CAPÍTULO CUARTO

SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

NÉSTOR GANUZA ARTILES

RESUMEN

El capítulo IV trata de los riesgos y peligros que amenazan la seguridad de las sociedades modernas debido a su dependencia de las Tecnologías de la Información.

Se introduce al lector en los asuntos de mayor conflictividad dentro del marco internacional de la ciberseguridad; en los dilemas que surgen de la necesidad de proteger las redes y los servicios de información y a su vez proteger las libertades individuales inherentes a sociedades democráticas, en especial la libertad de expresión y la protección de la intimidad.

Se estudian y analizan dos casos de ciberataques de gran transcendencia mundial: los ciberataques cometidos contra Estonia, en la primavera de 2007, conocidos por ser el primer caso en que unas operaciones cibernéticas afectan de manera clara, drástica y global a la seguridad nacional de un país; y los ciberataques cometidos contra Georgia, en el verano de 2008, conocidos por ser el primer caso en el que las operaciones cibernéticas son iniciadas y conducidas conjuntamente con operaciones militares armadas.

Por último se analiza la situación de la ciberseguridad en la OTAN y el proceso de transformación que la OTAN está llevando a cabo en dicha materia.

Palabras clave: Ciberataque, ciberdefensa, ciberseguridad, ciberamenaza, ciberdisuasión, OTAN, NCIRC, CDMA, CCDCOE, Estonia, Georgia, Rusia, DDoS, botnet, investigación forense.

CYBERSECURITY SITUATION IN INTERNATIONAL FIELD AND THE NATO

ABSTRACT

Chapter IV deals with the risks and dangers that threaten the security of modern societies due to its dependency on Information Technology.

It introduces the reader in the most contentious issues within the cyber security international framework, on the dilemmas that arise from the need to protect networks and information services while protecting individual liberties inherent in democratic societies, particularly freedom of expression and privacy.

It is studied and analyzed two cases of cyber attacks of world importance: cyber attacks committed against Estonia, in the spring of 2007, known for being the first case in which cyber operations affect the national security of a country in a clear, dramatic and comprehensive fashion; and cyber attacks committed against Georgia, in the summer of 2008, known as the first case in which the cyber operations are initiated and conducted in conjunction with armed military operations.

Finally we analyze the state of cyber security in NATO and the transformation process that NATO is carrying out in this issue.

Key words: Cyber attack, cyber defense, cyber security, cyber threat, cyber deterrence, NATO, NCIRC, CDMA, CCDCOE, Estonia, Georgia, Russia, DDoS, botnet, forensic investigation.

INTRODUCCIÓN

Tópico es iniciar el tema que nos ocupa subrayando la dependencia de las sociedades modernas y de los países desarrollados de los sistemas de información. En cualquier introducción de cualquier libro relacionado con el tema aparece esta idea como básica para el desarrollo de sus argumentos posteriores, no en vano el desarrollo de la sociedad de la información en los países avanzados es a su vez su gran fortaleza y su gran debilidad.

A pesar de los riesgos que conlleva una sociedad cada vez más interconectada digitalmente y cada vez más olvidada de los procedimientos

tradicionales, la tendencia digital es imparable; lo que significa que hay que afrontar el futuro como es y gestionar los riesgos asociados.

Los riesgos asociados son numerosos, entre los que destacan, una mayor y más compleja actividad criminal desarrollada por grupos organizados o delincuentes individuales; una más prolífica actividad terrorista que hace uso del ciberespacio ampliamente para actividades terroristas y para apoyo a ellas; una mayor y más compleja actividad de espionaje, ya sea industrial, militar o político; una mayor variedad y cantidad de ataques a las infraestructuras críticas nacionales, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades modernas; un mayor índice de ataques camuflados, orquestados por Estados y encubiertos bajo apariencia de ataques con origen en bandas criminales, activistas políticos, etc.; una mayor participación de ciudadanos particulares en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por reto o por lucro; y un largo etcétera de riesgos como causa de la atracción que el ciberespacio produce al ofrecer una mayor rentabilidad, globalidad, facilidad e impunidad para todo este tipo de actividades.

Como reacción a esta avalancha de amenazas, que en definitiva son amenazas al estado de bienestar y al sistema democrático de los países desarrollados, surge la necesidad de militarizar la red.

La militarización de la red no debe ser entendida como una ocupación de la red por fuerzas militares con el objetivo de controlar los movimientos en ella, sino como el derecho de las naciones a disponer de ciber armamento en defensa de sus legítimos intereses. Nuestros enemigos las poseen y las usan. Un percepción mal entendida que confine la capacidad militar a los medios convencionales nos pondría en una clara y peligrosa situación de desventaja.

El comandante jefe de la Fuerza Aérea Británica, Sir Stephen Dalton, declara en un discurso pronunciado en el Instituto Internacional de Estudios Estratégicos de la Defensa del Reino Unido, que

> *«el crecimiento exponencial de la disponibilidad de medios de información significa que debemos entender cómo distribuir y proteger nuestros intereses nacionales en el dominio cibernético y, aunque se trata claramente de una cuestión de gobierno, la defensa tiene un interés legítimo en el desarrollo de capacidades defensivas y ofensivas cibernéticas. En el futuro nuestros adversarios pueden usar ciberataques contra nuestros sistemas de informa-*

> *ción. De hecho nuestros sistemas informáticos nacionales están, hoy, bajo ataques constantemente. Nuestros enemigos actuales ya están utilizando efectivas operaciones de información y propaganda, a través de Internet, sobre las bajas civiles para tratar de influir en la opinión pública y limitar nuestras actividades. En fin, que van a usar todos los medios posibles a su alcance para tratar de anular nuestra libertad porque entienden que cuando se utiliza con eficacia, es su ventaja comparativa»* (1).

El antiguo Director de la Inteligencia Nacional de los Estados Unidos, Mike McConnell, declara que las ciber armas deben ser consideradas como armas de destrucción masiva (2).

La carrera armamentística cibernética es un hecho (3). Según el experto analista de ciber seguridad Kevin Coleman la carrera comenzó en 2006 con una docena de países participando en su desarrollo y utilización. En 2007, el número de países aumentó en un 450%. Las cyber armas han proliferado en todo el mundo y ahora son parte de los arsenales en 150 países, 30 de los cuales han incorporado unidades cibernéticas dentro de sus ejércitos (4). En la actualidad, se estima que participan en la carrera más de 200 países, grupos terroristas, organizaciones criminales, organizaciones extremistas y facciones de activistas.

El panorama se vuelve más sombrío, dudoso y alarmante cuando se considera que las organizaciones criminales, los grupos extremistas y terroristas también han entrado en la carrera.

Los servicios de inteligencia militar de todo el mundo están tratando de monitorizar el desarrollo y la venta de armas cibernéticas, así como qué de identificar los grupos que están detrás de los ataques cibernéticos. Un gran número de agencias gubernamentales están interesadas

---

(1) Artículo publicado el 16 de febrero de 2010 por «The Independent». http://www.independent.co.uk/news/media/online/twitter-is-a-weapon-in-cyber-warfare-1900535.html

(2) Mr. Mike McConell en una entrevista ofrecida en el programa televisivo «Charlie Rose Show», el 8 de enero de 2009.

(3) Kevin G. Coleman en su informe «el derecho a disponer de ciber armamento» («The right to bear cyber arms». http://www.technolytics.com/Right_to_bear_cyber_arms_CCH9-2.pdf

(4) Kevin G. Coleman, en su artículo «Private Sector-Military Collaboration Vital to Confront Cyber Threats». http://www.defensetech.org/2010/04/19/private-sector-military-colaboration-vital-to-confront-cyber-threats/

en el aprendizaje de las capacidades de las armas cibernéticas y las intenciones de los activistas y extremistas para el uso de tales armas (5).

Sin duda alguna el Ciberespacio debe ser considerado y estudiado para su posible inclusión en la doctrina militar como un espacio de la batalla más, conjuntamente con los espacios de tierra, mar y aire; de tal manera que las operaciones conjuntas dispondrían de un componente más.

En este capítulo se analizará la situación internacional en ciberseguridad a través del estudio de dos casos reales de ciber guerra (Estonia 2007 y Georgia 2008) y a través del análisis de la situación actual en la OTAN.

LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL

La respuesta ante ciber ataques solo es efectiva desde una perspectiva internacional, en donde es vital consolidar acuerdos firmes de colaboración entre Estados, organizaciones o alianzas militares internacionales, el sector privado, la industria y el sector académico.

Maeve Dion, investigadora del Centro de Protección de Infraestructuras Críticas de la Universidad de George Mason en los Estados Unidos, advierte del peligro de conflicto en el área de ciberseguridad entre la OTAN y la Unión Europea, por la diferente prioridad que dichas organizaciones establecen en sus programas relacionados con la materia y esto a la larga es fuente de problemas para los países pertenecientes a ambas organizaciones (6).

A su vez en la respuesta deben tomar parte diferentes actores que hablan diferentes lenguajes, por lo que es necesario trabajar de manera concienzuda en la coordinación multidisciplinar en los campos científico, tecnológico, político, diplomático, económico, jurídico, militar y de inteligencia.

El ruido legal alrededor del mundo cibernético no hace más que favorecer los intereses de ciertos países y de grupos criminales y terroristas que les conviene un cierto grado de ambigüedad jurídica para situarse en una posición de ventaja sobre los países democráticos, en los que las libertades públicas y los derechos de expresión y privacidad, entre otros,

(5) Op.Cit. 3

(6) Maeve Dion, en el prefacio del libro «International Cyber Incidents, legal considerations». Eneken Tikk, Kadri Kaska y Liis Vihul, publications@ccdcoe.org

hace que las fuerzas armadas y las fuerzas del orden y seguridad tengan muchas restricciones a la hora de hacer uso del ciberespacio.

Valga de ejemplo, el uso casi tabú que se hace del término «ciber ataque» en los entornos políticos y militares de los países democráticos, haciéndose uso de eufemismos tales como «ciber defensa activa».

Las múltiples líneas borrosas que surcan el ciberespacio como, el uso legal de equipos de penetración (red team), el uso legal de monitorización de las redes, el uso legal de datos personales para investigaciones forense de ciber ataques (7), la determinación de las fronteras nacionales y la integridad territorial en el ciber espacio, la atribución legal de ciber ataques, las competencias policiales y militares, etc; no hacen más que beneficiar a potenciales enemigos y adversarios que hacen uso de las armas cibernéticas para atacar a sociedades democráticas que a su vez cuestionan el uso de las mismas armas para defender sus intereses.

Sin ir más lejos, todas las actividades educativas y ejercicios en la OTAN relacionados con el hecho cibernético son de ciber «defensa». Existe una duda moral y legal en ciertos sectores de si se puede instruir y entrenar a militares en el uso de herramientas de ciber ataque, ya que dicha formación les puede servir para realizar acciones delictivas privadas sin el control de los propios ejércitos.

Como si esto fuera un caso distinto a la instrucción y entrenamiento con armas de fuego, esencia de los ejércitos y que también pueden ser usadas a posteriori para cometer delitos sin el control de los propios ejércitos.

La formación de unidades militares específicas de ciberguerra no es más que la obligación que tienen los ejércitos de adaptar sus funciones a las tecnologías del momento, como en su día se hizo con la incorporación de las unidades de misiles, NBQ (8) o guerra electrónica.

Otro tema de discusión en el ámbito internacional acerca de la ciber seguridad es el concepto de «disuasión cibernética». ¿Cómo lograr una efectiva disuasión ante ciber ataques?

La disuasión se entiende como la firme intención y predisposición de un Estado víctima de un ataque de causarle al atacante un daño mayor del sufrido en justa represalia y en legítima defensa. La disuasión tiene

(7) Por ejemplo, es actualmente debatido en países desarrollados si la dirección IP es dato personal o no.

(8) NBQ: Nuclear, bacteriológico y químico.

como objetivo persuadir a los atacantes de llevar a cabo sus malévolas intenciones. Es una manera efectiva de prevención.

En la disuasión cibernética, a diferencia de en la nuclear, el principal problema consiste en ¿cómo amenazar y prevenir un atacante que se desconoce?. En la disuasión nuclear el atacante deja su firma instantes después de lanzar un ataque nuclear, en la disuasión cibernética, en muchos casos no es posible saber con exactitud quién es el originador, responsable u organizador de los ciber ataques. Además, en los pocos casos que es posible una identificación cierta, ésta se logra después de meses de trabajo forense y la reacción del Estado víctima ya no es inmediata y la legítima defensa podría no ser un argumento válido.

Por otro lado, en la mayoría de los casos, los ciber ataques se basan en atacar desde multitud de puntos dispersos por el globo a unos pocos puntos concretos de la víctima. La represalia inmediata no es posible, puesto que atacar a los atacantes no surtiría efecto por la imposibilidad de la concentración de objetivos y por la duda de si el atacante realizó el ataque deliberadamente o su infraestructura fue secuestrada sin su conocimiento.

El concepto de disuasión en el ciberespacio debe cambiar totalmente su filosofía y basarse en la prevención, en hacer al atacante no rentable el ataque y en una sólida colaboración internacional y no en una represalia instantánea.

Para finalizar este apartado valga una reflexión sobre el uso del ciberespacio por parte de los terroristas.

En primer lugar, los terroristas necesitan que sus acciones sean lo suficientemente graves como para mantener atemorizada a una determinada sociedad durante un tiempo relativamente largo; y para ello nada mejor que un atentado con daños o posibilidad de daños físicos graves o mortales a personas. En este caso, el ciber espacio es un terreno todavía por explorar por los grupos terroristas más influyentes, que fundamentalmente usan la red como plataforma de apoyo logístico, de comunicaciones, de reclutamiento y propagandística.

En segundo lugar, los terroristas necesitan de un gran aparato mediático que de publicidad a sus acciones de la manera más rápida y extensa posible. En este caso los terroristas no tienen que esforzarse mucho, ya se encargan los propios medios de comunicaciones de los países democráticos, en donde la libertad de información está garantizada, de hacerles esa función y el ciberespacio garantiza su cobertura a nivel mundial.

EL CIBER CASO ESTONIA 2007

Antecedentes

En la primavera de 2007 el gobierno de la República de Estonia anuncia su decisión de realizar excavaciones en la plaza de Tonismäe, con motivo de encontrar restos de soldados caídos durante la segunda guerra mundial enterrados en el subsuelo y posteriormente identificarlos y enterrarlos en el cementerio militar de Tallin.

La decisión del gobierno incluía el traslado y emplazamiento, de forma permanente, de la estatua conocida como «el soldado de bronce» (9) a la entrada del mencionado cementerio militar.

El soldado de bronce es considerado por la «comunidad rusa» en Tallin (10) como un símbolo de sus caídos en la segunda guerra mundial y es costumbre depositar flores a sus pies en señaladas fechas conmemorativas de la victoria rusa. Por el contrario para la «comunidad estonia» el soldado es considerado como un símbolo de la era soviética que trae no buenos recuerdos a muchos estonios. Según Rain Ottis (11), para la minoría local rusa el soldado representa al «libertador» mientras que para los estonios representa al «opresor».

La situación que se vivía era de normalidad; la comunidad rusa utilizaba la plaza y el monumento como lugar de celebración en fechas señaladas y los estonios toleraban los actos sin darle más importancia.

Pero la situación cambió el 9 de mayo de 2006 cuando la policía tuvo que intervenir en una trifulca entre miembros de la comunidad rusa que

---

(9) El soldado de bronce es un monumento instalado en la mencionada plaza en 1947 con motivo de la conmemoración de la victoria del ejército soviético sobre el ejército alemán durante la segunda guerra mundial. En 1947 Estonia formaba parte de la extinta Unión Soviética bajo régimen de Stalin.

(10) Según el Registro de Población hasta el 1 de enero de 2009, 1.364.100 personas viven en Estonia, en representación de más de 100 etnias diferentes. Los principales grupos étnicos son: estonios (68,6%), rusos (25,6%), ucranianos (2,1%), bielorrusos (1,2%) y finlandeses (0,8%). Según el Censo de Población del año 2000, en Estonia se hablan 109 lenguas. El 83,4% de los ciudadanos estonios habla estonio como lengua materna, el 15,3%, ruso, y el 1% restante habla algún otro idioma. Datos extraídos de la Embajada de Estonia en Madrid. http://www.estemb.es/estonia/integracion

(11) Rain Ottis, experto en Ciber seguridad que formó parte del equipo encargado por el gobierno estonio de planificar y ejecutar la respuesta a los ciber ataques sufridos por Estonia en 2007, en su informe «Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. (9)

portaban banderas de la extinta Unión de Republicas Socialistas Soviéticas y estonios que portaban banderas de la República de Estonia –entre partidarios pro-kremlin y movimientos nacionalistas estonios–. A partir de este hecho la sociedad estonia se fue polarizando cada vez más y el soldado de bronce se convirtió en el punto de encuentro de manifestantes extremistas, cada vez más con mayor agitación; de tal manera que la plaza a partir de entonces tuvo una vigilancia especial por parte de la Policía.

Con la sociedad cada vez más polarizada, animada por la prensa local y por la prensa rusa, y con manifestaciones nacionalistas localizadas alrededor de un símbolo con dos significados enfrentados; el debate en la sociedad estonia estaba servido (12), ¿Por qué no trasladar el símbolo de un lugar céntrico y emblemático de la ciudad a una zona más apartada donde las manifestaciones no tengan tanta visibilidad y repercusión?

Así que el gobierno estonio anunció su decisión del traslado a principios de la primavera de 2007 y el 26 de abril de 2007 comenzaron los trabajos preparatorios. Este hecho provocó una manifestación, seguida de actos vandálicos sin precedentes en Estonia por el número de participantes, por la violencia de sus actos, por el número de arrestados –1.300– y por el número de heridos –cientos–, incluyendo un muerto. Para encontrar un hecho de similar magnitud en Estonia, hay remontarse a los disturbios provocados por la Fuerza Aérea Soviética en 1944 y la anterior ocasión en que como consecuencia de disturbios callejeros en Tallin hay víctimas mortales hay que remontarse a 1918.

Estos disturbios fueron conocidos como «la noche de los cristales«. En concreto, en la mañana del 26 de abril de 2007, numerosas personas se congregaron de manera pacífica en la plaza del soldado de bronce para protestar por la decisión del gobierno de trasladar el monumento, pero por la tarde se unió un grupo con una actitud violenta, el cual se enfrentó a la policía y horas más tarde comenzaron actos vandálicos por la ciudad, rompiendo escaparates. La policía no tomó el control de la situación hasta el siguiente día, el 27 de abril de 2007.

---

(12) Hay que considerar que la sociedad estonia no está habituada a desordenes públicos, manifestaciones, huelgas, etc. El autor de este capítulo lleva viviendo en Estonia desde Julio de 2008 sin haber presenciado, o tenido noticia alguna, a través de amigos y compañeros o a través de medios de comunicación de ninguna manifestación, protesta pública o huelga.

El 27 de abril de 2007 mientras proseguían los enfrentamientos callejeros entre la policía y grupos violentos de la comunidad rusa, varios hechos significativos surgieron simultáneamente:

a) comenzaron los ciber ataques a sistemas de información de la infraestructura pública y privada estonia.

b) los medios de comunicación locales, nacionales e internacionales se hacían eco de la situación con desigual puntos de vista.

El ICDS (13) declara que la gran mayoría de la prensa nacional e internacional informó fehacientemente de los hechos incluyendo los actos vandálicos y los destrozos producidos a establecimientos y negocios. Por el contrario, los medios de comunicación rusos no informaron sobre el vandalismo y enfocaron la noticia como un acto de violencia ejercido por la policía estonia contra pacíficos manifestantes. Lo cual fue un perfecto caldo de cultivo para diversos artículos agresivos contra Estonia y su forma de resolver el asunto, incluyendo unas declaraciones de un parlamentario ruso que consideró el acto como causa de guerra (14).

El Baltic News Services (15) y el Postimees (16) informan sobre hechos que inducen a pensar en la implicación de la Embajada rusa en Tallin en la organización de los actos vandálicos de la noche de los cristales.

En concreto el Baltic News en su edición del 25 de abril de 2007 informa acerca de reuniones sostenidas repetidamente entre Sergei Overtshenko, consejero de la embajada rusa y Dmitri Linter leader de la «Patrulla Nocturna», grupo sospechoso de llevar a cabo los actos vandálicos durante la noche de los cristales.

El Baltic News en su edición de 18 de abril de 2007 y el Postimees en su edición de 25 de abril de 2007 informan acerca de la reunión sostenida el 18 de abril de 2007 entre Andrei Zarenkov, líder del Partido Constitucional Estonio, y firme defensor del soldado de bronce y Vadim Vassilyev, primer secretario de la embajada rusa. Posteriormente a la reunión, el mismo día, Zarenkov anunció que la jefatura del Partido Constitucional Estonio ha decidido reclutar agitadores voluntarios con la misión

(13) ICDS: International Centre of Defence Studies. www.icds.ee.

(14) «Russia's involvement in the Tallinn disturbances», 12.05.2007, a compact overview compiled by the ICDS. www.icds.ee.

(15) Ibid

(16) Ibid

de convencer a los militares estonios que la intervención de las Fuerzas Armadas Estonias en el conflicto sería inaceptable.

c) comenzaron las acciones de movimientos juveniles, en especial el movimiento «Nashi» (17), las más destacables: el bloqueo de la embajada estonia en Moscú y la agresión a la embajadora durante una conferencia de prensa.

Según el ICDS hay suficientes datos para afirmar que el Kremlin está directamente relacionado con la organización y decisión del bloqueo de la embajada estonia en Moscú (18).

Según el «Eesti Päevaleht»(19) en su edición del 2 de mayo de 2007 el bloqueo se caracterizó por unos aspectos que no suelen coincidir en una manifestación pública espontánea; como que los participantes en el bloqueo disponían de un autobús para prepararse las comidas, de 30 tiendas de campañas exactamente iguales, de modernos dispensadores de agua, equipos de sonido, pancartas de material de gran calidad que se cambiaban cada día, etc.

Pero el hecho incuestionable es que la embajada estuvo asediada durante una semana (del 27 de abril al 1 de mayo), impidiendo el normal desarrollo de entradas y salidas del recinto, incluyendo a la embajadora Marina Kaljurand y el Vice-Cónsul Silver Laanemäe, sin que la policía remediara la intolerable situación.

La evidencia más clara de la implicación del kremlin en el asedio se deriva de una conversación telefónica mantenida por el Ministro de Asuntos Exteriores de la Federación Rusa Yevgeny Primakov con su homólogo alemán Frank-Walter Steinmeier, sacada a la luz por «The Financial Times, Germany» el 5 de mayo de 2007, en la que el ministro ruso aseguraba que el gobierno de la federación rusa se aseguraría de que la policía forzara la finalización del bloqueo bajo una condición, que la embajadora estonia abandonara Moscú.

El hecho es que el mismo día que la embajadora abandonó Moscú, los bloqueadores levantaron el bloqueo y la policía las barreras de protección.

---

(17) Nashi: es un movimiento de jóvenes políticos en Rusia, que declara ser movimiento democrático antifascista.

(18) Op. Cit.7

(19) http://www.epl.ee/

Es claro para el autor que los ciber ataques no fueron un hecho aislado sino que estaban enmarcados dentro de una situación política claramente definida, en la que hay considerar además el poco agrado que causo en el kremlin la adhesión de Estonia a la OTAN en 2004. El grado de implicación de las autoridades rusas en el conflicto, en las manifestaciones y actos vandálicos en Tallinn y en el bloqueo y acoso a la embajada y embajadora en Moscú es difícil de determinar, pero existen multitud de datos que apoyan la tesis de que los enfrentamientos no fueron espontáneos sino que contaron con la complicidad de las autoridades rusas.

Cronología de los ciber ataques

Los ciberataques a Estonia tuvieron lugar entre el 27 de abril y el 18 de mayo de 2007, a.i. Durante este periodo los ataques variaron su objetivo, volumen y método, pero en líneas generales se pueden distinguir dos fases principales:

Fase 1, del 27 al 29 de abril, en donde los ataques debida a la inmediatez del conflicto tenían un componente emocional y esto en sí mismo constituía la motivación para unirse a los ciberataques y como todo acto emocional eran básicamente de naturaleza simple, es decir, sin grandes complejidades de carácter técnico y organizativo y sin capacidad de convocar a un número de atacantes lo suficientemente grande como para causar daños serios y poner en una situación de crisis o indefensión a Estonia.

Según Lauri Alman(20), la primera fase se caracterizó por el uso de herramientas de ciber ataque rudimentarias y simples, llevados a cabo por hacktivistas (21) sin grandes conocimientos técnicos, los cuales hacían uso de herramientas que a su disposición se emplazaban en sitios web, rusos mayoritariamente, conjuntamente con las correspondientes instrucciones (22). Las herramientas estaban especialmente diseñadas para atacar sitios web de Estonia y especialmente del gobierno, del ministerio de Defensa y de los principales partidos políticos.

(20) Lauri Alman, durante el conflicto era el Secretario de Estado de Defensa de Estonia y formaba parte del comité de crisis formado para la ocasión.

(21) Ver glosario

(22) Lauri Alman en la entrevista ofrecida a Wyatt Kash para GCN (www.gcn.com) el 13 de junio de 2008. http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx

El primer ataque, registrado e informado(23), relacionado con el caso Estonia fue contra sitios web gubernamentales durante la noche del 27 de abril de 2007(24).

En concreto, cuenta Laury Alman que miembros del gobierno estonio se encontraban en una reunión en la sala de situación del gobierno cuando el responsable jefe de relaciones públicas entra en la sala y comenta que no eran capaces de cargar los comunicados de prensa en los sitios web oficiales del gobierno, los miembros del gobierno allí presentes no le dieron más importancia hasta que fueron advertidos expresamente que estaban bajo ciber ataque, esto ocurrió la noche del 27 al 28 de abril de 2010 a la 01 de la mañana (25).

Una vez confirmado que el país estaba bajo ciber ataque el gobierno procedió de manera inmediata a organizar un equipo de respuesta liderado y coordinado por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian CERT)(26) y compuesto por personal experto de los ministerios de Comercio y Comunicaciones, y de Defensa, así como de los servicios de Inteligencia.

Este fue un gran triunfo de Estonia: *identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirle de la autoridad necesaria.*

Fase 2, del 30 de abril al 18 de mayo, en donde el conflicto en las calles se difumina trasladándose al ciber espacio, donde los ánimos de los ciudadanos de Estonia (rusos y estonios) se calman y no hay lugar para ataques emocionales, en esta situación más fría los ataques se volvieron más complejos tanto en el aspecto técnico como en el organizativo y en la coordinación; sucediéndose ataques mucho más sofisticados que necesitaban de un mayor conocimiento de las herramientas de ciber guerra, al menos por parte de los organizadores y de un uso de grandes «botnets»(27) y de una coordinación minuciosa y precisa.

---

(23) Es importante recalcar esto, «ataque informado», porque en muchos casos los ataques recibidos por entidades importantes son silenciados por miedo a perdida de reputación, fiabilidad o fidelidad de los clientes.

(24) Op. cit., 13

(25) Ibid.

(26) CERT: Computer Emergency Response Team.

(27) Una botnet es una red formado ordenadores secuestrados o infectados –robots informáticos o bots–, que ejecutan tareas de manera autónoma y automática y que normalmente pasan desapercibidas para el legítimo propietario o usuario. El Centro

Los sitios web usados en la primera fase que sirvieron de plataforma de lanzamiento de ataques seguían en funcionamiento en esta segunda, pero con mejoras añadidas, como listas de objetivos y calendario en los que se indicaba hora y lugar del ataque para conseguir un enorme volumen de peticiones simultáneas sobre los mismos servicios informáticos con el fin de dejarlos fuera de servicio (28).

Una de las características más interesantes de esta fase es la relación existente entre la situación política y los ciberataques. Como ejemplo más revelador, valga destacar, el espectacular incremento de los ataques coincidiendo con la fiesta nacional rusa conmemorativa de la victoria sobre el ejército alemán en la segunda guerra mundial, esto es el 9 de mayo de 2007. El incremento fue del 150% a las 11 horas de la noche (hora local estonia) del 8 de mayo que coincide con el comienzo de la fiesta nacional en Moscú (00.00 horas del 9 de mayo, hora de Moscú).

Según José Nazario (29), se registraron 21 ataques de denegación de servicios distribuidos (DDoS (30)) durante el 3 de mayo de 2007, 17 durante el 4 de mayo, 31 durante el 08 de mayo, 58 durante el 09 de mayo y 1 durante el 11 de mayo (31).

Tipos de ataques

Los tipos de ataques llevados a cabo en el caso Estonia fueron principalmente los siguientes:

a) Ataques de denegación de servicios (DoS)

El ataque de denegación de servicio es un ataque informático que utiliza el protocolo TCP/IP para conseguir que un determinado servicio o recurso prestado por un sistema de información sea inaccesible a los usuarios legítimos. El ataque se puede realizar desde un solo punto o desde muchos puntos simultáneamente.

---

de Mando y Control de la Botnet puede controlar todos los ordenadores o servidores infectados de forma remota.

(28) Rain Ottis, overview of events, 02 de mayo de 2007, CCDCOE activation team, TDCCIS

(29) José Nazario es un destacado analistas de ciber amenazas a nivel mundial, forma parte del equipo de Arbor Networks. http://asert.arbornetworks.com/authors.php#authID8

(30) DDoS: ver glosario.

(31) José Nazario, Arbor Networks, 17 de mayo de 2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

Cuando el ataque procede desde muchos puntos simultáneamente, generalmente haciendo uso de Botnets, se denomina «ataque distribuido de denegación de servicio» (DDoS).

En general, se necesita un número muy grande de atacantes ejerciendo peticiones de servicio simultáneamente sobre un mismo objetivo para conseguir la perdida de conectividad de la red de la victima por el consumo de su ancho de banda o sobrecarga de los recursos computacionales.

Son varias las maneras de congregar un número grande de atacantes sobre un mismo objetivo simultáneamente, entre las que se destacan:

– La propaganda: como en la primera fase del caso Estonia, se motiva emocionalmente a potenciales atacantes y se les da instrucciones precisas y apoyo técnico para sus acciones. Este es el caso básico, pero con resultados normalmente mitigables por la dificultad de congregar un número suficiente para causar daño.
– A través de botnets: secuestrando recursos computacionales de personas o entidades que normalmente desconocen su aportación, y controlando dichos recursos desde un punto origen –Centro de Mando y Control de la Botnet–.
– A través de granjas de servidores (32): ya sea usando granjas de servidores asociadas a instituciones estatales, o alquilándolas en el sector privado.
– Una combinación cualquiera de las tres anteriores.

En el caso Estonia, los métodos más usados fueron DDoS mediante «inundación ICMP (33)», «inundación UDP (34)» y peticiones deforma-

(32) Granja de Servidores: es un grupo interconectado de servidores que sirve para ejecutar tareas que necesitan de una gran capacidad computacional.

(33) Inundación ICMP (ICMP flood) consiste básicamente en el envío masivo y continuado de peticiones ping (peticiones mediante paquetes ICMP Echo que tratan de comprobar la accesibilidad de una determinada entidad de la red) a un solo objetivo, obligando a la víctima a responder a todas las peticiones ping (con paquetes ICMP Echo reply, pong) respuesta en. Si el desequilibrio entre número de peticiones y la capacidad de respuesta de la víctima es grande se produce una sobrecarga de la red y del sistema de la víctima.

(34) Inundación UDP (UDP flood): consiste básicamente en el envío masivo y continuado de peticiones UDP (el protocolo UDP no necesita de conexión previa, ni tiene confirmación de errores. Es usado fundamentalmente en servicios de audio y de video en tiempo real). Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.

das y con menos intensidad «inundación SYN (35)» y el «ping de la muerte (36)».

Se sospecha que además de botnets secuestradas se usaron también botnets y granjas de servidores de alquiler, pero no se ha podido comprobar hasta la fecha.

Según Linnar Viik (37) los últimos ataques no fueron realizados a través de redes de ordenadores zombis si no a través de algo que no se puede comprar en el mercado negro –en alusión a una intervención estatal organizada–, una capacidad estatal de ciber guerra y esto es algo que debe ser profundamente analizado pues constituye un nuevo nivel de riesgo. En el siglo 21 la competencia de un estado no es sólo su territorio y su espacio aéreo sino además su infraestructura electrónica (ciber espacio) (38).

José Nazario contabilizó 128 ataques de denegación de servicio durante el periodo comprendido entre el 03 y el 11 de mayo, de entre los cuales, 115 usaron el método de inundación ICMP y 10 consumieron 90 Mbps durante 10 horas, por lo que deduce que «*alguien está muy, pero que muy empeñado en causar daño a Estonia y este tipo de cosas se incrementarán en los próximos años*» (39).

b) Ataques de desfiguración de sitios web (web site defacement)

El ataque de desfiguración de web es un ataque mediante el cual se accede a un sitio web clandestinamente con el objetivo de modificar el aspecto visual.

---

(35) Inundación SYN (SYN flood) consiste básicamente en el envío masivo de peticiones de conexión (paquetes TCP/SYN) a un solo objetivo. El objetivo atacado trata cada uno de los paquetes recibidos como una petición de conexión y responde con paquete TCP/SYN-ACK para establecer la conexión y se mantiene a la espera de la respuesta del supuesto peticionario (paquete TCP/ACK). La respuesta nunca llega porque la petición es falsa y todo esto consume la capacidad del servidor e impide que dé respuesta a peticiones legítimas.

(36) Ping de la muerte (Death ping): consiste básicamente en el envío masivo de paquetes ICMP muy pesados (mayores a 65.535 bytes) con el objetivo de colapsar el sistema atacado. Es un ataque que aprovechaba una vulnerabilidad de los sistemas operativos anteriores a 1998, por lo que este ataque fue efectivo solo en unos pocos casos muy determinados.

(37) Linnar Vikk, durante el caso Estonia era asesor del gobierno en materia de tecnología de la información.

(38) Linnar Vikk en un aartículo de Peter Finn para el Washington Post, 19 de mayo de 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

(39) Op. cit. 22

En el caso Estonia se realizaron ataques de este tipo fundamentalmente a sitios web oficiales modificando los contenidos originales por otros de carácter apologético de la causa rusa y en lengua rusa.

Uno de los principales objetivos en estos ataques fue el primer ministro de Estonia Andrus Ansip. En uno de estos ataques los hackers modificaron el contenido del sitio web del partido político del primer ministro y entre otras cosas emplazaron una fotografía de Andrus Ansip con bigote tipo Hitler.

c) Ataques a servidores de sistemas de nombres de dominio

Un sistema de nombres de dominio es un sistema jerárquico que asocia información variada con nombres de dominios asignados a cada uno de los participantes en servicios o recursos conectados a internet o a una red privada. Su función más importante, es traducir nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos mundialmente.

Un ataque de este tipo es tremendamente peligroso pues el servidor DNS es una pieza fundamental e indispensable para el funcionamiento de internet.

En el caso Estonia, en las webs que servían de apoyo a los atacantes no avezados en las tecnologías de la información se daban instrucciones de cómo atacar DNS conjuntamente con las direcciones IP y URL de objetivos. Los DNS destacados como objetivos en las webs maliciosas fueron el servidor DNS nacional –administrador de los nombres de dominio de la administración pública–; el EENet –administrador de los nombres de dominio de la red de servidores de las instituciones del Gobierno y de Educación– y los DNS de proveedores estonios de servicio de internet (40).

d) Correo basura (spam)

Correo basura son aquellos mensajes de correo electrónico que se reciben sin haberlo solicitado, sin permiso o autorización del receptor, habitualmente no deseados y de remitentes desconocidos. En la ma-

(40) Eneken Tikk, Kadri Kaska y Liis Vihul, International Cyber Incidents, legal considerations. ccdcoe@ccdcoe.org (3)

yoría de los casos con finalidad publicitaria. Cuando el correo basura se recibe en grandes cantidades puede llegar a ser molesto para el receptor.

En el caso Estonia, no hablamos de correo de carácter publicitario molesto para el receptor, sino de ataques bien organizados basados en el envío masivo de correos electrónicos generados por robots a direcciones oficiales gubernamentales y direcciones privadas de personajes relevantes de la política estonia.

Este tipo de ataque es más sencillo y efectivo de lo habitual si se realiza contra un país como Estonia, debido a la política de transparencia cibernética que el gobierno estonio impulsa desde 2001 y que obliga a publicar todas las direcciones de correo electrónico y webs de todos los servicios públicos. Una vez más la democracia y las libertades públicas juegan un papel en favor de los «malos».

Objetivos

El tipo de objetivos es una evidencia de que los ataques no fueron espontáneos y fueron meticulosamente estudiados para conseguir una mayor daño a nivel político, económico, comercial y de comunicaciones y en definitiva de pérdida de confianza y reputación de un país que tiene por orgullo ser uno de los países más comprometidos con la tecnología de la información y la ciber sociedad (41).

(41) Datos extraídos de http://estonia.eu/about-estonia/economy-a-it/economy-at-a-glance.html que dan idea de la vinculación de Estonia con la ciber sociedad:
- 76% de la población de 16 a 74 años son usuarios de Internet (2010, Estadísticas de Estonia).
- 63% de los hogares tiene acceso a Internet (2009, Estadísticas de Estonia).
- Todas las escuelas de Estonia están conectados a Internet.
- Todas las ciudades de Estonia y los pueblos están cubiertos por la red de puntos públicos de acceso a Internet.
- Hay más de 1100 zonas de Internet inalámbrico gratuito en todo el país. Más información: www.wifi.ee
- Los ingresos pueden ser declarados a la Administración Aduanera y Tributaria a través de Internet. En 2010, el porcentaje de declaraciones de impuestos electrónicas fue del 92%.
- Los gastos efectuados en el presupuesto general del Estado se pueden seguir en Internet en tiempo real.
- El Gobierno ha cambiado las reuniones del gabinete por sesiones sin soporte de papel mediante un sistema de documentación basado en web.
- Todo el territorio de Estonia tiene garantizada la cobertura de telefonía móvil digital.

Los objetivos políticos más atacados fueron las webs, redes y servicios del gobierno, primer ministro, presidente de la república, parlamento, oficina de estudios estatales, ministerios, policía y partido política del gobierno.

Estonia es un país donde la actividad política, –y me refiero al trabajo propio de los políticos en el desempeño de sus funciones–, se realiza mayoritariamente a través de sistemas de las tecnologías de la información. Las sesiones del gobierno y los consejos de ministros se realizan exclusivamente a través de intranet, evitando casi al 100% la burocracia del papel. Un ataque con éxito a las redes que controlan dicha actividad provocan de inmediato una crisis de comunicación política.

Los objetivos económicos estuvieron enfocados principalmente en los servicios de e-banking de los principales bancos nacionales, Hansapank y SEB Eeesti Uhispank. Estonia ofrece un perfil adecuado para facilitar a un ciber atacante el estudio y la decisión de los objetivos financieros: los dos bancos mencionados controlan el 80% del mercado bancario nacional con lo que se facilita la concentración de los ataques y los ciudadanos estonios hacen uso mayoritariamente de los servicios bancarios a través de internet –del orden del 90% de todas las transacciones bancarias se realizan electrónicamente– con lo que el daño está asegurado.

A día de hoy las entidades bancarias afectadas no han hecho públicas las pérdidas sufridas debido a los ciber ataques.

A los daños producidos por los ciber ataques hay que añadir los daños comerciales debido al cierre de la frontera de la Federación Rusa a transportes de gran tonelaje procedentes de Estonia, coincidiendo en tiempo con los ciber ataques. Otra evidencia del interés de la Federación Rusa en causar daño a Estonia.

Los objetivos de comunicaciones se enfocaron en los proveedores de servicios de internet más importantes, Elion, Elisa y Starman; en los administradores de servicios de nombres de dominio, DNS Nacional, EEnet y en los medios electrónicos de comunicación más influyentes: Postimees, Delfi, EPL y Baltic News.

En definitiva Estonia reunía una serie de requisitos que la hacían altamente atractiva para sufrir un ciber ataque masivo por parte de su vecino, la Federación Rusa, principal sospechoso de instigar y organizar los ataques:

1. La entrada de Estonia en la OTAN no fue vista con muy buenos ojos por parte de su vecino. El «soldado de bronce» es una excusa perfecta y elemento catalizador para iniciar un conflicto con un país no amigo con ánimo de causar daño (42).
2. Estonia es un país con una dependencia grande de las tecnologías de la información con lo que un ciber ataque puede ser una buena elección si se quiere causar mucho daño sin obtener a cambio ninguna baja, perjuicio o imputación legal.
3. Estonia es un país de dimensiones reducidas (43) y perteneciente a la OTAN, con lo que un ciber ataque masivo puede dar lugar a una situación de crisis de seguridad nacional y así de paso comprobar y estudiar la fortaleza y la capacidad cibernética de las alianzas internacionales.

   Ene Ergma (44), portavoz del parlamento estonio, declara «Estonia es un estado miembro de la OTAN, un ataque a Estonia es una manera de comprobar las defensas de la Alianza. Los atacantes pueden examinar la capacidad de respuesta de la OTAN bajo la tapadera del conflicto «soldado de bronce». Cuando observo una explosión nuclear y la explosión sucedida en mi país en mayo, veo la misma cosa, como la radiación atómica, la ciber guerra no hace sangre pero lo destruye todo» (45).

La respuesta técnica

La respuesta técnica a los ataques fue variada, básicamente el proceso fue el siguiente: primero, se eliminaron las funcionalidades de los servicios web para ahorrar ancho de banda, segundo se solicitó más ancho de banda al proveedor y finalmente se cortaron las conexiones con el extranjero.

El 30 de abril de 2007 el gobierno estonio bloqueó el tráfico de internet procedente de Rusia, filtrando todas las direcciones con extensión «punto ru» (.ru). Al día siguiente los proveedores de servicios de internet

(42) Op. Cit. 14.

(43) Estonia tiene una superficie de 45.228 km2, similar a la extensión de la comunidad autónoma de Aragón (47.720 km2) y una población de 1.340.415 habitantes, inferior al municipio de Barcelona (1.621.537). www.estonia.eu.

(44) Ene Ergma, científica y política, doctora por el Instituto Ruso de Investigación Espacial. Portavoz del parlamento estonio.

(45) Ene Ergma en una entrevista concedida a Josua Devis para wired.com. http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia#ixzz10MKnJXOC

de Estonia se vieron forzados a suspender el servicio a todos los clientes durante medio minuto para poder reinicializar las redes (46).

Como ejemplo significativo valga comentar el caso del Postimees (47), el periódico electrónico de más tirada en Estonia(48). Ago Väärsi, editor jefe, descubrió el 28 de abril de 2010 que sus servidores de páginas estaban inundados de peticiones (más de 2,3 millones) y quedaron fuera de servicio más de 20 veces. Habitualmente la capacidad no usada de los servidores es de un 30 %, por lo que la capacidad de los servidores mantienen un margen de seguridad para demandas extras, pero en este día la capacidad no usada de los servidores empezó a caer drásticamente, 20%, 10%, 5%, 0%, el sitio web es inaccesible por saturación.

El correo no deseado –spam– sobrecargaba los servidores y se come todo el ancho de banda; Väärsi elimina la funcionalidad de comentarios para ahorrar ancho de banda, pero los atacantes variaban sus formas de ataques y mantenían fuera de servicio a los servidores.

Ante nuevos ataques Väärsi estaba preparado, no solo había eliminado la posibilidad de comentarios sino que había hecho las páginas mucho más ligeras eliminando la publicidad y las fotografías, pero los servidores seguían fuera de juego.

Se vio obligado a solicitar un aumento de ancho de banda a su proveedor Elion, pero con 110 Mbps, el máximo disponible, no era suficiente para mantener los servidores operativos.

Inmerso en el estudio de la situación, descubre que la mayoría de peticiones de acceso procedían de Egipto, seguido por Vietnam y Perú –evidentemente no era debido a un repentino interés de los egipcios, vietnamitas o peruanos en la vida social de Estonia o en la lengua estonia–, por lo que decidió cortar la conexión con el extranjero. El ancho de banda se recuperó inmediatamente, el servicio comenzó a funcionar pero sólo en Estonia, el periódico no podía informar al mundo de lo que estaba pasando. Batalla perdida.

La misma medida de cortar la conexión con el extranjero fue tomada por bancos y organizaciones gubernamentales.

---

(46) Peter Finn en un artículo en el Washington Post, 19 de mayo de 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

(47) www.pstimees.ee

(48) En Estonia el 40 % de la población lee el periódico diariamente por internet.

Hillar Aarelaid, el jefe del equipo nacional de respuesta ante incidentes informáticos (CERT), fue encargado por el gobierno de Estonia de la coordinación de la respuesta en el conflicto, pero el CERT estonio no tiene más capacidad para hacer frente a grandes botnets dispersadas por el globo que la de desconectar a Estonia del resto del mundo.

La lucha contra las botnets requiere una defensa basada en una coordinación internacional. Aarelaid necesitaba del apoyo de influyentes personalidades con capacidad de tomar decisiones sobre la conectividad de internet a nivel mundial. A tal efecto se reunió, el 8 de mayo de 2007, con Kurtis Lindqvist, Patrick Fälstrom y Bill Woodcock (USA).

Inmediatamente, Aarelaid y su equipo comenzaron examinar el tráfico para descubrir las fuentes originales de los ataques. Entre otros hallazgos encontraron una botnet, compuesta por ordenadores situados en los EE.UU. que habían sido secuestrados.

Pero la respuesta técnica es claramente insuficiente. Lauri Alman comenta como ejemplo, que cuando empezaron a anular botnets con la ayuda de la Unión Europea y de los Estados Unidos, los administradores de las botnets fueron lo suficientemente astutos como para trasladar las botnets a jurisdicciones menos amigables o menos desarrolladas jurídicamente, de tal manera que la cooperación con Estonia no era posible (49).

Después del ataque, Estonia toma una serie de medidas técnicas encaminadas a fortalecer la capacidad de prevención y respuesta ante incidentes informáticos, entre las cabe destacar, fortalecer la infraestructura vertebral de Internet (backbone), ampliar las conexiones con la «World Wide Web» para que la capacidad en Internet sea más difícil de desbordar, integrar todos los servicios electrónicos del gobierno en un solo sistema centralizado (X-Road) y ampliar e invertir aún más en la capacidad de detectar ataques cibernéticos.

La respuesta política

En general, las naciones aisladamente no tienen capacidad para hacer frente a ciber ataques masivos cometidos a través de botnets dispersadas por el mundo.

(49) Op.Cit. 14

Las naciones no tienen capacidad técnica para ejecutar acciones sobre el tráfico de internet que circula por redes que físicamente se encuentran fuera de su territorio y no tienen competencia jurídica para imponer sus leyes fuera de su jurisdicción; por lo tanto sólo y exclusivamente desde la cooperación internacional se puede abordar el problema.

Relevantes son las palabras del Presidente de la República de Estonia en su discurso del 24 de septiembre de 2010 en la asamblea general de las Naciones Unidas, en el que recuerda que para hacer frente a los desafíos de seguridad del siglo veintiuno, es indispensable la cooperación exitosa entre todos los estados, organizaciones internacionales y regionales; y en este sentido, las amenazas informáticas no son una excepción; e insta a la construcción de una capacidad amplia transfronteriza e intersectorial para la protección de las infraestructuras críticas de información. La necesidad de una cooperación más estrecha entre los Estados, el sector privado y la sociedad civil es urgente ya que en caso de un ataque cibernético, todas las medidas tradicionales de seguridad podrían ser inútiles (50).

El apoyo internacional en Estonia fue organizado por el Ministro de Defensa, quién inmediatamente puso en conocimiento de la situación a sus aliados de la OTAN y de la Unión Europea.

Era claro que el artículo 4 (51) del Tratado de Washington, respaldaba a Estonia para requerir una consulta formal de los estados miembros de la OTAN, por considerar el conflicto como un caso que afectaba a la seguridad nacional y a la independencia política.

Pero el requerimiento de la aplicación del artículo 5(52) del Tratado era un paso de tuerca más que debía ser cuidadosamente meditado y

---

(50) Toomas Hendrik Ilves, presidente de la república de Estonia, en su discurso en la asamblea general de las Naciones Unidas, New York 24-09-2010. http://president.ee/en/speeches/speeches.php?arhiiv=2010

(51) Tratado de Washington, 4 de abril de 1949, **artículo 4**. Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada.

(52) Tratado de Washington, 4 de abril de 1949, **artículo 5**. Las Partes acuerdan que un *ataque armado* contra una o más de ellas, que tenga lugar en Europa o en América del Norte, ser considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudar a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas

finalmente fue descartado, según se desprende de las palabras que en su día pronunció el Ministro de Defensa estonio, «en estos momentos la OTAN no define claramente el ciber ataque como una acción militar…, ningún ministro de defensa de un estado miembro definiría un ciber ataque como una acción militar a día de hoy (53)».

En un primer momento, Estonia obtuvo la cooperación de sus aliados en la Unión Europea y Estados Unidos para anular botnets; seguidamente con la ayuda de sus aliados aumentó su capacidad en internet (ancho de banda, troughput) pero tuvo que hacerlo gradualmente y sin revelar la capacidad real, debido a que la red era constantemente monitorizada por los atacantes para, entre otras cosas, tener información puntual del ancho de banda de la infraestructura nacional estonia y modificar sus ataques de acuerdo con la inteligencia obtenida.

Observadores de los CERTS nacionales de los Estados Unidos y de la OTAN visitaron Estonia durante el 8 y 10 de mayo para observar de primera mano la situación y dar apoyo técnico. El CERT nacional de Finlandia fue especialmente útil para llevar a cabo la coordinación internacional entre CERTs nacionales.

El simple hecho de difundir la noticia de que Estonia había consolidado una cooperación internacional para localizar a los ciber criminales y ponerles ante la justicia, hizo que el número de atacantes disminuyera (54).

Después del ataque el gobierno estonio toma una serie de medidas políticas encaminadas a fortalecer la capacidad de prevención y respuesta ante incidentes informáticos, entre las cabe destacar: a) la firma de acuerdos de cooperación en incidentes informáticos con las principales entidades bancarias estonias, con los principales proveedores de servicio de internet y con las principales operadoras de telecomunicaciones; b) el impulso de iniciativas en el seno de la OTAN y de la Comisión Europea encaminadas a la cooperación con el sector privado; y c) el desarrollo y puesta en marcha de la Estrategia Nacional de Ciberdefensa

---

que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.

(53) Op. Cit. 43 (3)

(54) Ibid

en la que identifica la infraestructura de información crítica y las acciones necesarias para su defensa.

Estonia dio al mundo tres lecciones de respuesta política a un ciber ataque masivo contra la seguridad nacional.

1. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional.
2. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica.
3. Reconocieron desde el primer momento ante el mundo que estaban siendo víctimas de un ciber ataque (55).

Estas tres acciones fueron posibles debido a la formación y conocimiento que los políticos estonios tienen sobre el mundo de las tecnologías de la información; incluyendo el Presidente de la República de Estonia, Toomas Hendrik Ilves, que ha ejercido en diversos ocasiones de orador de apertura en conferencias internacionales relacionadas con el tema y demostrando un amplio conocimiento (56).

La respuesta legal

Toda respuesta legal ante este tipo de ciber ataques tiene dos caras, la nacional y la internacional. La nacional, con la aplicación de la legislación nacional aplicable a estos casos y la internacional, con la aplicación de los acuerdos bilaterales y multinacionales de cooperación en materia criminal.

Las autoridades estonias consideraron que los ciberataques debían ser tratados como crímenes cibernéticos y debían ser castigados de acuerdo con el código penal estonio y perseguidos e investigados de acuerdo con las leyes nacionales y los acuerdos internacionales.

Pero Estonia se encontró con dos problemas legales de difícil solución:

---

(55) No es práctica habitual por parte de ningún gobierno ni gran empresa reconocer que se ha sufrido un ciber ataque con éxito debido al miedo a la pérdida de fiabilidad y reputación.

(56) Ejemplos de sus discursos se pueden encontrar en la web oficial del presidente de la republica, www.president.ee. es digno de destacar su discurso de inauguración de la Conferencia sobre ciber conflictos, Tallinn 16-06-2010.

1.º Los legisladores estonios no previeron los ciberataques en la dimensión de lo acontecido en Estonia y la máxima pena prevista en el código penal, en la época del conflicto, para delitos de ataques cibernéticos era de un año. Esto hacía inviable la investigación en internet con el fin de identificar a los atacantes, pues la legislación estonia solo permitía la recolección y análisis de datos extraídos por medios electrónicos de internet relativos a personas individuales cuando el crimen que abre el proceso de investigación tiene asociado una pena de más de tres años (57).
2.º Cuando los atacantes, debido a la cooperación internacional, vieron que sus botnets estaban siendo anuladas movieron sus redes a jurisdicciones con menos o ninguna disposición o capacidad a cooperar, es decir movían sus elementos de ataque a «paraísos legales cibernéticos», como Egipto, Vietnam o Perú.

La cooperación internacional dio sus frutos en forma de alejar las botnets de sus territorios y de identificar potenciales direcciones IP fuente de los ataques, pero, por un lado, el desplazamiento de las botnets a paraísos ciber legales y por otro, el rechazo de países, como Rusia, a identificar, aprehender y poner a disposición judicial a las personas asociadas con las mencionadas direcciones IP hicieron infructuoso todo el trabajo legal acometido por las autoridades estonias (58).

El 10 de mayo de 2007, la oficina del fiscal general de Estonia, Norman Ass, tramitó un escrito oficial a su homólogo de la Federación Rusa, en base al acuerdo de ayuda legal mutua entre los dos países firmado en 1993, en la que se exhortaba a identificar a las personas que habían tomada parte en los ataques. En el escrito se incluía información detallada de direcciones IP, sitios web y foros de internet localizados en territorio de la Federación Rusa que estaban involucrados en los ataques.

Una de las direcciones IP implicadas pertenecía al gobierno de la Federación Rusa (59) y fuentes oficiales estonias declaraban que en la

(57) Op. Cit. 31. // Paradójico, la democracia y las libertades públicas impidieron la persecución de delitos que atentaban contra la propia democracia y las libertades públicas.
(58) Es claro desde un punto de vista legal, que solo las personas individuales y no las direcciones IP pueden ser puestas a disposición judicial.
(59) Gadi Evron, en su artículo «Battling botnets and online mobs» en la revista «Science & Technology» Winter/spring 2008, página 125.

investigación forense habían identificado direcciones IP que pertenecían a la administración presidencial y agencias estatales rusas (60).

Un año y un mes más tarde de la petición, Estonia recibe la respuesta en la que Rusia rechazaba la cooperación alegando que lo requerido no estaba contemplado en el acuerdo de ayuda legal mutua del 93.

La falta de cooperación de Rusia era tan manifiesta que incluso Rein Lang, Ministro de Justicia estonio llego a declarar sobre las autoridades rusas: «ni siquiera descuelgan el teléfono» (61).

A día de hoy sólo una persona relacionada con el conflicto, Dmitri Galushkevich (62), ha podido ser declarado culpable. Su delito, «bloqueo ilegal de datos informáticos con el propósito de obstaculizar el funcionamiento de un sistema informático»; la condena, el pago de una multa de 22.900 coronas estonias (1.464 Euros).

En definitiva, el caso Estonia lanza un mensaje al mundo: «cometer ataques cibernéticos puede salir gratis o, en todo caso, muy barato».

Investigación forense

Una vez que se recupera la normalidad en la vida de los estonios, es momento de hacer análisis y valoración de los hechos.

La investigación forense se basa en la recolección y estudio de toda la actividad cibernética registrada (63) y rastrea la ruta de los ataques en sentido inverso hasta llegar a la fuente o centro de mando y control de la botnet.

Para acceder hasta el origen es necesario el permiso y la cooperación de las autoridades de los territorios por donde el ataque transcurrió, y como ya se ha mencionado previamente, en el caso de la Federación Rusa, el permiso no fue obtenido.

A partir de este hecho se abren todo tipo de especulaciones e hipótesis, ya que, las direcciones IP asociadas a organismos estatales y gubernamentales rusos, podían ser los orígenes de los ataques o podían

(60) Op. Cit. 29
(61) Ibid
(62) Dmitri Galushkevich, ciudadano estonio de etnia rusa, en el momento del ciber conflicto tenía 19 años de edad y estudiaba en la Universidad de Tecnología de Tallinn.
(63) Mediante el análisis de logs.

ser direcciones IP asociadas a máquinas secuestradas que formaban parte de la ruta o itinerario del ataque, pero no el origen.

Diferentes datos ilustran sobre la magnitud del evento: más de 178 países estuvieron involucrados (64); 128 ataques DDoS en dos semanas, de los cuales, 58 fueron en un solo día; y algunos ataques llegaron hasta los 200 Mbps(65).

Conclusiones

– La implicación de Rusia y de ciudadanos rusos en los ataques no ofrece ninguna duda a la luz del número de evidencias recolectadas: el tráfico malicioso a menudo contenía elementos de motivación política en lengua rusa, instrucciones precisas de cuándo, cómo y qué atacar fueron diseminadas por números foros, blogs y sitios web rusos (66).
  Según Ene Ergma, los ciberataques fueron un test para comprobar la capacidad de respuesta y el nivel de organización de la OTAN (67). Según Rain Ottis, fueron una operación de información rusa contra Estonia (68).
  Pero sin duda los datos más consistentes de la implicación de las autoridades rusas en el asunto, si bien no claramente como autores materiales pero sí como inductores, colaboradores necesarios o cómplices, son: a) la renuncia por parte del gobierno ruso a acatar el acuerdo de ayuda legal mutua con Estonia, b) la dejación de funciones por parte de las autoridades rusas en el bloqueo durante dos semanas de la embajada estonia en Moscú o en la agresión a la embajadora y c) la presión económica ejercida por Rusia coincidiendo con los ciberataques, evidenciada por el corte de la frontera a transportes pesados procedentes de Estonia, cancelaciones de contratos de importación de productos fabricados en Estonia, cancelación de transportes ferroviarios, como el que unía San Petersburgo con Tallín, etc. (69).

(64) Según Katrin Parmage, portavoz del Centro Informático Estatal de Estonia en un artículo de Marge Tubalkain-Trell para el Baltic Bussiness News, http://balticbusinessnews.com/?PublicationId=b737410e-e519-4a36-885f-85b183cc3478
(65) Op. Cit. 31
(66) Op. Cit. 14
(67) Op. Cit 48
(68) Op. Cit 11
(69) Op. Cit 14

– La amenaza cibernética es real y muy atractiva para los que quieran causar un gran daño corriendo mínimos riesgos.
– La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura crítica nacional conllevando riesgos de daños físicos para la población.
  Un ejemplo claro de esto es el «gusano Stuxnet», un código malicioso que, según los investigadores, es capaz de tomar el control de los sistemas de control automatizados de las fábricas que previamente ha infectado y puede llevar a cabo acciones para las que está programado.
  A través de la ingeniería inversa del código del Stuxnet, expertos en ciber seguridad de los Estados Unidos declaran que el «Stuxnet es esencialmente un misil cibernético de precisión de carácter militar, desarrollado a principios de 2009 y diseñado para destruir un objetivo de alta importancia del mundo real, como una planta nuclear».
– El derecho a disponer de ciber armamento, es un derecho de toda sociedad democrática para poder hacer frente, con los mismos medios, a aquellos que quieren perjudicar sus legítimos intereses.

Otro ciber caso interesante, por ser el primer caso en el que se combinan operaciones militares y operaciones cibernéticas, es el Caso Georgia 2008. Como en el caso Estonia, hay hechos suficientes que inducen a pensar que el gobierno de la Federación Rusa estuvo detrás de la coordinación de las ciber operaciones, pero, a día de hoy, la demostración legal no es posible.

EL CIBER CASO GEORGIA 2008

Presumiblemente, y acorde con el análisis lógico de los hechos acontecidos, Rusia acumuló experiencia en la desestabilización de países a través de las ciber operaciones contra Estonia en 2007 y contra Lituania en 2008. ¿Por qué no dar un paso más y combinar las operaciones armadas con las cibernéticas?

Después de su experiencia con Estonia y Lituania, la primera oportunidad que se le presenta para practicar su capacidad conjunta «Fuerzas Armadas - Fuerzas Cibernéticas» es en el conflicto con Georgia. Vayamos al asunto.

Antecedentes

Georgia es un país que limita al norte con Rusia, al este con Azerbaiyán, al sur con Armenia y Turquía y al oeste con el Mar Negro. Tiene una población de 4.601.000 habitantes y una superficie total de 69.500 km². Es un país poco desarrollado en materia de tecnología de la información, lo que hace que el desarrollo de sus actividades políticas, sociales y financieras sean poco dependiente de las TI y por consecuencia los ciber ataques causan un menor daño que en el caso Estonia; pero por otro lado, esa falta de desarrollo tecnológico hace que su capacidad de respuesta ante ciber ataques sea también reducida.

Osetia del Sur es un territorio situado en el Cáucaso en la frontera entre la Federación Rusa y Georgia. Tiene una población aproximada de 80.000 habitantes y una superficie total de 3.900 km². Durante la época soviética tenía la consideración de Óblast (70) Autónomo dentro de la República Socialista Soviética de Georgia.

En 1989 la región de Osetia del Sur declaró unilateralmente su independencia tras vencer en una guerra con Georgia y se convirtió en una república independiente de facto, pero Georgia –y la mayor parte de la Comunidad Internacional (71)–, siempre la ha considerado como parte de su territorio, como así lo era en la época soviética.

Debido a esta disparidad de criterios la región era un foco continuo de conflictos. Para tratar de lograr y mantener la estabilidad en la zona, en 1992 se creó una fuerza de mantenimiento de la paz bajo mandato de la OSCE (72). La fuerza de mantenimiento de la paz estaba compuesta por tropas de Rusia, Georgia y Osetia del Sur y el mando lo ostentaba la Autoridad Militar Rusa (73).

El 7 de agosto de 2008 se inició la Guerra de Osetia del Sur entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia por el otro; con una ataque, que por sorpresa, realizaron las Fuerzas Armadas de Georgia contra Fuerzas Separatistas.

---

(70) Óblast: En la extinta Unión de Repúblicas Socialistas Soviéticas, los óblasts eran entidades administrativas de tercer nivel, el primer nivel era la propia URSS, el segundo nivel era la República que a su vez se componía de Óblasts.

(71) A día de hoy, solo Rusia, Abjasia, Nauru, Nicaragua y Venezuela reconocen oficialmente a Osetia del Sur como Republica Independiente.

(72) OSCE: Organización para la Seguridad y la Cooperación en Europa.

(73) Algo así como «poner al lobo a cuidar del rebaño».

Este hecho provocó la reacción inmediata de Rusia, que consideró el hecho un ultraje contra ciudadanos rusos fuera de las fronteras y consideró su obligación defenderles de tal ultraje.

Al día siguiente, el 8 de agosto de 2008, los rusos iniciaron una serie de operaciones militares en territorio de Osetia del Sur, extendiéndose posteriormente a otras regiones de Georgia y al Mar Negro; más allá de la zona de responsabilidad del mandato OSCE de mantenimiento de la paz.

El 9 de agosto de 2008, el presidente de Georgia, Mikheil Saakashvili, declaró el estado de guerra, al considerar los hechos acontecidos como una agresión Militar por parte de la Federación Rusa contra Georgia.

Tres días más tarde, el 12 de agosto de 2008, el Presidente de la Federación Rusa, Dmitri Medvédev, decreta el fin de las operaciones militares rusas en territorio georgiano y acepta el plan de paz propuesto por la Unión Europea; plan que entre otras cosas obliga a las Fuerzas a volver a las posiciones anteriores al comienzo del conflicto.

Cronología de los ciber ataques

Los ciber ataques contra Georgia se produjeron en tres fases diferenciadas:

– 1.ª fase: Pre-conflicto armado. Junio de 2008-7 de agosto de 2008. Ataques de pequeña escala.

Durante este periodo se contabilizaron ataques DDoS de pequeña escala contra sitios web oficiales de Georgia. El primer ciber ataque fue registrado en Junio de 2008, dos meses antes del inicio del conflicto (74). Estos ataques se enmarcan dentro de las tensas relaciones que mantenían Rusia y Georgia

– 2.ª fase: Conflicto armado. 8 de agosto de 2008 – 12 de agosto de 2008. Ataques bien organizados y coordinados.

Durante los cinco días que duró el conflicto armado se sucedieron ciber ataques contra sitios web pertenecientes al Presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias.

(74) Artículo publicado en el «Washington Post» por Kim Hart, el 14 de agosto de 2008, «Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar». http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623_pf.html

El primer ataque a gran escala y con un alto grado de sofisticación en su ejecución se produjo coincidiendo con la primera ofensiva de las Fuerzas Rusas en territorio de Georgia.

Es importante destacar, que a medida que el conflicto armado se intensificaba, a su vez se incrementaba el número de ciber ataques (75).

Deliberadamente o no, el caso es que, los ciber ataques debilitaron la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto; y debilitaron la capacidad de información y de comunicación entre el Gobierno y los ciudadanos, a la vez que, a través de la ciber propaganda, trataron de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

– 3ª fase: Post-conflicto armado. 13 de agosto de 2008 – 28 de agosto de 2008. Ataques de menor escala.

Coincidiendo con la finalización del conflicto armado, el 12 de agosto de 2008, las operaciones cibernéticas sufrieron una importante reducción en número e intensidad pero el conflicto en el ciber espacio, parecía no estar incluido en el acuerdo de paz y las ciber operaciones continuaron hasta el 28 de agosto.

El fin de las operaciones cibernéticas no se debió a ningún tipo de acuerdo, sino a la falta de rentabilidad de los ciber taques. Por un lado las medidas de ciber defensa lograron bloquear gran parte de los ciber ataques y por otro, el entusiasmo de los hacktivistas iba decreciendo después de la finalización del conflicto armado.

El último gran ataque contra Georgia fue registrado el 27 de agosto de 2008.

Tipos de ataques

Los tipos de ataques fueron parecidos al caso Estonia de 2007, no especialmente sofisticados pero si muy efectivos y tuvieron influencia en el desarrollo de las operaciones armadas.

(75) Roland Heickero, Swedish Defence Research Agency, en la publicación «Emerging Cyber Threats and Russian Views on Information Operations». http://www2.foi.se/rapp/foir2970.pdf

Los tipos de ataques llevados a cabo en el caso Georgia fueron principalmente (76):

a) Ataques prolongados y múltiples de tipo «ICMP flood», «TCP SYN flood», «HTTP flood» contra web sites oficiales;
b) Ataques DDoS a través de botnets, con centros de mando y control dispersos en diferentes países, que hacían uso de «scripts» (77) no especialmente sofisticados, mejor organizados –técnica y operativamente–, mejor coordinados, con mayor poder dañino y con un mayor número de participantes que en el caso Estonia, y
c) Ataques de tipo inyección SQL, no especialmente sofisticados pero bien planeados y organizados y que se basaban en reconocimientos de objetivos y evolución continua de los ataques acorde con la inteligencia obtenida. Estos ataques son de difícil detección.

Las redes sociales fueron ampliamente utilizadas como instrumento para reclutar voluntarios y para la descarga de «malware».

Objetivos

La elección de los objetivos perseguía la finalidad de causar una pérdida de capacidad operativa y de confianza en las instituciones políticas, militares y financieras del país y bloquear la capacidad de comunicación entre dichas instituciones, entre el gobierno estonio y sus ciudadanos y entre Georgia y el mundo exterior.

Los objetivos políticos se concretaron en los sitios web del Presidente de la República de Georgia, del Parlamento, del Ministerio de Asuntos Exteriores, del Ministerio de Ciencia y Educación, de Instituciones Educativas (78).

Los objetivos militares se concretaron en los sitios web del Ministerio de Defensa (79).

Los objetivos financieros se concretaron en los sitios web del Banco Nacional de la República de Georgia y de la mayor institución bancaria del país (TBC) (80).

---

(76) José Nazario (Arbor Network) y Andre M. DiMino (Shadowserver Foundation), en la publicación «An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008».
(77) Un script es un programa simple de ordenador, desarrollado para realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario.
(78) www.president.gov.ge, www.parliament.ge, www.mfa.gov.ge, www.mes.gov.ge, www.naec.gov.ee
(79) www.mod.gov.ee
(80) www.nbg.gov.ge, www.tbc.ge

Y los objetivos de comunicaciones se concretaron en los sitios web y foros de las principales agencia de comunicaciones, agencias de noticias y televisión (81).

La respuesta técnica

Georgia disponía de reducida capacidad técnica para hacer frente a los ciber ataques, por lo que la cooperación internacional, tanto institucional como privada fue fundamental para hacer frente a los ataques.

La respuesta técnica en el caso de Georgia fue principalmente el bloqueo del dominio «.ru» y el traslado de los sitios web a otras plataformas fuera de las fronteras georgianas.

La respuesta política

Georgia tuvo gran facilidad para acceder al apoyo multinacional debido a los precedentes de Estonia y Lituania, fundamentalmente.

Estonia contribuyó, de inmediato, enviando expertos del CERT-EE para ayudar en la respuesta técnica. La contribución de estos expertos fue fundamental debido a la experiencia adquirida un año antes. Además, ofreció su infraestructura para alojar sitios web oficiales de Georgia.

Polonia también fue rápida en su apoyo, prestando su infraestructura para alojar sitios web que habían quedado fuera de servicio.

Entre la cooperación privada es de destacar la de las empresas americanas Google y Tulip Systems Inc., cuyo director ejecutivo es un expatriado georgiano, Nino Doijashvili. Ambas, entre otras cosas, cedieron su infraestructura para hospedar las webs atacadas.

La respuesta legal

Como se puede suponer, Georgia encontró las mismas dificultades para forzar una respuesta jurídica en este asunto, puesto que el presunto origen de los ciberataques se sitúa en territorio ruso, y la cooperación para identificar a los responsables no es aceptada por quién tiene facultad para ello.

---

(81) www.forum.ge, www.civil.ge, www.presa.ge, www.aspny.ge, www.rustavi2.com, www.news.ge, www.interpress.ge, www.tblisiweb.info, www.os-inform.com, www.hacking.ge

Pero además en este caso se da la circunstancia de la coincidencia de un conflicto armado y un conflicto cibernético que invita a pensar en la aplicación de la ley de conflictos armados –LOAC–, que se aplica a los conflictos armados internacionales y en la conducción de operaciones militares y de «actividades relacionadas con los conflictos armados».

Investigación forense

El proyecto Grey Goose 2 (82), identificó dos sitios web rusos desde donde se organizaron cibera taques coincidiendo con el conflicto armado: «www.stopgeorgia.ru» y «www.xakep.ru».

En estos sitios se informaba detalladamente de los pasos a seguir para atacar sitios georgianos; se detallaban listas de objetivos, se ofrecían descargas de programas ad hoc para participar inmediatamente en ataques masivos DDoS, se animaba a la participación a simpatizantes con la postura rusa y toda la información era actualizada permanentemente.

La web «stopgeorgia.ru» fue creada poco tiempo después –en pocas horas– de que las Fuerzas Rusas invadieran el territorio de Osetia del Sur; usaba una dirección IP relacionada con el proveedor de servicios Steadyhost –www.steadyhost.ru– que tiene su registro en Nueva York pero que es operado desde San Petersburgo. Se piensa que este proveedor tiene sus oficinas en el mismo edificio que el Centro de Investigación de la Capacidad Militar de Países Extranjeros del Ministerio Ruso de Defensa.

De las investigaciones realizadas por las diferentes instituciones y expertos que siguen ciber incidentes por todo el mundo, como la Fundación Shadowserver o Arbor Networks; se deducen los siguientes datos: a) Los ciber ataques fueron de mayor intensidad que los registrados en el caso Estonia 2007, b) el 90 % de los ataques fueron llevados a cabo por voluntarios o hacktivistas (83) y c) sitios web oficiales de Georgia –incluidos entidades bancarias– estuvieron fuera de servicio durante días.

(82) El proyecto Gery Goose 2 es una iniciativa de Inteligencia de Fuentes Abiertas (Open Source Intelligence -OSINT) lanzada el 22 de agosto 2008 y cuya misión era examinar cómo se desarrollaron las operaciones cibernéticas Rusas contra Georgia y analizar los responsables, en concreto analizar la implicación del gobierno ruso y de los movimientos de voluntarios rusos patrióticos.

(83) Shaun Waterman, «Analysis: Russia-Georgia cyberwar doubted». http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html

Conclusiones

a) Como en el caso Estonia, la participación del gobierno ruso no ha sido probada hasta la fecha; aunque existen suficientes indicios para deducir que Rusia es, al menos, cómplice en la organización de los ciber ataques. Los indicios están fundamentalmente basados en tres hechos: a) la falta de cooperación de Rusia para identificar a los responsables; b) Rusia es el principal o único beneficiario de los resultados de la ofensiva cibernética y c) los ciber ataques evolucionaban acorde con la evolución de las operaciones armadas y para ello se necesitaba información que solo era accesible por parte de las autoridades políticas y militares rusas.
b) Las ciber operaciones estuvieron bien planificadas, organizadas y coordinadas en tiempo y espacio; existían webs donde se emplazaba información detallada para unirse a los ataques y programas ad-hoc para realizar ciber ataques que producían resultados beneficiosos para Rusia en el conflicto armado con Georgia y además, dichos ciber ataques evolucionaban de acuerdo con la inteligencia obtenida. Esto no solo requiere el uso de operaciones cibernéticas ofensivas (CNA (84)) sino de operaciones cibernéticas de explotación (CNE (85)).
c) Las ciber operaciones fueron iniciadas y conducidas en conjunción con las operaciones armadas y sirvieron para debilitar la capacidad de respuesta militar y política de Georgia, como operaciones psicológicas y desmoralizantes al bloquear la comunicación entre el Gobierno y el pueblo georgiano y como operaciones propagandísticas para reclutar adeptos a la causa Rusa.
d) El uso de patriotas voluntarios es una herramienta al alcance de los gobiernos para realizar operaciones cibernéticas (CNO) contra otros países y evitar la imputación legal.

LA CIBERSEGURIDAD EN LA OTAN

El ciber ataque de la primavera de 2007 a Estonia representa un hito y un reto histórico para la OTAN; es la primera vez que un estado miem-

(84) Las operaciones cibernéticas o CNO (Computer Network Operations) se componen de operaciones de ataque (CNA, Computer Network Attack); operaciones de defensa (CND, Computer Network Defence) y de operaciones de explotación (CNE, Computer Network Exploitation).
(85) Ibid.

bro solicita apoyo a la OTAN por un ataque a la infraestructura crítica de información del país.

Se da la paradójica situación de que la mayoría de los expertos en ciber seguridad de la OTAN se enteran de la noticia en Washington, mientras atendían al congreso de ciber seguridad (86) que anualmente organiza la Oficina de Seguridad de la Alianza (87).

Como queda demostrado por los hechos, la OTAN no disponía de una plan de acción en caso de ciber ataque a un estado miembro; hasta ahora se habían considerado problemas de índole nacional, puesto que muchas naciones de la OTAN y en especial los Estados Unidos de América recibían y reciben a diario ciber ataques –de la misma envergadura y mayor– contra la infraestructura crítica de información del país, sin que esto constituya causa de intervención por parte de la OTAN.

Pero el caso de Estonia es diferente, pues debido a la dimensión del país (88), los ataques le llevaron una situación de crisis de seguridad nacional. La intervención de la OTAN, de alguna manera, era más que justificada. Pero no había un plan de acción.

No solo los ciberataques a Estonia representaron un caso de reflexión para la OTAN, también otros casos, como el ciberataque a Lituania (89) en julio de 2008, el ciber ataque a Georgia en julio de 2008 y el ciber ataque a Kirguistán en enero de 2009 (90).

La OTAN se enfrentó con el problema de manera decidida en la cumbre de Bucarest (91), celebrada entre los días 2 y 4 de abril de 2008. Como consecuencia de la reunión se llegó al acuerdo expresado en la sección 47 de la declaración de la cumbre:

> *«La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciber ataques. Hemos adoptados recientemente la Política de Ciber Defensa, y estamos desarrollando las estructuras y autoridades para llevarla*

(86) NATO Cyber Defence Workshop 2007, Washington, Estados Unidos
(87) NOS: NATO Office of Security
(88) Op. Cit. 34
(89) Lituania es un país miembro de la OTAN desde el 24 de marzo de 2004.
(90) Georgia y Kirguiztán son dos naciones con una estrecha relación de cooperación con OTAN a través de su participación en el partenariado por la paz (Partner for Peace) desde 1994.
(91) http://www.summitbucharest.ro/en/1.html

a cabo. Nuestra política en materia de Ciber Defensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciber ataque. Continuamos con el desarrollo de las capacidades de ciberdefensa de la OTAN y con el fortalecimiento de los vínculos entre la OTAN y las autoridades nacionales».

De la declaración se desprenden tres líneas de acción principales: a) medidas a adoptar por la propia OTAN para mejorar su capacidad de ciber defensa, b) medidas a adoptar por las naciones para mejorar la protección de los sistemas de información crítica desplegados en sus territorios y c) medidas a adoptar por ambas partes, OTAN y Naciones, para mejorar la coordinación, el intercambio de información y el apoyo mutuo.

En este capítulo, se tratará de la acción a) medidas adoptadas por la OTAN para mejorar su capacidad de ciberdefensa; dejando las siguientes acciones para otros capítulos de este cuaderno.

La Ciberdefensa en la OTAN

La OTAN a posteriori de los ciberataques a Estonia, realiza un análisis y estudio del caso y elabora un informe de lecciones aprendidas (92).

Como consecuencia del estudio, se concluye que la OTAN no sólo no disponía de un plan de acción en caso de ciber ataque, sino que ni siquiera disponía del concepto de Ciberdefensa y su correspondiente política.

El 7 de enero de 2008, es una fecha clave para la Ciberdefensa en la OTAN; el Consejo firma la Política de Ciber Defensa de la OTAN (93) con el objetivo de mejorar la capacidad de la OTAN para proteger los sistemas de información y comunicaciones (CIS) de importancia crítica para la Alianza contra ciber ataques.

(92) «Report of the examination of the lessons learned from the recent cyber attacks», AC/322-D(2007)0050 -01.10.2007.
(93) «NATO Policy on Cyber Defence», C-M(2007)0120.

Como consecuencia de la política, la OTAN impulsa una serie de acciones para mejorar su capacidad de ciberdefensa, entre las que se destacan:

a) Desarrollo del concepto (94) de Ciberdefensa (95).
b) Impulso y apoyo para adquirir cuanto antes la capacidad operativa completa de respuesta ante incidentes informáticos (96).
   La OTAN disponía de una hoja de ruta para lograr la capacidad operativa completa de respuesta ante incidentes informáticos (NCIRC FOC)(97). El caso Estonia tuvo un efecto catalizador para acelerar el proceso; en el momento de los ataques la OTAN disponía de una capacidad inicial (NCIRC IOC) (98).
   La NCIRC consta de un centro de apoyo y coordinación de ciberdefensa (CDCSC(99)) y de un centro técnico (NCIRC TC)(100), lo que se puede considerar el NATO CERT. En estos dos centros se concentran gran parte de los expertos de seguridad de la OTAN.
   Debido a que la respuesta ante un ciber ataque es multidisciplinar, este centro coordina su trabajo con otras entidades –consejos, grupos de trabajo, agencias, centros, etc– con responsabilidad en diversas materias dentro de la OTAN, como política de la alianza, estandarización, recursos, relaciones públicas, asuntos jurídicos, asuntos económicos, acreditación de sistemas de seguridad, inteligencia, coordinación con países miembros, comunicaciones y otras áreas de seguridad como seguridad del personal, de las instalaciones, de la documentación, etc.
c) Impulso y apoyo para establecer cuanto antes el Centro de Excelencia de Ciber Defensa Cooperativa de la OTAN (CCDCOE) (101).
   El 28 de octubre de 2008 se establece oficialmente en Tallinn, capital de la República de Estonia, el Centro de Excelencia de la OTAN de Ciberdefensa Cooperativa; con la misión de mejorar la

(94) NATO Cyber Defence Concept, MC 0571, 04.02.2008
(95) No se puede profundizar mucho en el tema debido a que la mayoría de la información disponible es clasificada.
(96) Ibid.
(97) NCIRC FOC: NATO Computer Incidents Response Capability Full Operational Capability.
(98) NCIRC IOC: NATO Computer Incidents Response Initial Full Operational Capability.
(99) CDCSC: Cyber Defense Coordination and Support Centre.
(100) NCIRC TC: NATO Computer Incidents Response Capability Technical Centre.
(101) CCDCOE: Cooperative Cyber Defence Centre of Excellence (CCDCOE) Para más información: www.ccdcoe.org

capacidad y cooperación de la OTAN y sus estados miembros en Ciberdefensa a través del desarrollo de programas y proyectos de I+D+I, de formación, de análisis de casos reales y de consulta.
El centro está formado, a día de la publicación de este cuaderno, por personal experto en ciber seguridad procedente de 10 países: Estonia como país anfitrión, Alemania, EEUU, Eslovaquia, Hungría, Italia, Letonia, Lituania, Turquía y España.
La visión del Centro es dar respuestas y soluciones globales a problemas concretos y para ello los proyectos son acometidos por equipos multidisciplinares, en los que se involucran personal experto en ciber seguridad y especializado en tres ramas fundamentalmente: asuntos operativos, funcionales y militares; asuntos tecnológicos, académicos y científicos; y asuntos legales.
El centro depende jerárquicamente de un Comité de Dirección compuesto por representantes de los países componentes (102) y de la OTAN y tiene el estatus legal de Organización Militar Internacional. Dicho estatus le confiere al CCDCOE relación ambivalente con la OTAN; por un lado no forma parte de la estructura de mando la OTAN y por lo tanto no recibe ningún tipo de financiación por parte de la Alianza, y como consecuencia goza de cierta independencia; y por otro lado, está obligado a considerar las peticiones de la OTAN con la más alta prioridad.
Esta ambivalencia le confiere al centro unas características particulares en beneficio de los resultados de los proyectos que acomete: de facto está incluido en la estructura organizativa de ciberdefensa de la OTAN, formando parte del consejo de gestión de Ciber Defensa (NATO CDMB (103), se comenta en el siguiente apartado), mantiene una relación directa y estrecha con ambas partes de la ciberdefensa de la OTAN, la ciberdefensa operativa (NCIRC) y la ciberdefensa estratégica (NATO ACT) (104); pero por otro lado, mantiene una actividad significativa de colaboración con el sector privado y el sector académico y universitario.

d) La creación de la Autoridad para la gestión de la Ciber Defensa (NATO CDMA (105)) (106).

(102) El representante nacional español en el comité de dirección del CCDCOE es el jefe de la sección INFOSEC del Estado Mayor de la Defensa.
(103) CDMB: Cyber Defence Management Board.
(104) NATO ACT: NATO Allied Command of Transformation.
(105) CDMA: Cyber Defence Management Authority.
(106) Op. Cit. 98

La creación de la Autoridad para la gestión de la Ciber Defensa, es quizás el hito más importante en el proceso de construcción de la ciber seguridad de la OTAN. Es el establecimiento de una única autoridad con responsabilidad y medios para coordinar todas las actividades de ciberdefensa y las respuestas ante ciber incidentes. Es como dice el investigador Rex B. Hughes: «al contrario de como sucedió durante el ataque a Estonia, las naciones de la OTAN ahora disponen de un número de teléfono al que llamar en caso de una emergencia cibernética (107)»

La CDMA coordina todos los asuntos de Ciberdefensa a través del consejo de gestión de Ciberdefensa (CDMB) del que forman parte representantes de todas las autoridades de la OTAN, incluyendo el Consejo del Atlántico Norte (NAC); el comité militar (MC), las autoridades de emergencia política y civil, la autoridad de gestión de la política (NPMA (108)) y el comité de seguridad (NSC (109)); y es supervisado por el consejo de gestión de consulta, mando y control (NC3B (110)).

La misión de la CDMA es revisar y coordinar las capacidades de Ciberdefensa de la OTAN, centrándose particularmente en: a) la amenaza cibernética, b) en la gestión del riesgo de seguridad, c) en la valoración de las vulnerabilidades y d) en la continuidad de negocio de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza.

La cuestión es que la capacidad orgánica de Ciberdefensa de la OTAN no es suficiente para parar y disuadir ciber ataques; los ataques a la OTAN pueden ser dirigidos y redirigidos desde fuera del territorio responsabilidad de la OTAN (especificado en el artículo 6 (111) del tratado de Washington, por lo que es necesario que la

(107) El Doctor Rex B. Hughes es cofundador y director del proyecto de Ciberseguridad en Chatham House, Londres y es un investigador asociado de la Universidad de Cambridge-Instituto MIT. Actualmente sus investigaciones se centran en el análisis de cómo la ausencia de un marco coherente de seguridad cibernética a nivel mundial puede amenazar la integridad estructural del orden comercial internacional.

(108) NPMA: NATO Policy Management Authority.

(109) NSC: NATO Security Committee.

(110) NC3B: NATO Consultation, Command and Control.

(111) Tratado de Washington, Art. 6: A efectos del artículo 5, se considerará ataque armado contra una o varias de las Partes, el que se produzca: a) Contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer. b) Contra las fuerzas, buques o aeronaves de cualquiera de las

OTAN trabaje y consolide alianzas con países y organizaciones que no forman parte de la OTAN.

e) La creación de la Autoridad Militar para la gestión de la Ciber Defensa con la misión de revisar y coordinar las capacidades militares de Ciberdefensa de la OTAN (112).

La amenaza cibernética y el artículo 4 del tratado de Washington

El artículo 4 del tratado de Washington dice:

«Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada.»

¿Qué indicadores reflejarían de manera objetiva que un ciber ataque determinado atente contra *la integridad territorial, la independencia política o la seguridad* de un país miembro de la OTAN?

El art. 4 trata exclusivamente del derecho de consulta y a juicio de una sola de las partes, con lo que se entiende que no es necesario que se dé una situación objetiva y de consenso entre todas las partes para ejercer el derecho.

No obstante, debido a las peculiaridades del ciber espacio, no estaría de más que las naciones y la OTAN, estudiaran y redefinieran el concepto de «integridad territorial» y «seguridad». Actualmente el concepto de integridad territorial(113) se ha considerado basado en la defensa de las fronteras físicas de un país. ¿Es este concepto aplicable al ciber espacio?

La amenaza cibernética y el artículo 5 del tratado de Washington

El artículo 5 del tratado de Washington dice:

«Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, sea con-

---

Partes que se hallen en estos territorios, como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer.

(112) Op. Cit 98

(113) La integridad territorial es un principio del derecho internacional que evoca el derecho y deber inalienable de un Estado de preservar sus fronteras de toda influencia exterior. Implica, por lo tanto, que los Estados no deben promover movimientos secesionistas o cambios en las fronteras de otros, cambios que se consideran actos de agresión.

siderado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudar a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.»

Consideraciones al respecto:

1. ¿Qué es un ataque armado?, ¿Se puede considerar un ciber ataque un ataque armado?

   Un ataque armado se puede considerar todo ataque que haga uso de un arma. Y según la Real Academia Española un arma es entre otras acepciones:

   1. *f. Instrumento, medio o máquina destinados a atacar o a defenderse.*

   2. *f. Mil. Cada uno de los institutos combatientes de una fuerza militar. El arma de infantería, de caballería, de artillería*

   4. *f. pl. Conjunto de las armas que lleva un guerrero o una unidad de guerra.*

   Y considera, entre otras, los siguientes diferentes tipos de armas: arma acorazada, aérea, antiaérea, arrojadiza, atómica, automática, blanca, defensiva, de fuego, de mano, de percusión, de precisión, mecanizada, motorizada, naval, nuclear, ofensiva, pesada, semiautomática.

   De acuerdo con la acepción 4. de la RAE, arma es el *conjunto de las armas que lleva un guerrero o una unidad de guerra.* Según esta acepción el conjunto de armas de un ciber guerrero o una ciber unidad estaría basado en hardware y software.

   De acuerdo con la acepción 2. de la RAE, arma es un c*ada uno de los institutos combatientes de una fuerza militar. El arma de infantería, de caballería, de artillería*. Aunque, oficialmente, pocos países consideren el arma o la fuerza cibernética dentro de su estructura de mando militar; de facto es que la mayoría de los países

avanzados gozan de unas fuerzas militares específicas, entrenadas y equipadas para la ciberdefensa (114). La Ciber Fuerza es una realidad.

La acepción que es realmente relevante para el caso que nos ocupa es la primera, arma es un *instrumento, medio o máquina destinados a atacar o a defenderse*.

Según esta definición, no cabe duda de que un código malicioso –software– diseñado para atacar un sistema de información, un sistema de control industrial o una infraestructura crítica, es un arma y por consiguiente un ciber ataque es en toda regla un ataque armado.

En algunos foros se discute que para ser considerado un ataque armado debe haber destrucción física de por medio. Pero a día de hoy nadie discute que existe tecnología suficiente para diseñar códigos que causen destrucción y daños físicos (115).

El artículo 51 de la Carta de las Naciones Unidas reconoce el derecho de legítima defensa al afirmar que «Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de *ataque armado* contra un Miembro de las Naciones Unidas». Con lo cual, la ONU no da más luz al asunto pues abunda en el mismo término, ataque armado.

De acuerdo con lo expresado, el autor considera que un ciber ataque es un ataque armado que puede dar lugar a la invocación del artículo 5 por parte de la nación OTAN víctima.

Otra cosa es, dilucidar en qué situaciones el ciber ataque es lo suficientemente grave como para invocar el artículo 5.

2. ¿Dónde poner el límite de aplicación del art. 5?

   Ardua tarea dilucidar que parámetros pueden ayudar a tomar la decisión de aplicar o no el artículo 5.

   Considerar el volumen o fuerza de los ataques no es muy relevante, pues lo que para países de dimensiones reducidas es una situación de crisis nacional, para otros, como los Estados Unidos, es el pan de cada día. Según José Nazario, el tamaño (100-200 Mbps) de los ataques sufridos por Estonia no es realmente novedoso, es un tipo de ataque de tamaño común (116).

---

(114) Más información en el cuaderno de la cátedra ISDEFE-UPM, «Seguridad Nacional y Ciberdefensa». Ver bibliografía.

(115) En el artículo de F-Secure en http://www.f-secure.com/weblog/archives/00002040.html, se describe minuciosamente cómo un código software malicioso puede causar, entre otras cosas, que una fábrica explosione.

(116) Op. Cit. 24

Además los Estados o grupos beligerantes pueden evitar la aplicación del artículo 5 mediante la utilización de las tácticas de guerra de baja intensidad (117) (118).

Considerar la integridad territorial, la independencia política o la seguridad nacional como criterios es controvertido debido a la falta de objetividad y a la falta de definición de los conceptos en el ciber espacio.

Hoy por hoy la única manera de dilucidar el asunto es caso por caso, pero eso llevaría un tiempo de estudio que podría ser demasiado largo en un tipo de guerra donde la respuesta tiene que ser inmediata.

En definitiva se necesitan planes de acción y equipos de reacción rápida para casos de ciber ataques, independientemente del proceso de toma de decisión de la aplicación del artículo 5; y la OTAN está trabajando en ello.

3. ¿Contra quién se aplicaría el art.5?

   Uno de los grandes problemas de los ciber ataques es lograr la identificación cierta del origen. Como ya se ha demostrado en capítulos anteriores, el limbo jurídico o falta de legislación internacional que facilite la investigación de los causantes de ciber ataques, se encuentren donde se encuentren; las características técnicas intrínsecas del ciber espacio; la guerra de baja intensidad; la presencia o coincidencia de actores de diferente índole: estados, grupos organizados con motivación política o económica, individuos particulares, atacantes secuestrados que desconocen que sus equipos están siendo usados para realizar acciones maliciosas; son verdaderos obstáculos para llegar a atribuir un ataque a un Estado, grupo o individuo.

   En los conflictos tradicionales la crisis se desata entre dos estados claramente definidos –enemigo convencional–. Con la irrupción del terrorismo a gran escala y las actividades en el ciber espacio en la frontera entre lo militar y lo delictivo; la amenaza en muchos casos no tiene cara o una identificación clara y evidente –enemi-

(117) La guerra de baja intensidad es una confrontación político militar entre Estados o grupos, por debajo de la guerra convencional y por encima de la competencia pacífica entre naciones. Involucra a menudo luchas prolongadas de principios e ideologías y se desarrolla a través de una combinación de medios políticos, económicos, de información y militares.

(118) Para más información, ver segunda conferencia «Cyber Warfare: as a form of Low-Intensity Conflict and Insurgency» en la referencia bibliográfica 1.

go asimétrico–. Actualmente la OTAN trabaja considerando todos los casos posibles, amenaza convencional, amenaza asimétrica y amenaza híbrida, la amenaza derivada de la confluencia de acciones convencionales con acciones asimétricas.
Otro hecho relevante a la hora de la toma de decisión de una intervención militar es el hecho evidente de que los límites entre las competencias militar y policial son cada vez más borrosos.

4. ¿Sería aceptable una respuesta tardía?
   En un caso de conflicto convencional o nuclear la respuesta del país atacado se produciría en caliente, es decir inmediatamente después de recibir el ataque y esto sería claramente aceptado por la comunidad internacional de acuerdo al derecho de legítima defensa establecido en el art. 51 de la carta de las Naciones Unidas.
   En el caso de un ciber conflicto de gran escala y en caso de llegar a una atribución clara e inequívoca del atacante, esto llevaría un tiempo que en muchos casos sería de varios meses y esto haría que la respuesta pueda ser entendida más como una represalia que como legítima defensa.

La amenaza cibernética y el artículo 6 del tratado de Washington

El artículo 6 del tratado de Washington dice:

> *«A efectos del artículo 5, se considerará ataque armado contra una o varias de las Partes, el que se produzca:*
>
> *a) Contra el **territorio** de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer.*
>
> *b) b) Contra las **fuerzas, buques o aeronaves** de cualquiera de las Partes que se hallen en estos territorios, como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer.»*

En el caso de la aplicación del artículo 6, estamos ante la disyuntiva de saber qué se entiende por territorio o por fuerzas en el caso de un conflicto en el ciberespacio.

Conclusiones

La OTAN debe hacer un esfuerzo de renovación de acuerdo al tipo de amenaza al que se enfrenta en la actualidad y al que se enfrentará en el futuro; y eso pasa por considerar el hecho cibernético en: a) la definición de conceptos, estrategias, doctrinas y procedimientos; b) en sus formas de actuación y c) en su ámbito de influencia internacional; consolidando colaboraciones y acuerdos entre la OTAN y Estados No-OTAN, el sector privado y organizaciones no gubernamentales. La OTAN está en ello.

BIBLIOGRAFÍA

Conference on Cyber Conflcit, Proceedings 2010. **Czosseck, Christian; Podins, Karlis;.** Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010. ISBN 978-9949-9040-1-3.

The Virtual Battlefield: Perspectives on Cyber Warfare. **Czosseck, Christian; Geers, Kenneth;.** Tallinn: IOS Press BV, 2009. ISBN 978-1-6750-060-5.

Tikk, Eneken; Kaska, Kadri; Vihul, Liis;. *International Cyber Incidents, Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

Frameworks for international cyber security. **Tikk, Eneken.** Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

Coleman, Kevin G. *Cyber Commander's Handbook, the Weaponry & Strategies of Digital Conflict.* Pittsburgh, PA: Technolytics, 2010. ISBN 978-0-578-03935-02995.

Pastor Acosta, Oscar; Pérz Rodríguez, José Antonio; Arnáiz de la Torre, Daniel; Taboso Ballesteros, Pedro;. *Seguridad Nacional y Ciberdefensa.* Madrid: Cátedra ISDEFE-UPM, 2009. ISBN 978-84-7402-364-0.

(SEMA), Sweedish Emergency Management Agency. *Large Internet Scale Attack.* Stockholm: Sweedish Emergency Management Agency (SEMA), 2008. ISBN 978-91-85797-14-1.

Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Stockholm: Sweedish Defence Reserach Agency, 2010. ISSN 1650-1942.

Ottis, Rain. *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2008.