. Los ciberatacantes pueden ser tanto Estados como actores no estatales. Con respecto a los actores no estatales tenemos que mencionar a los grupos terroristas, como por ejemplo Al-Qaeda que ha hecho uso de Internet para la consecución de muchos de sus fines.

Por otra parte está el hacktivismo, que se entiende como la utilización de los recursos y herramientas digitales de manera ilegal o legalmente ambiguas normalmente persiguiendo fines políticos. Las herramientas más comunes en este tipo de prácticas son: la desfiguración de páginas web, ataques de denegación de servicio, el robo de información o la parodización de páginas web. (Hacktivismo, s.f.) El grupo de hacktivistas más famoso de los últimos años es *Anonymous*. [4]

Y por último, debemos mencionar a los cibercriminales, que como su nombre indica, son personas que se dedican a perpetrar crímenes en la red. Estos crímenes pueden ser de lo más variado, pero por norma general están relacionados con ataques a empresas, robo de identidades o la difusión de archivos con propiedad intelectual.

En este trabajo nos centraremos en aclarar las diferencias entre el uso de estos ciberataques por parte de sendos actores, pero en especial por el uso por parte de ciertos

[4] El grupo Anonymous que nació en 2008 se ha dedicado desde entonces a luchar por la libertad de expresión y a manifestarse en acciones con la independencia de internet en contra de diversas organizaciones servicios públicos con presencia global y sociedades de derechos de autor. Anonymous es una organización a nivel mundial que empezó en las redes sociales y que se ha extendido por todos los rincones de la tierra. Los principales hacktivistas de esta organización son conocidos por ser de origen ruso. En el conflicto de Crimea, Anonymous declaró que estaba monitorizando las acciones de ciberataques en las infraestructuras informáticas del país.

actores estatales (Rusia y Estados Unidos), y la comparación de sus doctrinas estratégicas para aclarar ciertas acciones. El daño que se causa con un ciberataque puede ser extensivo o minúsculo, eso no define un ciberataque. Lo que sí lo define es la finalidad del daño causado con dicho ciberataque. El objetivo de dicho ataque tiene que conseguir afectar de algún modo a un objetivo económico, psicológico, social o político.

En el Anexo I se incluye un cuadro explicativo realizado por el *think tank* de ciberseguridad THIBER, con los tipos de actores que ordenan los ciberataques, sus objetivos principales, los tipos de ataques que suelen utilizar para la consecución de esos objetivos, y además el nivel de impacto que dichos ataques tienen sobre esos objetivos.

La doctrina estadounidense.

"Cyberspace technology is emerging as an "instrument of power" in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies." (Schiller, 2010)

The Joint Forces Command, 2010

El Departamento de Defensa de los Estados Unidos cada cuatro años publica un informe con un resumen sobre la defensa. El de 2010 declaraba que a través de sus relaciones de defensa exterior, los Estados unidos no sólo ayudan a advertir posibles crisis, sino que también mejoran la efectividad a la hora de responder a dichas crisis. El hecho de que el Departamento de Defensa cuente con un departamento especial llamado Departamento de Estrategia de Defensa para las Operaciones en el Ciberespacio (por el inglés *Department of Defense Strategy for Operating in Cyberspace*), nos muestra la gran relevancia que se le da a las relaciones internacionales dentro del ciberespacio por parte del ejecutivo estadounidense. El mismo DoD (*Department of Defense*), cuenta con una Estrategia Internacional para el Ciberespacio, cuyo objetivo es principalmente la colaboración con sus colaboradores de otras agencias y no solo agencias estatales estadounidenses, sino que también se centra en construir y mejorar las relaciones con otras agencias internacionales que tengan los mismos intereses dentro del ciberespacio. Otro de sus objetivos es la creación y el desarrollo de un marco común tanto legal como institucional para definir mejor los términos del ciberespacio, así como crear consciencia de las capacidades cibernéticas tanto de los ciudadanos como de los profesionales.

Los cinco pilares son el marco de la estrategia militar estadounidense para la ciberguerra. El primer pilar es el que habla de que el ciberespacio es un nuevo espacio para la guerra y que tiene similar valor para los Estados Unidos como los demás. El segundo pilar habla de cómo ha de favorecerse la defensa proactiva en lugar de la defensa pasiva que estaba viéndose como tendencia en los últimos años (un ejemplo de defensa pasiva es el uso de firewalls). El objetivo principal de este pilar es que se detecte con más rapidez la intrusión de cualquier ataque en una de las redes de Estados Unidos para así poder encontrar el foco del ataque y atacar al intruso.

El tercer pilar es la protección de infraestructuras críticas (CIP). El cuarto pilar es el uso de la defensa colectiva, lo que permitirá la pronta detección para incorporar esta herramienta a la estructura de defensa de ciberguerra. El último y quinto pilar es el mantenimiento de las ventajas del cambio tecnológico, esto incluye una mejora en las competencias informáticas y un aumento de las capacidades de inteligencia artificial. (Garamone, 2010)

Por su parte, el FBI cuenta con la *FBI Cyber Division* que es la división del FBI encargada de liderar los esfuerzos nacionales para investigar y procesar los crímenes en internet, entre los que se encuentran el ciberterrorismo, el ciberespionaje, las intrusiones en ordenadores y los ciber-fraudes más graves. Esta división se creó en el año 2002, y tiene tres áreas principales de interés: las intrusiones en los ordenadores, el robo de identidad y el ciber-fraude. La FBI Cyber Division trabaja a través de la *National Cyber Investigative Joing Task Force (NCIJTF)* y brigadas de ciber-investigadores que se encuentran en cada oficina de campo del FBI. (Federal Bureau of Investigation , 2015) Desde el año 2008 el NCIJTF es la principal agencia estadounidense responsable para la coordinación de investigaciones de ciber-amenazas y la que sirve de unión para la CIA, el Departamento de Defensa, el Departamento de Seguridad Nacional (Department of Homeland Security) y la Agencia Nacional de Seguridad (NSA). (Kraft & Marks, 2012)

El 4 de noviembre de 1952 Harry Truman creó en secreto la Agencia Nacional de Seguridad (en inlglés "*National Security Agency*", también conocida como la NSA). La NSA era precursora de la ASFA (*Armed Forces Security Agency*). Esta agencia es una agencia de inteligencia dependiente del Departamento de Defensa del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información. (Leandry-Vega, 2014)

La NSA provee de servicios y productos tanto al Departamento de Defensa, a la Comunidad de Inteligencia, a agencias gubernamentales, y a una selección de aliados y socios de la coalición. Además, también distribuye información crítica, estratégica y táctica a planificadores de guerra así como a combatientes. (National Security Agency , 2015) Para la NSA trabajan muy distintos tipos de especialistas que van desde matemáticos, a hackers, y operadores de puestos de escucha para espionaje, pasando por lingüistas, operadores de polígrafos, programadores o expertos en radiofrecuencia, entre otros.

Como es propio, por su misma naturaleza, la NSA requiere altos niveles de confidencialidad. Para ello cuentan con la misión *Information Assurance*[5] que está destinada a prevenir que los adversarios extranjeros puedan entrar a las redes y acceder a información confidencial o clasificada relacionada con la seguridad nacional. Así como también cuenta con la misión SIGNIT, del inglés *Signals Intelligence*, que recopila información que el gobierno considere interesante sobre comunicaciones extranjeras. Con esta misión también se da apoyo a las operaciones militares. La NSA también habilita la Red de operaciones de Guerra para derrotar a los terroristas y sus organizaciones tanto en territorio nacional estadounidense como en el extranjero. Todas estas acciones, como declaran en su página web oficial, desde el marco de las leyes estadounidense y la protección de la privacidad y las libertades civiles. La NSA existe para proteger la nación y sus clientes pueden contar con ellos para que les provean de lo que necesitan, cuando lo necesiten y donde quiera que lo necesiten.

La NSA trabaja en estrecha colaboración con el Ciber-comando de Estados Unidos (USCC, en inglés *United States Cyber Command*, también conocido como USCYBERCOM). Este comando fue creado en 2010, y tiene como misión el uso de técnicas informáticas con el objetivo de velar por los intereses de Estados Unidos. Es un comando sub-unificado que está bajo el mando del Comando Estratégico de los Estados Unidos. Es tan estrecha esta relación entre ambos actores, que el Almirante Michael S. Rogers es tanto el Comandante del USCC como el director jefe de la NSA/CSS.

«El USCYBERCOM planea, coordina, integra, sincroniza y conduce actividades para dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los Estados Unidos y sus aliados en el ciberespacio e impedir lo mismo a nuestros adversarios» (U.S. Department of Defense, 2010) En el emblema del comando, encontramos el texto «9ec4c12949a4f31474f299058ce2b22a», que está codificado en el algoritmo MD5, y que es parte de un código posible de hackear, y que es la declaración de la misión. (Jelinek, 2010)

[5] En español: seguridad de la información

Por su parte el USCYBERCOM está dentro de los llamados COCOMs, los comandos combatientes funcionales[6], por tanto se le dota al USCYBERCOM de la autoridad de organizar, entrenar y equipar sus propias fuerzas subordinadas, lo que le permitirá estar más preparado y explotar al máximo sus capacidades dentro de este nuevo concepto de guerra.

La mera presencia de un comando militar de ciberguerra (USCYBERCOM[7]) plantea la cuestión de si Estados Unidos lo usa para su uso oficial o se ha usado como arma estratégica para llevar a cabo operaciones militares en el ciberespacio. El USCYBERCOM es el principal responsable de ejecutar las misiones especiales del ciberespacio que se especifican en los planes estratégicos. También tiene como responsabilidad asegurar el derecho a la libertad de acción en el ciberespacio de los americanos, y ayudar a mitigar los riesgos a su seguridad nacional que derivan del crecimiento de la dependencia americana a operar en el ciberespacio. Entre el rango de sus actividades de seguridad, se incluye la concienciación sobre las operaciones en el ciberespacio, tanto para que haya una conciencia como nación, como para advertir sobre posibles riesgos. También se ofrece la posibilidad de ofrecer apoyo a autoridades civiles y a socios y aliados americanos internacionales. Todos los esfuerzos que se hacen desde este comando cibernético son un apoyo a las misiones que luchan contra los ataques DDoDs, defendiéndola nación de cualquier ciberataque o comandos de ciberatacantes, con la finalidad de defender las redes del Departamento de Defensa americano.

Todos somos conscientes de la necesidad de las nuevas tecnologías hoy en día, especialmente en el mundo militar, ya que pueden realizarse operaciones mucho más precisas que antes, simplemente tras el uso de las ciber-capacidades de cada ejército. El uso de los famosos drones para misiones de paz, es lo que nos hace reflexionar sobre hasta qué punto es legítimo el ataque a infraestructuras civiles cuando no estamos en una guerra, ya que esto se viene observando por parte de Estados Unidos, y es una conducta que no podemos distinguir como legítima o no, ya que se ponen en riesgo menos vidas

[6] Functional combatant commands.

[7] Comando de las fuerzas armadas que es subordinado del Comando Estratégico de Estados unidos (United States Strategic Command). Cuya principal misión es la centralización de los comandos que se dediquen a las operaciones del ciberespacio, la organización de los recursos cibernéticos y la sincronización de las redes militares de la defensa de Estados Unidos.

reales de efectivos militares, sin embargo, al no encontrarnos en un periodo de guerra, ¿cuál es el sentido real de los ataques a civiles? Ninguno.

En febrero de 2015 Estados Unidos ha presentado frente a la OTAN su estrategia de seguridad nacional. En esta estrategia los Estados Unidos declaran que uno de los principales objetivos y planes de la estrategia de defensa americana es reforzar la alianza que tienen con Europa a través de esta organización. En este comunicado se hace especial mención a los varios ataques que ha llevado a cabo Rusia al continente europeo y a la necesidad de Estados Unidos de mejorar y estrechar sus relaciones con sus socios europeos y los miembros de la Alianza Atlántica para llevar a cabo sus objetivos. Declara que el hecho de que Europa se vea como un aliado fuerte y seguro es uno de sus principales objetivos, ya que una Europa fuerte podrá ayudar a la mejor consecución de los objetivos dentro del mundo del ciberespacio. Rápidamente el tema de la declaración se desvía a los Balcanes, a Europa del Este, los Balcanes y el Cáucaso, haciendo especial mención a la agresión de Rusia a Ucrania. En conclusión, la declaración que se quiere hacer es que a través de la cooperación Euro-Atlántica y con la continuación de las labores de la OTAN bajo el liderazgo de los Estados Unidos podrá hacerse frente al uno de los mayores riesgos para la seguridad a nivel estratégico que tiene occidente hoy en día, que es Rusia. (Department of Defense of the United States of America, 2015)

El día 1 de abril de este año 2015, el Presidente Barack Obama declaró el estado de emergencia en cuanto a ciberataques mediante un comunicado que declaraba una orden ejecutiva directa. En este comunicado categoriza los posibles ciber-comportamientos que estarán penalizados con sanciones por parte de la jurisdicción americana. Este comunicado principalmente se centra en la categorización de los ataques DDoS, y de los ataques de obtención de información, en especial comercial, y que se mal use para obtener ganancias comerciales. Con este comunicado el presidente Obama también hace un llamamiento a sus principales aliados, como la OTAN y la Unión Europea para que creen los mismos mecanismos de sanciones para este tipo de ataques.

En el mes de abril, el Departamento de Defensa de Estados Unidos realizó una nueva Ciberestrategia debido al pasado estado de emergencia declarado por Barack Obama a principios de mes. (United States Department of Defense , 2015) Este documento pone de manifiesto como los Estados Unidos dependen del Internet y de sistemas de datos en el ciberespacio para llevar a cabo una gran cantidad de servicios críticos para la seguridad nacional. Esta dependencia deja a EEUU vulnerable en cuanto

a riesgos de posibles ciberataques peligrosos, ya que tanto actores estatales como no estatales planean llevar a cabo ataques perturbadores y destructivos en las redes de sus infraestructuras críticas, así como robar propiedad intelectual americana para debilitar la ventaja militar y tecnológica con la que cuenta hoy en día Estados Unidos.

El principal propósito de esta estrategia (la segunda que realiza el Departamento de Defensa americano) es guiar el desarrollo a las fuerzas que se encargan del ciber, a la vez que reforzar su postura en cuanto a ciberdefensa y ciberdisuasión. Principalmente esta ciberstrategia se centra en la construcción de cibercapacidades y modos de organización para las tres principales ciber-misiones del departamento de defensa: la defensa de la información, los sistemas y las redes del Departamento de Defensa; la defensa de los Estados Unidos y sus intereses contra ciberataques con graves consecuencias; la provisión de cibercapacidades integradas para el apoyo de las operaciones militares y los planes de contingencia. Esta estrategia establece cinco objetivos estratégicos y establece objetivos específicos para que consiga el Departamento de Defensa en los próximos cinco años y en adelante.

El primero es la construcción y el mantenimiento de las fuerzas y capacidades para poder llevar a cabo operaciones en el ciberespacio. Por lo que el Departamento de Defensa deberá entrenar a los agentes parte de la "Cyber Mission Force"[8], a la vez que construir organizaciones y comandos efectivos para así poder desarrollar totalmente las capacidades que el Departamento de Defensa requiere para operar en el ciberespacio.

El segundo, la defensa de la red de información del Departamento de Defensa, la seguridad de la información, y la mitigación de riesgos en las misiones del Departamento de Defensa. Para poder llevar a cabo las misiones de la manera más efectiva posible el Departamento de Defensa debe identificar, priorizar y defender sus redes e información más importantes. Así como también tiene que planear y realizar ejercicios para operar en un ciber-ambiente degradado y afectado en el caso de que un ataque a las redes del Departamento de Defensa tenga éxito o en el caso de que se vea afectada la infraestructura crítica de la que depende el Departamento de Defensa para sus planes operacionales y de contingencia.

[8] Fuerza para las Ciber-misiones.

El tercero, prepararse para llevar a cabo la seguridad nacional de Estados Unidos así como defender los intereses vitales de Estados Unidos de cualquier ciberataque que pudiera tener consecuencias importantes. Para ello el Departamento de Defensa desarrollará capacidades de inteligencia y alarma para anticipar prever amenazas; asociarse con organizaciones interinstitucionales clave para preparar la defensa de la nación en el ciberespacio; evaluar la postura de ciber-disuasión del Departamento de Defensa y proveer recomendaciones para su mejora.

El cuarto, la construcción y el mantenimiento de ciber-opciones viables y planear el uso de esas opciones para controlar el incremento de los conflictos y determinar el ambiente de conflictos en todas sus fases. Se debe proveer al presidente de los Estados Unidos con varias opciones viables en caso de la escalada de un conflicto. Estas opciones deberán ser válidas para el desarrollo de cibercapacidades para así poder conseguir con precisión objetivos de seguridad clave y también minimizar la pérdida de vidas y la destrucción de propiedades.

Y el último, el quinto, la construcción y el mantenimiento de sociedades y alianzas internacionales sólidas para la disuasión de amenazas comunes y así aumentar la seguridad y estabilidad internacional. Ya que las tres ciber-misiones del Departamento de Defensa requieren la colaboración cercana con socios y aliados extranjeros. La construcción de socios con capacidades se centrará en regiones prioritarias que incluyen Oriente Medio, Asia-Pacífico y Europa. El Departamento de Defensa se mantendrá siempre flexible y adaptable al medio para la consolidación de las alianzas y asociaciones necesarias, siempre teniendo en cuenta el medio cambiante.

La doctrina rusa.

"It's alarming that military intervention in internal conflicts in foreign countries has become commonplace for the United States."

Vladimir Putin [9]

Para comenzar a hablar del Internet en Rusia, debemos empezar por mencionar la Runet. La Runet es el nombre coloquial que se le da al conjunto de páginas web en ruso. En Rusia, la industria del internet se ha convertido en una industria más que autosuficiente e independiente de las grandes compañías de tecnología estadounidenses. Dichas empresas, como Google o Facebook, sí que tienen una presencia notable en el país. Sin embargo, en Rusia estas empresas no han llegado a dominar el mercado, ya que son empresas rusas las que reinan el mundo de las herramientas de búsqueda, las redes sociales o el sistema de correo electrónico. Un claro ejemplo de esto es Yandex, una empresa rusa que es un buscador que cuenta con el 64% del control del mercado. Yandex no se dedica solamente a la búsqueda de información, sino que cuenta cun un servicio de Mapas de Yandex, (Yandex Maps), Yandex Money (un servicio de pagos en-línea) y Yandex Photos. También es importante destacar que el servicio más importante de correo electrónico en el país es Mail.ru, que pertenece a un grupo llamado Digital Sky Technologies, empresa que ha invertido suculentas sumas de dinero en famosas empresas como Facebook, Zynga o Groupon. (Barnett, 2011)

Sin embargo, las empresas de comunicación por internet no rusas siguen teniendo una presencia importante en el país, por lo que el gobierno ruso, sintiéndose amenazado por la presencia de dichas empresas, decidió crear una legislación para que las empresas extranjeras conservasen la información de los usuarios rusos dentro de las fronteras de Rusia. Las autoridades rusas declararon que esta ley de información personal era una medida necesaria de seguridad para proteger el país de riesgos extranjeros y espionaje estadounidense. Desde fuera podemos verlo como una medida de control de la población dentro de las redes sociales y del mundo de internet.

El 12 de febrero de 2013 Vladimir Putin firmó el nuevo «Concepto de Política Exterior de la Federación de Rusia». Dicho documento sentó las bases de actuación de

[9] En español: «Es alarmante ver como la injerencia en asuntos internos en conflictos de países en el extranjero se ha convertido en una corriente para los Estados Unidos.»

Rusia en cuanto a política exterior al menos hasta el año 2018 y es el sucesor del aprobado por Medvedev en julio de 2008 (sucesor del que formuló Putin en el año 2000 en su primera presidencia). (Ruiz González, 2013) En el Concepto de 2013, se tratan todos los temas relacionados con la política exterior y de seguridad de Rusia. El concepto se estructura de la siguiente manera: La política exterior de la Federación de Rusia y el mundo moderno; las prioridades de la Federación de Rusia para afrontar los problemas globales; las prioridades regionales y el desarrollo y puesta en práctica de la política exterior de la Federación de Rusia. (Putin, Vladimir; Ministerio de Defensa de la Federación Rusa , 2013) Ahora explicaremos cada una de las partes más en concreto.

El principal objetivo de la política exterior rusa, según este concepto de 2013 es asegurar la protección de los individuos, la sociedad y el Estado. Al analizar los puntos básicos del Concepto de 2013, podemos sacar como conclusión que Rusia sigue siendo muy estable en comparación con los conceptos anteriores. En este destaca, en relación con el poder blando y la promoción del idioma y cultura rusos, la necesidad de crear un dialogo constructivo entre civilizaciones dentro de la esfera rusa, ya que parece que la imagen de la Federación de Rusia, por su propia situación interna, está empeorando en los últimos años. (Putin, Vladimir; Ministerio de Defensa de la Federación Rusa , 2013)

En cuanto a su visión del mundo, en el Concepto se hace evidente el descontento ruso con el orden de seguridad mundial que surgió tras la Guerra Fría (con la supremacía en poder de Estados Unidos que se hace ver como la única superpotencia y que se ha hecho valer de esto para resolver conflictos unilateralmente, al margen del Consejo de Seguridad de las Naciones Unidas donde otras grandes potencias como Rusia o China podrían limitar ese ejercicio y poner en duda la supremacía militar).

En relación a las medidas de fortalecimiento de la seguridad internacional podemos observar una clara continuidad en los planteamientos rusos: se pretende la reducción del papel del poder militar y la primacía del Consejo de Seguridad para autorizar el uso de la fuerza (para que no se actúe en ningún Estado con la intención de «proteger»). En cuanto a lo relativo a la cooperación en cuestiones económicas y medioambientales Rusia va detrás de un desarrollo basado en la innovación, debido a su reciente entrada en la Organización Mundial del Comercio (OMC). Rusia debería hacerse incorporado a la Organización para la Cooperación y el Desarrollo Económico (OCDE), sin embargo tras los incidentes en Crimea la OCDE paralizó este anexo. En relación a la

economía rusa siempre se puede observar una tendencia hacia el proteccionismo, lo que dificulta el objetivo de modernizar y diversificar la economía rusa. (Ruiz González, 2013)

En el Concepto de 2013 destaca la constante referencia hacia la lucha contra el terrorismo internacional. Y sobre todo se hace una vehemente referencia en contra del despliegue por la OTAN de un escudo antimisiles balísticos cerca de las fronteras de la Federación de Rusia. Este hecho es algo que se ha convertido en uno de los principales obstáculos en la relación de Rusia con Occidente.

En el apartado sobre las prioridades regionales de Rusia en el mundo, se deja claro la relación de Rusia con cada una de las regiones de interés para Rusia e incluso con algunos Estados Individuales. A grandes rasgos podemos decir que Rusia pretende mantener buenos lazos de cooperación en todos los sentidos con los Estados de su esfera de influencia tradicional y pretende que reinen la paz y la prosperidad en dichos territorios para así poder afianzar los lazos en la región. Mirando más hacia el Oeste, Rusia dice abogar por una asociación trilateral con Estados Unidos y la Unión Europea tanto en materias económicas como de seguridad. Sin embargo, la presencia de la OTAN siempre se ha puesto en medio de la consecución de estos objetivos, ya que el Kremlin reitera su oposición a la expansión de la Alianza a territorios de su esfera de influencia tradicional.

Hacia el Este, se plantea la necesidad de una cooperación Rusia-China-India, sin embargo es algo complicado debido entre los históricos conflictos entre China e India. Sin embargo, las relaciones de Rusia con China son bastante importantes, se coordinan acciones a través de la Organización de Cooperación de Shanghái (OCS) en territorios de Asia Central, además de desarrollarse una cooperación bilateral activa en la gran mayoría de los campos. En relación a Afganistán, Rusia se muestra preocupada por la inestabilidad en la zona, debido a su cercanía y a las posibles consecuencias que dicha inestabilidad tiene para Asia Central en términos del crecimiento del terrorismo islamista y del tráfico de todo tipo de ilícitos. Rusia siempre ha buscado la contribución en la estabilidad de la región, sin embargo hace hincapié en el principio de no-injerencia en los asuntos internos, como declara en todo momento en el Concepto. (Putin, Vladimir; Ministerio de Defensa de la Federación Rusa , 2013)

Como conclusión del análisis del Concepto de 2013 podemos declarar que Rusia ya no tiene aspiraciones de integrarse en Occidente, todo lo contrario. Rusia pretende establecerse como uno de esos nuevos polos de poder aislados cuyos intereses deben

importar, evitando que se repitan los eventos del pasado, donde se ignoraban los intereses rusos, por lo que las tensiones y conflictos escalaban rápidamente.

Por otra parte Rusia también tiene una política estratégica relacionada con el ciberespacio, ellos lo llaman la *Doctrina para la seguridad de la información de la Federación rusa.* De hecho, desde Moscú nunca se utiliza el término «ciber» cuando se dan los comunicados o cuando se realizan las nuevas doctrinas para el mundo del ciberespacio y los ciberataques. Siempre se usa la palabra «información», o el término «informatización». A diferencia de Estados Unidos o China, Rusia no separa los temas relacionados con la información de otros temas como operaciones psicológicas, operaciones de redes o seguridad de las operaciones. Por lo que cada vez que en los párrafos siguientes de este trabajo de investigación se mencione el término información o guerra de información estaremos refiriéndonos el mundo ciber o la ciberguerra.

En general, los documentos oficiales provenientes del Gobierno ruso plantean que el mundo es un lugar oscuro y hostil, un lugar donde la tendencia es una guerra cibernética contra Rusia. Estos documentos también dan unas definiciones de guerra de la información bastante alejadas unas de las otras, ya que ellos separan los temas relacionados con la información de otros temas como se ha mencionado antes. Aunque existe un aspecto positivo frente a esto, y es la creación del concepto de 'estrategia de ciberseguridad', que resalta los aspectos positivos de la sociedad de la información moderna y se plantea para protegerla. En general, el tono de estos documentos es la posición de defensa que siente Rusia frente al resto del mundo, por lo que revelan poca información sobre cómo Rusia pretende llevar a cabo la guerra de la información contra otros Estados, aunque sí que deja entrever muchas cosas.

La estrategia nacional de seguridad es el documento más importante de todos, ya que define todo el sistema de seguridad del país, así como otros documentos importantes, como la Doctrina Militar se realizan bajo las guías que mande el Consejo Nacional de Seguridad. Esta estrategia nacional de seguridad da especial relevancia a la guerra de la información, lo que significa ciberguerra en argot ruso, así como también pone de manifiesto que la estrategia para las guerras de información es una herramienta que los Estados pueden emplear para mejorar su seguridad nacional:

«La guerra de la información es cada vez un fenómeno más grande, y las amenazas al mundo industrial y las zonas en desarrollo, junto con su desarrollo socioeconómico y sus instituciones democráticas están creciendo», dice el artículo 10 de la estrategia de

seguridad nacional rusa. En su artículo 26 declara que toda disuasión estratégica conlleva el desarrollo y la implementación de un sistema complejo de medidas de todas las índoles, (incluyendo la de la información) que pretenden reducir o eliminar los riesgos de posibles acciones destructivas provenientes de cualquier estado (o coalición de estados) que estuviese atacando.

Este documento también expresa el miedo ruso de que otros países estén por delante de Rusia en temas relacionados con la guerra de la información, en especial en los aspectos que conciernen al ejército. En especial en su artículo 30 dice que las amenazas a la seguridad militar son: las políticas de un gran número de países de gran relevancia mundial que pretenden tener una superioridad militar y armamentística, principalmente en cuanto a las fuerzas nucleares estratégicas, a través del desarrollo de medios de guerra de alta precisión, alta tecnología, siempre dedicados a la guerra de la información.

La *Doctrina militar de la Federación Rusa* que se publicó el 26 de Diciembre de 2014, también deja claro que la información es una herramienta que tiene que saber usarse para la seguridad nacional, entre otras. Y también que la guerra de la información predomina en muchas de las acciones que vemos hoy en día, como por ejemplo, en el artículo 12 se identifica como riesgo militar principal el uso de las tecnologías de la información y la comunicación para la consecución de objetivos militares o políticos para así después poder actuar en consecuencia de esa información. Actuar contra el derecho internacional, actuar contra la soberanía, independencia política e integridad territorial de los estados y por tanto atacar contra la paz mundial, la seguridad internacional, y la estabilidad tanto global como regional.

Ya en el año 2000 y debido a la preocupación creciente que se tenía desde el gobierno ruso sobre los aspectos más técnicos de la guerra de la información, se publicó la *Doctrina para la seguridad de la información de la Federación Rusa*. Esta doctrina hace la labor de catalogar los principales riesgos y retos para la seguridad de la información rusa. Este documento sigue en pleno vigor, a pesar de que se hayan publicado muchos otros documentos oficiales que tratan este mismo tema. Todos lo toman a este como referencia y no lo suplantan, sino que lo complementan. Es este documento el que pone de manifiesto el uso de la guerra de la información por otros países en contra de la Federación Rusa. Esta doctrina pone de manifiesto la importancia de las tecnologías de la información para la estrategia militar rusa:

> «Se espera que el desarrollo por varios estados del concepto de guerra de la información conlleve a peligrosas medidas de acción en las esferas de la información de otros países del mundo, para así interrumpir la normalidad y el funcionamiento de los sistemas de información y telecomunicaciones, pudiendo obtener acceso no autorizado a los recursos de información que tengan almacenados. »
>
> Se declara en la sección 3 de esta doctrina.

En general, dentro del ejército ruso existe un gran debate sobre qué papel debería tener la información y las guerras de la información en general. Sin embargo, y como ya hemos visto anteriormente, es un tema que está presente entre los principales retos a los que debe enfrentarse esta fuerza militar a diario. Los más pesimistas siguen pensando que los medios tradicionales, son los que siguen guiando las guerras hoy en día, sin embargo existe otra rama del ejército ruso que ve claramente que eso no es así, como por ejemplo la anexión ilegal de la Península de Crimea, que si bien estuvo apoyada por algunos militares rusos, para poder llevarse a cabo necesitó de la guerra de la información para poder llevarse a cabo. Es importante para ellos porque esto les da un poder que anteriormente no tenían, y ni siquiera requiere sangre o tanques, si no tecnología y mano de obra cualificada. Por suerte, en Rusia cuentan con un número desconocido de expertos y hackers, los mejores del mundo, dicen algunos.

En el pasado mes de abril, desde la oficina de prensa del Consejo de Seguridad de Rusia se declaró que Rusia «ha comenzado el desarrollo de la nueva edición de la Doctrina de Seguridad de la Información de la Federación Rusa. La actualización de los enfoques para la protección de los intereses nacionales en el ámbito de la información en función de las realidades contemporáneas se convertirá en una base de la nueva edición de la Doctrina» (RT.com, 2015)

Por último, la creación de las *Russian Information Troops* [10] se dio después de los sucesos en Georgia del año 2008 que se explicarán más adelante en este trabajo. Después de que se revisasen las acciones que se llevaron a cabo en Georgia, desde el Kremlin, rápidamente se dieron cuenta de que habían fallado tanto en el área de la tecnología de la información como también en el aspecto más psicológico de la guerra de la información,

[10] En español: Tropas rusas de la información.

y estas dos áreas son las más importantes para el pensamiento estratégico militar ruso. La respuesta a este fallo, después de mucho sopesarlo, fue la creación de las Tropas de la Información, un comando totalmente dependiente de las Fuerzas Armadas rusas. Dicho comando cumpliría con las necesidades del ejército en cualquiera de sus operaciones militares relacionadas con el mundo de la información. Incluso se crearon unas fuerzas especiales de la información dentro del mismo comando del ejército, dentro de este comando se les prepararía para poder actuar de manera efectiva en operaciones bajo unas condiciones de crisis inmediata. Dichas operaciones entrarían en el espectro completo de los temas posibles en las operaciones de la información. (Giles, 2011)

Igor Panarin, analista político de la antigua KGB y actualmente profesor del Ministerio del Exterior de Rusia y experto en relaciones Rusia-Estados Unidos, fue de los primeros en destacar la necesidad de unas tropas especiales para la información, que estuvieran preparadas para las ejecución de operaciones efectivas bajo las condiciones de una potencial crisis. (Panarin, 2008) Declaró que el objetivo de estas operaciones deberían cubrir todos los aspectos de las operaciones de información, dijo que «el objetivo es….crear centros en los que se puedan detectar ataques de hackers desde el territorio extranjero.» (BBC Monitoring , Russian TV highlights hacker attacks on Georgian sites, 2008)

Más tarde, tras la creación de las tropas, declaró que el personal de las *Information Troops* debería estar compuesto por diplomáticos, expertos en informática, periodistas, escritores, publicistas, traductores, operadores de comunicación, diseñadores de páginas web y hackers entre otros. Para poder construir contramedidas de información es necesario construir un centro para la determinación de entidades de información crítica e importante del enemigo, que incluya como eliminarles físicamente y como llevar a cabo una guerra electrónica, una guerra psicológica, la creación de contra-propaganda sistémica y el entrenamiento de hackers para poder llevar a cabo todas las operaciones en la red. (BBC Monitoring, 2008)

Podría decirse que las Russian Information Troops son el equivalente soviético del USCYBERCOM, ya que es un organismo que depende del ejército, y cuya principal misión es velar por la seguridad informática nacional. Sin embargo, las Russian Information Troops se crearon en un contexto de guerra física, y por tanto tienen una naturaleza holística más hostil y ofensiva que el USCYBERCOM, que es por naturaleza

un elemento de defensa, pero con las capacidades suficientes para llevar a cabo una ofensiva.

Casos EEUU

El fenómeno Wikileaks (guiado por su fundador Julian Assange).

En abril de 2010 se publicase un vídeo clasificado en el que se puede ver cómo helicópteros Apache americanos abrían fuego contra civiles iraquíes. Al poco tiempo se publicaron los «*Diarios de Guerra de Afganistán»,* con varias decenas de miles de mensajes clasificados que contenían información que se había intercambiado hasta el momento por las tropas de Estados Unidos hasta esa fecha. Después a esto le siguió el "Irak War Logs", y después los comunicados entre el departamento de estado estadounidense con sus embajadas en los que se filtraban secretos diplomáticos, lo que fue denominado como "CableGate". El caso de WikiLeaks es un clarísimo ejemplo de cómo puede la información propagarse a través de Internet con una gran facilidad, y también de cómo evitar esta propagación es una tarea casi imposible.

Como conclusión del fenómeno de WikiLeaks podemos decir que ha sido un referente en cuanto a fugas de información, con ello queda de manifiesto que todas las medidas de seguridad resultan inútiles si las personas que manejan la información tienen malas intenciones y no tienen un compromiso. También se ha comprobado que la fuga de información afecta de forma directa a la seguridad nacional de un estado, poniendo no solo en peligro la estabilidad nacional e internacional como la vida los militares y los ciudadanos. Tomando aparte los factores éticos de estas acciones, queda de manifiesto la debilidad y fragilidad de las organizaciones nacionales e internacionales contra este tipo de comportamientos. De ahí que en general exista una gran necesidad de crear e implantar nuevas políticas de seguridad.

Edward Snowden y la NSA.

En relación con el fenómeno de WikiLeaks, debemos destacar las filtraciones que realizó el empleado de la Agencia Nacional de Seguridad americana (NSA) Edward Snowden sobre secretos de estado norteamericanos altamente clasificados. Las filtraciones revelaban como el Gobierno de los Estados Unidos forzó al gigante de las telecomunicaciones, Verizon, a entregarle las conversaciones telefónicas de millones de ciudadanos americanos. La segunda declaración fue para revelar la existencia de un programa llamado PRISM, que recogía información de internet de las principales compañías de internet estadounidenses (entre ellas Google, Facebook o Apple). Las

reacciones que estas revelaciones causaron en la comunidad internacional fueron de alarma y descontento con los servicios de seguridad y defensa estadounidenses.

Y como en el caso de WikiLeaks, nos muestra la rapidez con la que puede difundirse la información a día de hoy, así como la vulnerabilidad de los Estados. Lo más importante de este caso es que fue la NSA, dependiente del departamento de Defensa de los Estados Unidos quien solicitó estas escuchas y quien creó el sistema de transcripción y búsqueda de información relevante para la seguridad nacional, así como para el uso de estas informaciones como parte de la estrategia de seguridad del país. Este caso nos demuestra la capacidad de la NSA para el control del ciberespacio y la información. Estos actos podrían considerarse como actos de ciberespionaje por parte del Gobierno de Estados Unidos a sus propios ciudadanos para conservar la seguridad nacional.

Stuxnet.

Desde principios del nuevo siglo pudimos observar que las infraestructuras críticas eran posibles víctimas de ataques debido a la importancia de lo que protegían. Ya en el año 2000 un empleado cabreado de la mayor extractora de gas natural del mundo, *Gazprom*, instaló un troyano que hacía posible acceder a un panel de control de uno de los centros, y esto casi causa un gran desastre natural. Y como este ejemplo se han visto muchos desde entonces. Sin embargo, es Stuxnet quien nos hizo estar realmente alerta. Stuxnet se descubrió por primera vez en junio de 2010, por la empresa VirusBlokAda, procedente de Bielorrusia, sin embargo se cree que muchos de sus componentes ya fueron gestados un año antes. Stuxnet fue el primer prototipo real de «ciber-arma» que dio el pistoletazo de salida a la nueva guerra armamentística del mundo. Se sabe que la finalidad con la que se concibió fue con la de obtener información de los programas nucleares de Irán a través de sus sistemas SCADA[11]. El objetivo de Stuxnet era instalar un *rootkit*[12] en los sistemas PLC en las configuraciones que usan la mayoría de las infraestructuras nucleares en Irán. Existe una gran controversia sobre quién fue su creador. Algo está claro, los creadores de Stuxnet eran profesionales que estaban altamente cualificados en el sector de ciberseguridad y también que fueron contratados para atacar un objetivo muy

[11] Acrónimo de Supervisory Control And Data Adquisition (Supervisión, Control y Adquisición de Datos), que permite controlar y supervisar procesos industriales de manera remota, a distancia.

[12] Programa que oculta la presencia de malware en el sistema. (definición de Kaspersky Lab)

claro y concreto, Irán. A pesar del debate, muchos opinan que vino directamente de los gobiernos de Israel[13] y Estados Unidos[14].

Otros.

Para demostrar la hipótesis de este trabajo también se van explicar otros casos previos en la historia militar de Estados Unidos:

- En 1982 un sistema de control de ordenadores que se robó de una empresa canadiense por espías soviéticos causó que un gaseoducto soviético explotase. El código que controlaba el sistema fue modificado por la CIA para que incluyese una bomba lógica, lo que conllevó al cambio de la fuerza de las bombas de surtido, causando así la explosión. (Murphy, 2010)
- En 1998 para que Estados Unidos y las fuerzas de la OTAN pudiesen llevar acabo de manera satisfactoria los bombardeos contra los objetivos serbios en Kosovo, los Estados Unidos tuvieron que hackear el sistema de defensa del aire serbio para engañar al sistema de control de tráfico aéreo serbio. La misión se cumplió con éxito, y tal fue el éxito que los Estados Unidos se negaron a seguir hackeando en el sistema porque se corría el riesgo de que se hiciese daño a la población civil. (Murphy, 2010)

[13] La creencia de la implicación del gobierno de Israel viene por las referencias que el código de Stuxnet hace a la palabra "Myrtus", que en hebreo significa Esther, y existe un libro que se llama el Libro de Esther que relata un complot persa para destruir el estado de Israel.

[14] El movimiento de Anonymous asegura que está en posesión del código de Stuxnet, y que lo obtuvo directamente por una empresa de seguridad americano, y que les aseguraron que éste fue desarrollado conjuntamente por Estados Unidos e Israel.

Casos Rusia

Al comenzar a hablar del caso ruso es importante mencionar el caso de la "*Russian Business Network*" (a partir de ahora RBN). Según expertos en seguridad informática esta empresa con base en San Petersburgo fue uno de los puertos mundiales para páginas web que se dedican a la pornografía infantil, robos de identidad y envíos de spam. Esos mismos expertos declararon que las autoridades del gobierno ruso no pusieron de su parte en las labores de investigación para intentar terminar con la empresa. La empresa se dedicaba principalmente a vender alojamiento a personas que estaban involucradas con actividades criminales. (Bizeul, 2007) Lo más destacable de la RBN es que no importaba cual fuera la actividad a la que se dedicaba la página web que requería sus servicios o cuales quera que fueran sus objetivos, la RBN siempre encontraría la manera de satisfacerles. (Bizeul, 2007)

El 6 de noviembre de 2007 la RBN desapareció de internet, sin dejar rastro de sus operaciones, aunque realmente no se sabe si realmente desapareció o simplemente encontró una manera de volverse invisible a los ojos de los rastreadores de seguridad informática, ya que la RBN cuenta con jóvenes con un gran potencial informático. La compañía ya se había vuelto invisible para los ojos de los rastreadores en más de una ocasión, así que no se sabe que esperar al respecto, y como ya se ha mencionado antes, los ataques en Georgia en 2008 se creen que tuvieron su origen en redes basadas en la RBN, ya que seguían su mismo método de operaciones.

El futuro de la RBN nunca estuvo claro, pero a día de hoy, años después de su desaparición de Internet, no se han encontrado rastros de ella. Sin embargo, hay varias corrientes de pensamiento al respecto: la primera es que los hackers rusos de la RBN se mudaron a China, ya que se encontraron varias direcciones IP que realizaban operaciones parecidas a las de la RBN dentro de las redes chinas, ya que se cree que China podría darle a la RBN mayores recursos económicos y tecnológicos, mayores sistemas de seguridad y también una mayor lista de posibles clientes con intenciones maliciosas con respecto al cibercrimen organizado. Otra de las teorías que se mantienen es que la red se ha quedado inoperativa, pero bajo los mandos de las autoridades de la federación rusa.

Hay que mencionar el grupo juvenil *Nashi* o también conocido como juventudes putinistas. Este grupo de juventudes es un movimiento político en Rusia que se declara como un movimiento anti-fascista. En 2008 este grupo se separó en varios grupos diferentes. Entre esos grupos encontramos el grupo Nashi 2.0, que hasta el año 2012 se

dedicó a hacer propaganda vía online (Twitter y otras redes sociales) y que contaba con más de 15.000 seguidores.

Centrándonos más en el tema de este trabajo de investigación, debemos comenzar por señalar el caso de Estonia en 2007. Estonia y Rusia tienen una larga historia de momentos tensos en sus relaciones bilaterales, ya que los problemas entre estos pueblos tan diferentes se remontan a hace cientos de años, antes de la creación de los Estados modernos. En 1940, y durante la Guerra Fría, el Kremlin recolocó a cientos de miles de nacionales rusos en el territorio de lo que hoy en día es Estonia. El objetivo de esas migraciones en masa tenía dos caras: aumentar la cohesión del Bloque del Este y «rusificar» la cultura de Estonia. Después del final de la Guerra Fría y de la disolución de la Unión Soviética, el gobierno de Tallin implementó medidas para minimizar las influencias rusas en la cultura estonia. A pesar de que Estonia se unió a la OTAN en 2004 y con ello ratificó y recibió el Artículo 5 de la Alianza Atlántica de garantía de seguridad mutua, se continuaba pensando que Moscú tenía algún plan paralelo. Después de años intentándolo, Estonia al fin recibió los planes de contingencia de la OTAN para proteger el país en caso de que Rusia intentase llevar a cabo una invasión de su territorio. Al margen de estos planes enviados por la OTAN, Estonia también creó planes nacionales de ciberdefensa contra posibles agresiones rusas.

Los ciberataques contra Estonia ocurrieron justo en el momento con más tensiones entre la población de Estonia y la minoría rusa del país. El 30 de abril de 2007, el gobierno cambió de lugar una estatua clave que rememoraba la Unión Soviética, decisión que molestó a la población de habla rusa que vivía en el país, que era alrededor de 26 por ciento de la población de Estonia en el año 2007. Para la población de habla e identidad rusa esta estatua del «Soldado de Bronce» representaba la libertad y era un gran signo de identidad. Su recolocación se vio como un signo de mayor marginalización para la identidad de esta minoría étnica rusa, mientras que para los estonios fue un signo liberador ya que la estatua para ellos era un claro símbolo de la opresión vivida durante el período que vivieron dentro de la esfera de la Unión Soviética.

Las protestas callejeras contra la degradación del Soldado de Bronce derivaron entonces en ciberataques enviados contra organismos públicos y entidades privadas como bancos o periódicos. Cabe destacar que Estonia es uno de los países que más usan Internet en sus actividades cotidianas: las últimas elecciones celebradas en el país (2011) fueron las segundas en celebrarse sólo por Internet en Estonia. «La web del Gobierno recibe en

condiciones normales entre 1.000 y 1.500 visitas al día; en el momento más álgido de los ataques, en la primera semana de mayo, se llegaron a recibir entre 1.000 y 1.500 por segundo», explica Mikko Maddis, portavoz de Defensa. El portavoz de defensa dejó claro que estos ataques habían desbordado las capacidades del sistema.

Durante el período del 27 de abril al 18 de mayo las páginas web de las infraestructuras estatales, de dos de los bancos principales, de los principales partidos políticos así como de todos los ministerios del gobierno dejaron de funcionar debido a diversos ataques de denegación de servicio distribuido (DDoS). Incluso, hubo un momento en el que los hackers desactivaron el servidor del correo electrónico del parlamento. Tanto oficiales estonios, como el Ministro de Exteriores estonio Urmas Paet acusaron rápidamente a Rusia de la perpetración de los ataques, sin embargo, los expertos de la Comisión Europea y de la OTAN no fueron capaces de encontrar evidencias creíbles de que el Kremlin estuviese implicado en los ataques DDoS. (Martínez de Rituerto, 2007)

Desde la Unión Europea y la OTAN se calificaron los ataques como «inaceptables» al analizar los hechos y las consecuencias que trajeron los ataques tanto al gobierno estonio como a la sociedad civil. Estonia pidió a los ministros de Exteriores de la Unión Europea que intentaran solucionarlo, pero desafortunadamente los ciberataques no están regulados totalmente. El artículo 5 del Tratado del Atlántico Norte establece que un ataque armado contra uno o varios aliados, en Europa o en América del Norte, será considerado como un ataque dirigido contra todos. Por ejemplo: un ataque a un aeropuerto o un puerto son actos de guerra, sin embargo, los ciberataques no estaban en la época considerados como ningún tipo de ataques, y realmente no existía un protocolo para ello. Hoy en día se ha planteado ya en varias ocasiones la necesidad de una tipificación más concreta de los tipos de ataques dentro del contexto de la OTAN, ya que cada día los ataques cibernéticos son más comunes, sin embargo, es complicado que esto avance, y por consiguiente, la creación de una jurisdicción internacional que a ello acompañe. A ello hay que sumarle la imposibilidad e improbabilidad que existe de poder sorprender a un ciberatacante en el momento en el que está realizando dicho ciberataque, ya que esa es la única manera de saber exactamente de dónde procede; una vez que el hacker está offline ya no puede controlarse. (Martínez de Rituerto, 2007)

El caso de Estonia es muy particular, porque el Internet es parte de la vida social y gubernamental de país hasta puntos exagerados. Podría decirse que en Estonia se vive en una e-sociedad y por lo tanto se tiene un *e-government*. Esto es tal, que no solo se vota

online, sino que también se pagan todos los impuestos de manera electrónica, y la banca online de todo el país está desarrollada con micro-pagos móviles. Tanto es así que también las infraestructuras del gobierno se manejan de forma totalmente de forma electrónica. (Gobierno de Estonia , s.f.)

Los ciberataques tuvieron consecuencias principalmente para las páginas web del gobierno, ya que dejaron de funcionar. El banco más importante del país tuvo que cerrar sus accesos online para poder frenar los ataques y que no se extendiesen a más infraestructuras. Se hizo un gran esfuerzo por parte de los ISP de otros países para poder alcanzar la capacidad de frenar los ataques y así poder terminar con ellos para que no afectasen otras infraestructuras críticas estonias y para que no traspasasen las fronteras del país. (Tikk, Kaska, & Vihul, 2010) Los trabajadores del gobierno declararon que tuvieron que «volver a la edad de piedra» al tener que decirles a los demás trabajadores que tenían que comunicarse a través de «teléfonos o faxes». (Martínez de Rituerto, 2007)

Para seguir comentando el caso ruso, hablaremos del caso de Georgia en 2008. Semanas antes de que se lanzasen las primeras bombas en Georgia, se pudo observar cómo se llevó a cabo un ciberataque. Lo más destacable de dicho ataque fueron las grandes cantidades de paquetes de datos que recibían las páginas oficiales del gobierno de la República de Georgia que contenían el siguiente mensaje: «*ganar+amor+en+Rusia*». Fue un experto en seguridad informática estadounidense quien ya el 20 de julio de 2008 comenzó a darse cuenta de los ataques. Dichos ataques venían cargados de una gran cantidad de ataques DDoS, que tuvo como consecuencia que cayeran los servidores gel gobierno georgiano.

Varios investigadores de Shadowserver, que es un grupo de voluntarios que rastrea la actividad maliciosa en la red, realizaron un informe señalando que la página web del ahora expresidente georgiano Mijail Saakashvili había quedado inutilizada durante 24 horas debido a múltiples ataques DDoS. En un principio se indicó que esos ataques estaban basados en un servidor en los Estados Unidos, sin embargo esto después fue desmentido. Este ataque sirvió como prueba inequívoca para demostrar que los siguientes ataques que se perpetraron a las instituciones georgianas estaban relacionados. Y no solo estamos hablando de ciberataques, sino que también hay que señalar el bombardeo que se llevó a cabo en la región georgiana de Osetia. (Markoff, 2008)

En ese momento no estaba claro quién estaba directamente detrás de los ciberataques a Georgia. A pesar de eso el Gobierno georgiano no tardó en acusar a Moscú.

Desde el Kremlin siempre han negado rotundamente la complicidad con los ataques. A través de ordenadores del gobierno georgiano también se atacaron a los medios de comunicación principales y las más importantes compañías de transportes justo después de la entrada de las tropas rusas en la provincia georgiana de Osetia del Sur.

El Banco Nacional de Georgia también se convirtió en objetivo para los ciberatacantes. Su página web fue infectada con imágenes de dictadores del Siglo xx a la vez que con imágenes del por entonces presidente de Georgia, Mijail Saakashvili, y junto a esas imágenes aparecían frases despectivas hacia su persona, así como insinuaciones de que él también era un dictador. De nuevo, desde Tiflis se acusó práticamente de inmediato al Kremlin como responsables de los ciberataques. Y, de nuevo, Rusia negó cualquier tipo de relación con los mismos.

Aparte de los ataques DDoS que paralizaron la infraestructura de internet limitada que tiene Georgia, se re-direccionaron grandes masas de datos de internet desde empresas de telecomunicaciones rusas, e incluso se creó una página web en ruso que se llamaba «stopgeorgia.ru» desde la que se encontraron rastros de los ataques DDoS y desde la que se ponía a disposición de usuarios menos avanzados la descarga que hacía falta para enviar el virus DDoS a las infraestructuras georgianas. Poco después se descubrió que esas masas de información que creaban los ataques provenían de la RBN (Russian Business Network), la banda criminal en forma de empresa con sede en San Petersburgo, aunque esta ya se creía agotada desde 2007. Se encontraron programas maliciosos que se conocen como botnets (explicado anteriormente), que estaban mandando flujos de información inútiles a los ordenadores de la infraestructura política georgiana.

Las instrucciones de como entrar en las páginas web del gobierno georgiano se distribuían en páginas web en ruso y también en blogs, y también se distribuyeron listas de páginas web georgianas que eran vulnerables a ataques remotos por inyecciones SQL, facilitando el acceso a estas páginas y su vulnerabilidad. Esto es similar a lo que pasó en el caso de Estonia, cuando las instrucciones de cómo hacer crecer el ataque se distribuyeron en páginas rusas solamente en ruso. Una pequeña diferencia entre los dos ataques es que los que se llevaron a cabo en Georgia se extendieron tanto que no sólo se llevaron a cabo desde suelo ruso, sino que hackers desde todos los rincones del mundo los llevaron a cabo también. Lo que sugiere que una botnet o diferentes botnets estaban detrás de estos ataques. De lo que no cabe duda es que los hackers tienen que ser de procedencia Rusia, porque los ataques se realizaban en ruso.

La gran diferencia entre los ataques que sufrió Estonia con los que sufrió Georgia es en la dependencia que tienen los georgianos del internet. En comparación, Estonia tiene 52 usuarios de internet por cada 100 habitantes, es una e-sociedad, como ya hemos dicho antes; mientras que Georgia solamente cuenta con 7 usuarios de internet por cada 100 usuarios. Este número relativamente bajo de usuarios de internet muestra la falta y la necesidad de infraestructuras de telecomunicaciones más avanzadas en las infraestructuras gubernamentales. Y, aunque, el número de internautas georgianos ha crecido en los últimos años de manera progresiva, la Comisión Nacional de Comunicaciones de Georgia (la autoridad reguladora georgiana del sector de las comunicaciones electrónicas) declaró que en el año 2007 había 7 internautas por cada 100 habitantes porque en 2006 con la llegada de la banda ancha a Georgia el número de internautas creció ese año un 81%. (Carr, 2011)

El principal problema de Georgia es por tanto la dependencia de interconexiones con Rusia, ya que por su situación geográfica Georgia no tiene muchas otras opciones de importar las redes de internet, sus opciones reales son Turquía, Armenia, Azerbaiyán y por supuesto Rusia. Por lo que realmente Georgia depende de Rusia para sus conexiones, ya que la mayoría de sus redes pasan por Rusia, más que por cualquiera de los otros países vecinos. La opción de desviar las redes para que pasen por otros países es prácticamente imposible para Georgia, lo que sigue condicionando sus relaciones.

También, como con el caso de Estonia, no se puede asegurar que el Gobierno ruso estuviese detrás de los ataques, pero sí se puede decir que el gobierno ruso sabía de los ataques, y no solo hizo nada para detenerlos, sino que les parecieron bien, ya que les ayudaban a conseguir sus intereses políticos y militares. Podemos alegar esto ya que ambos conflictos tienen como fondo una colisión a gran escala de intereses entre el país que sufre el ataque y las autoridades rusas. Así como también la coordinación y el apoyo a los ataques fueron principalmente mandados en idioma ruso y se llevaron a cabo desde o bien foros de Rusia o desde ambientes cercanos a Rusia. (Mshvidobadze, 2013)

Los investigadores han demostrado que la página web «stopgeorgia.ru» está relacionada con varias actividades criminales, como la falsificación de pasaportes o el duplicado de tarjetas de crédito robadas, etc. Todas estas actividades criminales son las que normalmente serían perseguidas por las autoridades, ya que son actividades ilegales, sin embargo, las autoridades Rusas se han mostrado sorprendentemente inactivas a la hora de detener a las personas responsables de las actividades ilegales. (Carr, 2011)

Los efectos de los ataques fueron terribles para las compañías de telecomunicaciones georgianas, ya que no pudieron dar servicio durante varios días. Prácticamente todas las compañías de telecomunicaciones georgianas fueron afectadas por los ataques porque no pudieron responder todas las peticiones que mandaban los ataques DDoS. Aunque si se mira desde otra perspectiva, el gran impacto de los ciberataques y la gran repercusión que tuvieron llamaron la atención de los medios de comunicación internacionales. Y esta repercusión en los medios de comunicación ayudó a Georgia en el momento en que tras la guerra se necesitó ayuda internacional. Pero, sin duda, la consecuencia más importante de estos eventos fue que la comunidad internacional se mentalizó de la realidad de estos eventos y comenzó una nueva era de investigaciones y no solo fueron beneficiosas para la comunidad internacional, sino que para Georgia también. (Carr, 2011)

El caso de Ucrania, el más reciente de todos los casos, comenzó como todos los demás casos de infiltraciones, con ataques DDoS seguido por un bloqueo de las comunicaciones telefónicas. Ukrtelecom informó que sus instalaciones fueron allanadas a principios de marzo de 2014 por hombres armados que manipularon el cableado de la fibra óptica, lo que causó la pérdida del servicio de algunos usuarios. Pero como en todos los casos anteriores, las autoridades de los servicios de seguridad rusos no admitieron nada al respecto, y en este caso en particular no han emitido comentario alguno sobre el incidente. Sin embargo, los expertos en seguridad internacional hablan de que Rusia podría estar actuando con moderación usando sus ciber-capacidades. (Bender & Kelley, 2014) Esto vuelve a dejar en entredicho la falta de conocimiento que tiene la comunidad internacional en general con respecto a cuales son las ciber-capacidades reales de Rusia.

Para los ataques realizados contra Ucrania, Rusia utilizó a sus mejores hackers. En marzo del 2014 BAE publicó un informe que hablaba de la complicada campaña de ciberespionaje que tenía como objetivo Ucrania en los primeros momentos de 2014, este programa se llamó el programa SNAKE. (BAE Systems Applied Intelligence, 2014) Este programa había funcionado durante ocho años, y podría definirse como un conjunto de complejas técnicas que evitaban las defensas de los países de destino y que dotaban a los hackers que atacaban con ello canales de comunicación cubiertos y fuera de peligro.

Dentro de la campaña SNAKE se incluyó un malware bastante potente denominado Uroburos, que hacía que los hackers fuesen capaces de controlar ordenadores, cerrar programas, robar enormes cantidades de información y traficar con

ella a través de internet. También parecía estar autorizado por ciberexpertos rusos, aunque como todos los tipos de ataques es imposible determinar a ciencia cierta la implicación del gobierno ruso, y por tanto saber si estaban detrás de ellos.

Igual que en el caso de Georgia, Ucrania comparte la mayoría de sus infraestructuras y redes informáticas con Rusia, por lo que desde Moscú podrían denegar los ataques alegando que si les atacasen, también podría haberles afectado a ellos mismos y sus infraestructuras. Desde los ataques en Georgia, encontramos un nuevo modo de atacar cibernéticamente, a través del envío de propaganda política que cuente con un gran poder de destrucción, causando un gran daño a la población civil. Se ha empezado a hablar de una «plantilla georgiana», ya que los ataques son tan similares que puede decirse que se siguió el mismo patrón. (Harris, 2014)

La facilidad con la que las fuerzas rusas entraron en los sistemas de telecomunicaciones se debe a que muchos ex países soviéticos cuentan con la tecnología llamada SORM ("System for Operative Investigative Activities") que es el sistema que llevan las infraestructuras del servicio de seguridad federal, la FSB, que es la sucesora de la KGB. Este sistema SORM salió a la luz este pasado mes de marzo, cuando se comunicó que las compañías de telecomunicaciones estaban siendo vigiladas y controladas por fuentes externas al gobierno ucraniano. (Recorded Future , 2014)

Sin embargo, podemos ver una clara diferencia con respecto a los ataques en Georgia del 2008. En los ataques a Georgia los foros de hackers rusos se dedicaron activamente a reclutar voluntarios para que enviasen ataques a Georgia. Con respecto a los ataques en Ucrania, muchos de esos hackers estaban enfadados con Putin, y apoyaban a sus amigos Ucrainanos. Otros, incluso, intentaron poner en evidencia al gobierno ruso al hacer pública información confidencial de los servidores del gobierno ruso que demostraba que estaba relacionado con los ataques.

Conclusiones

Tras llevar a cabo este trabajo de investigación, hemos de concluir repitiendo la idea de que a día de hoy convivimos en un mundo cada vez más interconectado en todos los sentidos, y en especial en el ámbito de las comunicaciones. Cada vez es más sencillo comunicarse con otras partes del mundo, por lo que este mundo de comunicaciones se vuelve más y más complejo. Debido a esta complejidad del sistema, hemos de tener en cuenta el hecho de que vivimos a merced de los ataques informáticos.

Los ataques informáticos es por definición cualquier hecho malicioso que conlleve al uso de internet como herramienta. Hoy en día cada vez es más común encontrarse con todo tipo de delitos informáticos. Esto es debido a la gran cantidad de actores que los cometen y tipos de ataques que se pueden llevar a cabo. Es muy complicado, por no decir imposible, sorprender a un ciberatacante en el momento en el que está llevando a cabo la acción, y esa es la única manera que existe realmente de poder atribuir dichos ataques a la persona que los comete. Los ciberatacantes no entienden de fronteras ni de legislaciones, ya que Internet no entiende de ello. Es por ello por lo que debemos resaltar la importancia del mundo ciber para las relaciones internacionales. Ya que los ciberataques afectan a todos los ámbitos de la política internacional y a los de las relaciones internacionales.

Por norma general son las empresas o las infraestructuras críticas de los estados los receptores de los ciberataques, sin embargo, corremos el riesgo de que estos ataques termine por sufrirlos la sociedad civil, ya que las infraestructuras de los Estados se diseñan para su protección. Entre los actores más comunes de ciberataques podemos encontrar desde actores estatales a grupos organizados no-estatales. En este trabajo nos hemos centrado en el uso de ciberataques como herramienta para las relaciones internacionales por parte de ciertos actores estatales: Estados Unidos y Rusia.

Estados Unidos y Rusia son dos grandes potencias a nivel mundial, y como tal, han hecho acopio de la importancia del mundo ciber para las relaciones internacionales y han incluido dentro de sus doctrinas de estrategia para la política exterior unos apartados explicando su postura con respecto al desarrollo de capacidades para el mundo ciber. Tal importancia le han dado que ambos países han informatizado sus ejércitos, y han creado comandos de actuación para la defensa de la seguridad nacional, así como para la consecución de sus objetivos políticos de manera más precisa gracias a los avances informáticos.

Como hemos podido observar durante el desarrollo de este trabajo de investigación, Estados Unidos ha ido desarrollando sus capacidades relacionada con la ciberseguridad desde hace varias décadas como hemos podido comprobar con los ejemplos de Kosovo y la explosión del gaseoducto soviético. Desde el año 2010 podemos comprobar como la necesidad de poner de manifiesto la importancia de la ciberseguridad ha estado más presente en Washington. Ejemplo de ello es la Estrategia para las Operaciones en el Ciberespacio del Departamento de Defensa estadounidense, que es una declaración de intenciones. Sin embargo esta estrategia es bastante defensiva, y se centra en el desarrollo de capacidades para la defensa de la seguridad nacional. En contraposición a esta estrategia, hemos podido ver desde el comienzo de la guerra del terror como el uso de drones ha servido para la eliminación de objetivos terroristas importantes.

El día 1 de abril de este año, el presidente de los Estados Unidos declaraba que el país estaba en un estado de emergencia ante ataques informáticos, por lo que a finales de ese mismo mes se presentó ante la OTAN para después hacerse pública la nueva Ciberestrategia del Departamento de Defensa de los Estados Unidos. Esta nueva estrategia es mucho más ofensiva que su antecesora, y pone de manifiesto la necesidad de una mejor cooperación internacional al respecto como novedad.

En Estados Unidos encontramos con dos grandes bloques de ciberseguridad, por una parte, a nivel federal, encontramos el cibercomando del FBI, que tiene que informar siempre a las organizaciones a nivel nacional. Este comando se centra en especial en robo de identidad y capital, por lo que puede decirse que se dedica más a la protección de los ciber-intereses de la sociedad civil que a los del ejército. Por otra parte, a nivel nacional nos encontramos con la Agencia Nacional de Seguridad (NSA) que es la principal encargada de la seguridad de las infraestructuras críticas del gobierno estadounidense. Para justificar la hipótesis de este trabajo hemos seleccionado la figura del USCYBERCOM. Este comando cibernético es dependiente de la NSA y a su vez mantiene grandes lazos con el ejército estadounidense, ya que es parte del Departamento de Defensa. El USCYBERCOM es el principal encargado de llevar a cabo las misiones estratégicas para defender la seguridad nacional tanto dentro como fuera de su territorio.

Los casos comentados en este trabajo de investigación, nos muestran como el ciberespacio estadounidense está militarizado y el control de la información que se lleva a cabo desde Washington es bastante elevado. Así como ponen de manifiesto la

vulnerabilidad de los Estados a la posible filtración (en este caso desde dentro de su propia organización) de información crítica y confidencial para la seguridad nacional. Y como Estados Unidos ha usado desde hace décadas su presencia en el ciberespacio como una herramienta más de las relaciones internacionales.

Rusia, por su parte ha demostrado en la última década que sus capacidades cibernéticas son mayores de lo que los expertos en este ámbito esperaban. Sí que es cierto que ya en el año 2000 se publicó la Doctrina para la seguridad de la información de la Federación Rusa. Dicha doctrina demostró la importancia que desde principio de siglo han tenido las nuevas tecnologías de la información para el gobierno de Moscú. Esta doctrina puede describirse como defensiva para la seguridad nacional rusa. Sin embargo, y debido al descontento que tiene la Federación con respecto al Orden Internacional vigente desde el fin de la Guerra Fría y a la concepción de que el mundo es un lugar oscuro y hostil que está cibernéticamente en contra de Rusia, hemos podido ver como otros países de la antigua Unión Soviética han sufrido ciberataques que provenían de territorio ruso. A pesar de que el gobierno de Moscú nunca ha admitido su relación con los ciberataques, es evidente que Rusia ha utilizado dichos ataques como estrategia militar.

La existencia de unas «tropas de información» rusas, pone de manifiesto la relación que existe entre la ciberseguridad rusa con los mandos del propio ejército. A pesar de que estas tropas de la información no están compuestas solamente por mandos del ejército, su creación fue justamente posterior al término del conflicto con Georgia en 2008. Estas tropas de información son las encargadas de prevenir los posibles ataques a las infraestructuras críticas rusas, pero también las encargadas de destruir al enemigo y por tanto son capaces de llevar a cabo ciberataques.

En 2013, en el Nuevo Concepto de Política Exterior de la Federación de Rusia podemos observar como el mundo ciber está presente en el ambiente de las relaciones internacionales y en cuanto a la política de defensa y seguridad de la federación. Y tras los incidentes de Ucrania, se ha declarado que el gobierno ruso ya está preparando una nueva estrategia para la ciberseguridad, o seguridad de la información en argot ruso, y que estará disponible muy pronto.

Tras analizar las capacidades cibernéticas rusas, podemos asegurar con firmeza que Rusia es después de China el principal riesgo para la ciberseguridad estadounidense,

ya que la cantidad de sus cibercapacidades no está tan clara, sin embargo sus intenciones y declaraciones sí que lo están.

Para concluir es importante remarcar la inexistencia de una legislación internacional que incluya los delitos informáticos, o la posible ampliación de la legislación ya existente en la actualidad para poder incluir estos conceptos. Esto sería posible con una mejor y diferente cooperación internacional al respecto. Sin embargo es complicado que se llegue a un acuerdo al respecto, ya que cada Estado o actor de las relaciones internacionales tiene conceptos diferentes sobre qué es un ciberataque y cómo combatirlo. A pesar de la existencia del Manual de Tallín, la comunidad internacional no pone suficiente de su parte para la creación de esta legislación o este nuevo sistema de gobernanza en el cual exista una legislación para los ciberataques o incluso unas normas para los conflictos cibernéticos o la ciberguerra.

Bibliografía

Aguirre Romero, J. M. (2004). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI . *Espéculo. Revista de estudios literarios nº 27* . Obtenido de http://www.ucm.es/info/especulo/numero27/cibercom.html

Awan, I. (2014). Debating the Term Cyber-terrorism: issues and problems. *Internet Journal of Criminology* .

BAE Systems Applied Intelligence. (2014). *Snake Toolkit Report 2014.* BAE SYSTEMS. Obtenido de http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

Barnett, E. (13 de Enero de 2011). Runet: Why the Russian internet doesn't need the West. *The Telegraph*. Obtenido de http://www.telegraph.co.uk/technology/news/8255183/Runet-Why-the-Russian-internet-doesnt-need-the-West.html

BBC Monitoring . (11 de Noviembre de 2008). Russian TV highlights hacker attacks on Georgian sites. RenTV.

BBC Monitoring. (29 de Octubre de 2008). Russia is underestimation information resources and losing out to the West. Novyy Region.

Bender, J., & Kelley, M. B. (6 de Marzo de 2014). The Ukraine-Russia Cyber War is Heating Up. *Business Insider*. Obtenido de http://www.businessinsider.com/the-ukraine-russia-cyber-war-is-heating-up-2014-3

Bizeul, D. (2007). *Bizeul.org.* Obtenido de RBN study - before and after : http://www.bizeul.org/files/RBN_study.pdf

Carr, J. (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld.* O'Reilly Media, Inc.

Centre of Excellence - Defence Against Terrorism . (2010). *Defence Against Terrorism Review Vol 3 No 2* .

Cruzado Reyes, J. A. (2011). *Delitos Informáticos y Ciberterrorismo: Fundamentos de Investigación.* Libres, Puebla : Instituto Tecnológico Superior de Libres.

Department of Defense of the United States of America. (2015). *National Security Strategy.* Washington D.C.

Embassy of the United States in London . (2015). Iran's Next Step in Building a 'Halal' Internet. Londres. Obtenido de http://london.usembassy.gov/iran118.html

Federal Bureau of Investigation . (2015). *FBI.gov*. Obtenido de Cyber Crime : https://www.fbi.gov/about-us/investigate/cyber

Fojon Chamorro, E., & Hernandez Lorente, A. (2014). Riesgos del ciberespacio. *Estudios de Política Exterior*. Obtenido de http://www.politicaexterior.com/actualidad/basicospolext-riesgos-del-ciberespacio/

Garamone, J. (2010). *Lynn Explains U.S. Cybersecurity Strategy.* Bruselas: American Forces Press Service. Obtenido de http://www.defense.gov/news/newsarticle.aspx?id=60869

Giles, K. (2011). "Information troops" - a Russian Cyber Command? . *International Conference on Cyber Conflict* (pág. 16). Tallin, Estonia : CCD COE Publications .

Gobierno de Estonia . (s.f.). *Estonia.eu*. Obtenido de e-Estonia: http://estonia.eu/about-estonia/economy-a-it/e-estonia.html

Haas, R. N. (Febrero de 2014). Put America's House in Order, Cover Story. *American Review Mag*. Obtenido de http://americanreviewmag.com/stories/Put-Americas-house-in-order

Hacktivismo. (s.f.). *Hacktivismo.com*. Obtenido de http://www.hacktivismo.com/news/

Harris, S. (2014). *@War: The Rise od the Military-Internet Complex* . Boston; Nueva York: Earnon Dolan Book Houghton Miffin Harcourt .

Infodefensa. (2013). *La OTAN publica un manual sobre la aplicación de la Ley Internacional a la Ciberguerra.* Infodefensa.com. Obtenido de http://www.infodefensa.com/es/2013/04/02/noticia-la-otan-publica-un-manual-sobre-la-aplicacion-de-la-ley-internacional-a-la-ciberguerra.html

Informática-hoy. (26 de 04 de 2010). *Informática-hoy*. Obtenido de ¿Qué es un Cracker? :http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

Instituto Español de Estudios Estratégicos , & Instituto Universitario'General Gutiérrez Mellado'. (2011). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid : Imprenta del Ministerio de Defensa. Obtenido de http://www.aeiciberseguridad.es/descargas/categoria6/5979259.pdf

Jelinek, P. (08 de Julio de 2010). A code you can hack: On CYBERCOM'S logo. *Marine CorpsTimes*.Obtenido de: www.marinecorpstimes.com/news/2010/07/ap_military_cyber_command_logo_070810/

Kraft, M., & Marks, E. (2012). *U.S. Government Counterterrorism: A guide to who does what* . CRC Press .

Leandry-Vega, I. (2014). *Usted no tiene privacidad: el fin del derecho a la privacidad.* Charleston,, Carolina del Sur , Estados Unidos: Editorial Espacio Creativo.

Markoff, J. (12 de Agosto de 2008). Before the Gunfire, Cyberattacks. *The New York Times*. Obtenido de http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

Martínez de Rituerto, R. (18 de Mayo de 2007). Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE. *El País*. Obtenido de http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

Microsoft. (1 de 10 de 2014). *Microsoft.com*. Obtenido de Resources: http://www.microsoft.com/es-es/security/resources/botnet-whatis.aspx

Mshvidobadze, K. (2013). The Global Cyberdomain and new challenges. *Georgian Foundation for Strategic and international studies, 11*, 1 - 13.

Murphy, M. (1 de Julio de 2010). Cyberwar: War in the fifth domain. Are the mouse and keyboard the new weapons of conflict? *The Economist*. Obtenido de http://www.economist.com/node/16478792?story_id=16478792&fsrc=rss

National Security Agency . (06 de 06 de 2015). *NSA* . Obtenido de About NSA : https://www.nsa.gov/about/index.shtml

Near East observatory . (2013). *Near East observatory*. Obtenido de Iran: The Cyber War : http://neobservatory.org/activities/projects/surveillance-censorship-project/case-description/iran-the-cyber-war/

OTAN. (2014). Wales Summit Declaration. *Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.* Wales. Obtenido de http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease

Panarin, I. (2008). The Information Warfare System: the Mechanism for Foreign Propaganda Requires Renewal. *Voyenno-Promyhlennyy Kuryer*.

Panetta, L. E. (2012). *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Washington D.C. : Department of Defense.

Pew Research Center. (2013). *Public Sees U.S. Power Declining as Support for Global Engagement Slips. America's Place in the World 2013.* Pew Research.

Putin, Vladimir; Ministerio de Defensa de la Federación Rusa . (12 de febrero de 2013). *Concepto de la Política Exterior de la Federación de Rusia.* Obtenido de Ministerio de Defensa de la Federación Rusa : http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/42e0019509d1b9bf44257b440042dccf!OpenDocument

Recorded Future . (2014). *The Russia-Ukraine Cyber Front Takes Shape.* Recorded Future: Creating an Insightful World .

RT.com. (7 de Abril de 2015). Rusia desarrolla una nuva doctrina de seguridad de información nacional. *RT*. Obtenido de http://actualidad.rt.com/actualidad/171278-rusia-doctrina-seguridad-informacion

Rubio, R. (2011). *Las Relaciones Internacionales en el Tránsito al Siglo XXI.* Cuadernos de la Escuela Diplomática de España 2011, 44 , Ministerio de Asuntos Exteriores y de Comunicación , Escuela Diplomática de España, Madrid . Obtenido de http://www.rafarubio.es/wp-content/uploads/ciberdiplomaciaintro.pdf

Ruiz González, F. J. (2013). *El Concepto de Política Exterior de Rusia: un estudio comparativo.* Instituto Español de Estudios Estratégicos .

Rush, G. E. (2002). *The Dictionary of Criminal Justice (5th ed.).* Guildford, CT: McGraw-Hill.

Sánchez Medero, G. (2013). El ciberespionaje. *Nueva Época, 13, Marzo-Mayo*, 10.

Sánchez Tapia, S. (2014). *Política Exterior y de Seguridad de los Estados Unidos: La "pax americana" después de Afganistán.* Madrid : IEEEE Documentos de Opinión .

Schiller, J. (2010). *Cyber Attacks & Protection: Civilization.* CreateSpace.

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* CCD COE . Nueva York : Cambridge University Press. Obtenido de https://issuu.com/nato_ccd_coe/docs/tallinnmanual/3?e=0/1803379

Singer, P., & Friedman, A. (2014). *Cibersecurity and Cyberwar: what everyone needs to know* . Nueva York: Oxford University Press .

Symantec. (2014 de 11 de 10). *Symantec*. Obtenido de http://www.symantec.com/es/mx/page.jsp?id=stuxnet

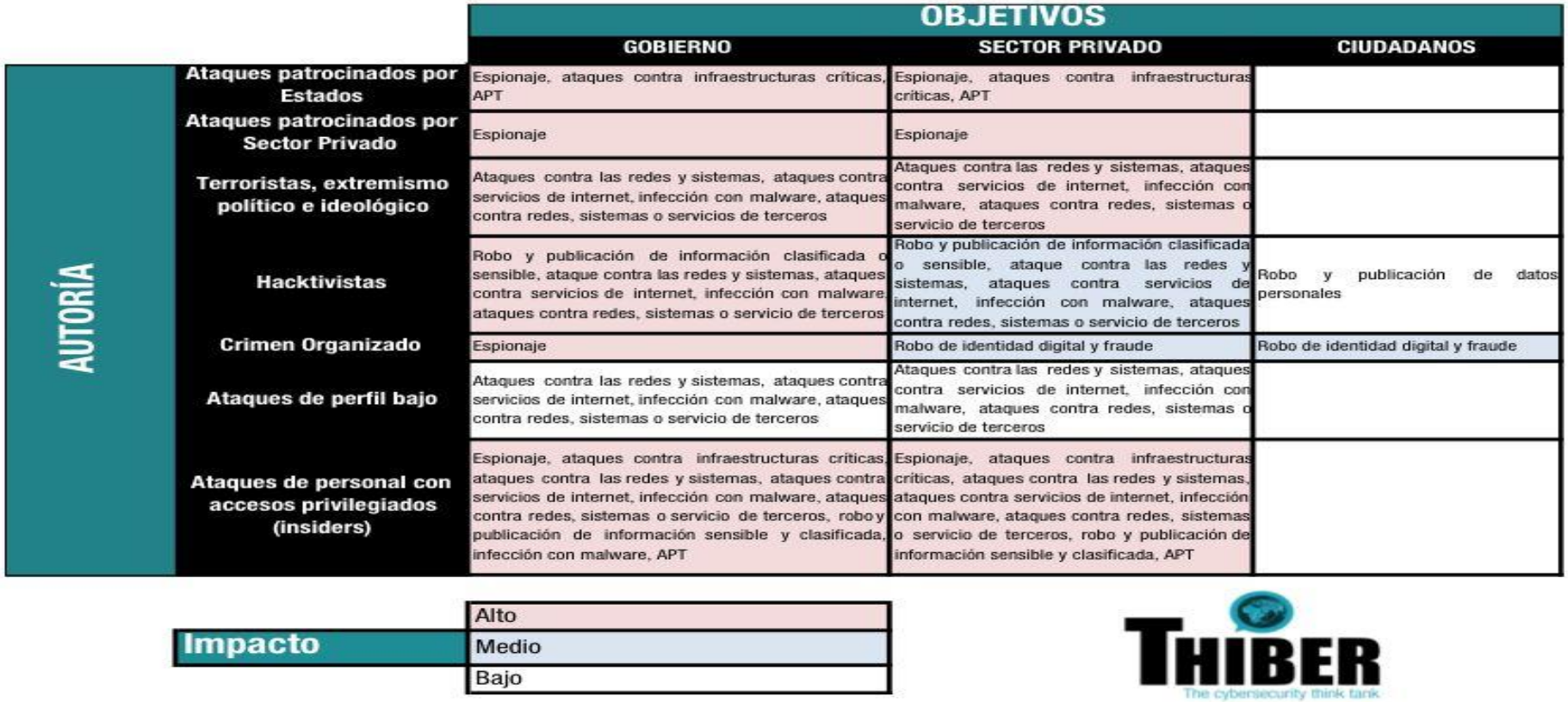
Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations* . Tallín : Cooperative Cyber Defence Centre of Excellence (CCD COE) Publications.

U.S. Department of Defense. (2010). *Cyber Command Fact Sheet.* Obtenido de http://www.stratcom.mil/factsheets/cc/

United States Department of Defense . (2015). *The Department of Defense (DoD) Cyber Strategy*.

Anexos

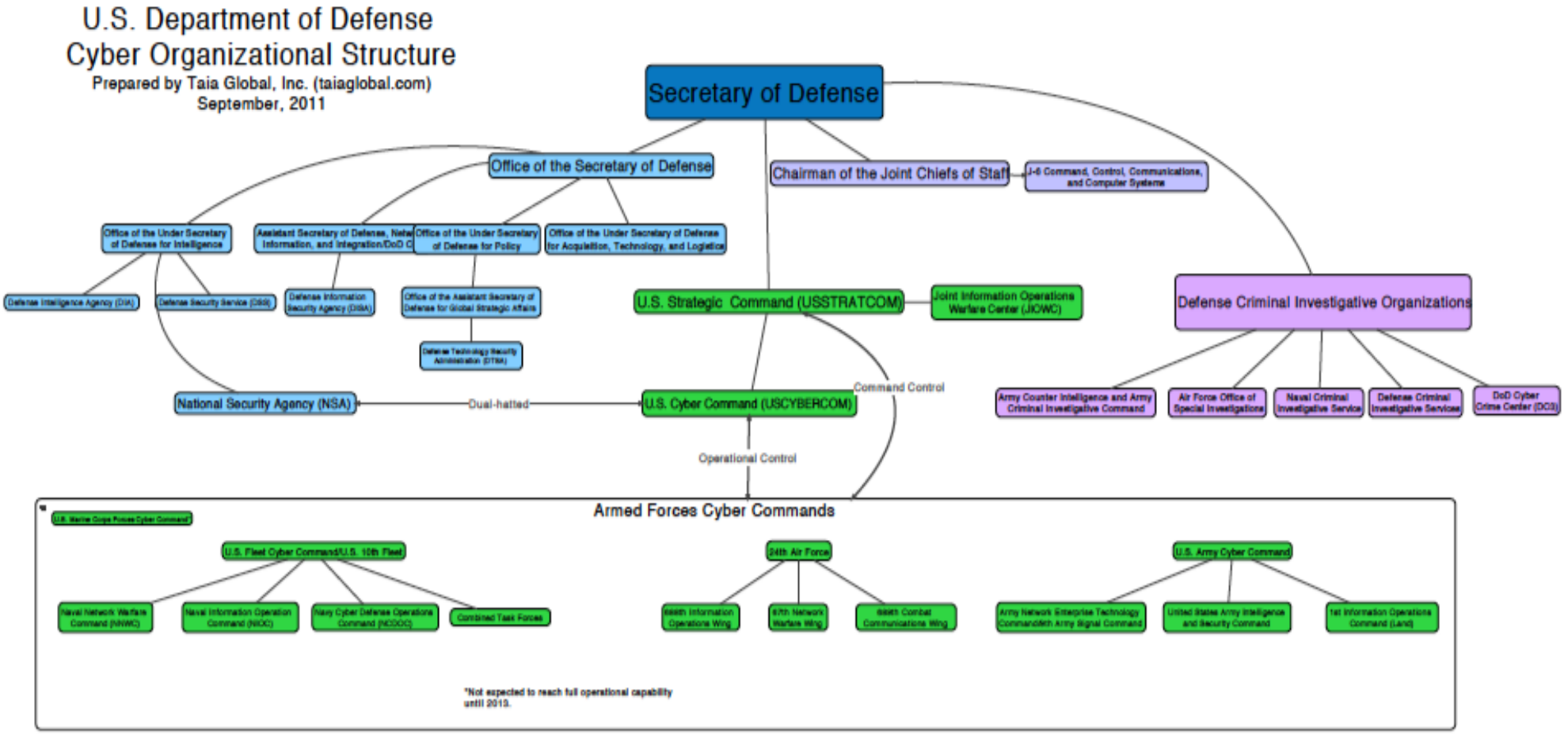
ANEXO I



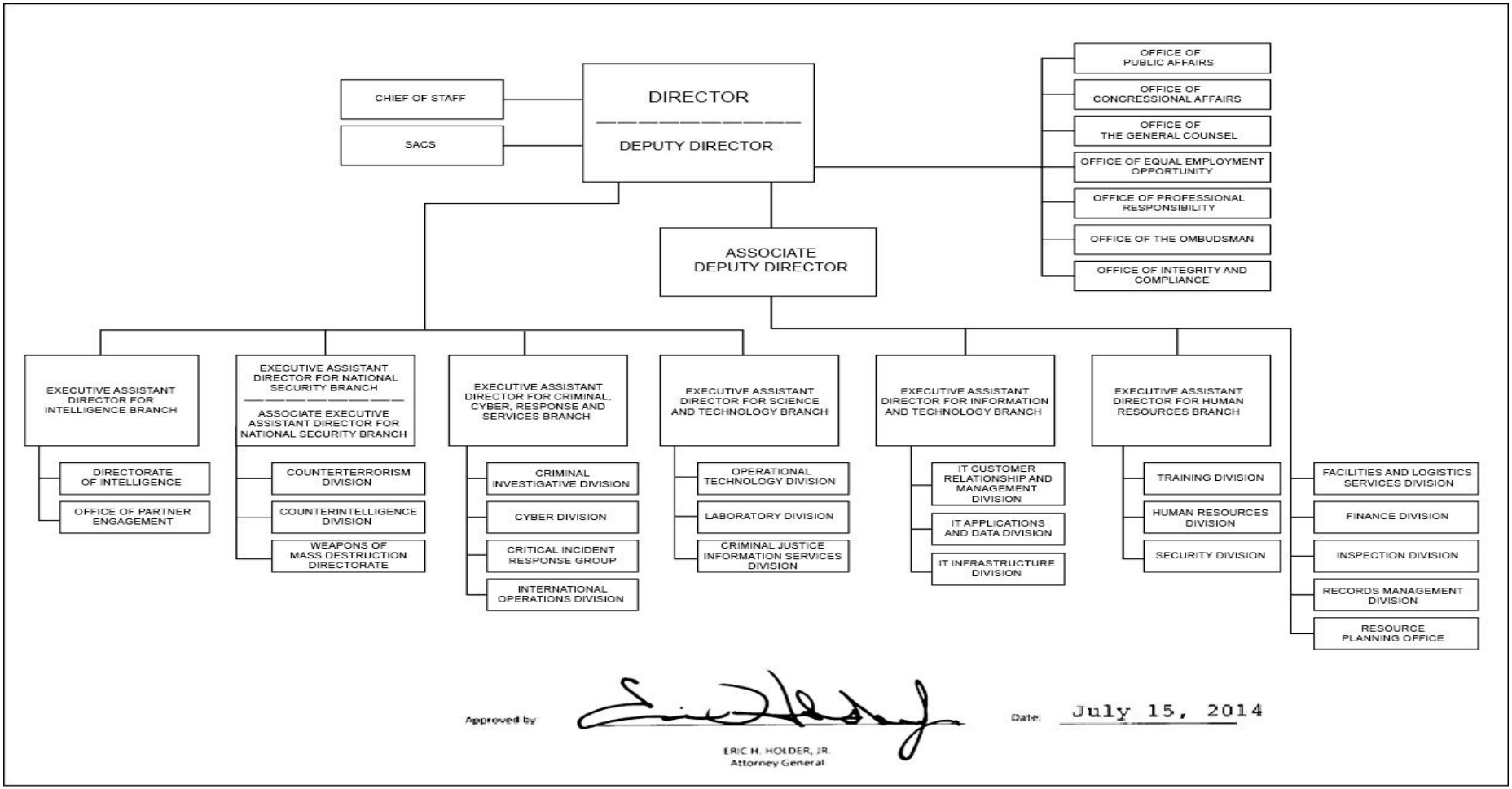
AUTORÍA	OBJETIVOS		
	GOBIERNO	SECTOR PRIVADO	CIUDADANOS
Ataques patrocinados por Estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	
Ataques patrocinados por Sector Privado	Espionaje	Espionaje	
Terroristas, extremismo político e ideológico	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Hacktivistas	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Robo y publicación de datos personales
Crimen Organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de perfil bajo	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros	
Ataques de personal con accesos privilegiados (insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, infección con malware, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, APT	

Impacto
Alto
Medio
Bajo

ANEXO 2 – Department Of Defense Cyber org



ANEXO 3 – Organización de la ciberseguridad del FBI



ANEXO 4 – Organización de la ciberseguridad rusa