ieee.es
Instituto Español de Estudios Estratégicos
1970 — 2020

Documento
Opinión

12/2020 17 de febrero de 2020

Gabriel Sánchez-Román Urrutia *

Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el ciberespacio

Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el ciberespacio

Resumen:

Las acciones ofensivas en el ciberespacio, o la simple presunción de contar con la capacidad de poder realizarlas, se están convirtiendo en métodos de disuasión cada vez más utilizados por los actores amenaza actuales del ciberespacio. Estos métodos de disuasión pueden ser comparables, por ejemplo, a la tenencia de submarinos por parte de los contendientes en la Segunda Guerra Mundial. Hoy en día, grupos organizados, como las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés), realizan acciones ofensivas en el ciberespacio que no pueden ser atribuidas a ningún Estado de manera certera. Sin embargo, debido a las infraestructuras de mando y control que utilizan, hecho que denota un fuerte apoyo económico detrás, la observación de sus Tácticas, Técnicas y Procedimientos (TTP) y los objetivos de sus acciones, hacen que se pueda aproximar la atribución a un determinado país. Las acciones en el ciberespacio, que tienen cada vez más influencia en las operaciones militares en sus dominios tradicionales (tierra, mar y aire), han irrumpido con fuerza en el marco de la guerra híbrida y la sola presunción de tener la capacidad de realizarlas podrá ser utilizada por los Estados como medida de disuasión para evitar ser atacados.

Palabras clave:

APT, guerra híbrida, submarinos, disuasión, ciberdefensa, ciberseguridad, guerra asimétrica, ciberguerra.

Advanced Persistent Threats (APT) as a deterrence measure in the cyberspace

Abstract:

Offensive actions in cyberspace and their potential performance are deterrence methods more and more used by threat actors in cyberspace, in the same way that submarines were used by some countries in the World War II. Nowadays, organized groups such as Advanced Persistent Threats (APT) perform offensive actions in the cyberspace. The truly attribution of offensive actions is not possible. Nevertheless, according to their Command and Control infrastructures, they are a strong economic support. From their observed Tactics, Techniques and Procedures (TTP) and their selected targets the attribution to a country could be guessed. Actions in the cyberspace are more and more influent in military operations in all of traditional domains. Offensive actions in cyberspace are strongly present in hybrid warfare. The potential performance of these actions will be probably used by States as a deterrence method in order to avoid being attacked.

Keywords:

APT, hybrid warfare, submarines, deterrence, cyberdefense, cybersecurity, asymmetric warfare, cyberwarfare.

Cómo citar este documento:

SÁNCHEZ-ROMÁN URRUTIA, Gabriel. *Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el ciberespacio*. Documento de Opinión IEEE 12/2020. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción

Como primera aproximación en la búsqueda de un símil de la disuasión en el ciberespacio, se tiende irremediablemente a una comparativa con la disuasión nuclear. A pesar de que ambas pueden provocar efectos devastadores, ciertas diferencias como la actividad en situación normal (nula en lo nuclear e incesante en el ciberespacio) y la certitud en la autoría y el armamento controlado en el panorama nuclear, frente a la compleja atribución y la variedad de «armamento» en el ciberespacio hacen que sean dos maneras de disuadir completamente diferentes.

El ciberespacio como un entorno *per se* asimétrico se trata de un dominio casi infinito donde las fronteras no están definidas. Las armas que se utilizan son muy específicas y prácticamente cualquiera, con los conocimientos necesarios, puede «fabricar» una. Además, la infinidad de actores que existen y el marco legal tan complejo en el que se encuadra, refuerza su condición asimétrica y, como adaptación a las nuevas tecnologías, por ende, su condición híbrida. La batalla que se libra en el ciberespacio encaja perfectamente dentro del concepto, relativamente nuevo, de guerra híbrida.

El general ruso Gerasimov, jefe de Estado Mayor de la Defensa y uno de los grandes impulsores de la guerra híbrida[1], defiende que el uso del ciberespacio tiene una enorme influencia en el combate que se libra en todos los dominios de guerra tradicionales (tierra, mar y aire) y que cobra aún más importancia en tiempo de paz. Las campañas de desinformación y de influencia y el cómo contrarrestarlas, concepto conocido como STRATCOM (*Strategic Communications*), en redes sociales o en la opinión pública pueden decantar la balanza hacia un lado u otro.

Dicho esto, la aproximación de la disuasión en el ciberespacio podría asemejarse a la que tuvieron los submarinos en las dos guerras mundiales. Tras la Segunda Guerra Mundial, el entonces primer ministro del Reino Unido, Winston Churchill, dijo: «Durante la guerra, he tenido miedo a una sola cosa, los submarinos», una frase que denota la importancia que tuvieron o pudieron llegar a tener los submarinos en la segunda de las grandes guerras.

[1] MONAGHAN, A. “The ‘War’ in Russia: Hybrid Warfare”. 2015.

A pesar de que ya participaron en la Primera Guerra Mundial, los submarinos llegaron a suponer en la segunda de las contiendas una gran amenaza para los Aliados, creyendo en un momento determinado tener la guerra casi perdida si los submarinos alemanes seguían hundiendo buques mercantes al ritmo que lo hacían.

Hoy en día, el ciberespacio se encuentra en un punto de inflexión muy similar a este. Resulta ser un dominio donde uno de los actores-amenaza deja, en ocasiones, en clara indefensión a algunos Estados —y por supuesto a las empresas—. Este actor amenaza, es lo que a la mar era el submarino en la Segunda Guerra Mundial, y no es otro que las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés).

Ante semejante panorama, surgen varias preguntas que podrían ser contestadas en los próximos años: ¿Serán los Estados capaces de sobreponerse a la amenaza como hicieron los Aliados en la Segunda Guerra Mundial? ¿Dejará de ser algo encubierto para que los Estados amedrenten a otros por la tenencia o no de APT?

Actores amenaza en el ciberespacio y su uso disuasorio

En el ciberespacio existen una gran cantidad de actores-amenaza que podrían clasificarse según su motivación a la hora de perpetrar un ciberataque. Por una parte, están los cibercriminales, cuyo objetivo principalmente es económico y realizan más de la mitad de los ciberataques que se producen en el ciberespacio. Por otro lado, el conocido como «hacktivismo», es una de las mayores motivaciones a la hora de realizar un ciberataque. De hecho, de este movimiento «hacktivista» nació uno de los actores más conocidos del ciberespacio, Anonymous[2].

Si nos centramos en objetivos más gubernamentales, se dan dos motivaciones principales: ciberespionaje y ciberguerra.

[2] COLEMAN, G., *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Versobooks, 2015.

El ciberespionaje podría tener una connotación comercial, ya que ciertas empresas podrían espiar a su competencia más directa a la hora de mantener su hegemonía en ciertos productos o servicios. Sin embargo, el aspecto gubernamental es el que predomina en el campo del ciberespionaje y, por ende, de la ciberguerra. Mientras que los actores que realizan «hacktivismo» son «conocidos» debido a que quieren difundir al mundo sus acciones y los cibercriminales son criminales al uso con un aspecto ciber, el ciberespionaje y la ciberguerra es un terreno oscuro.

Al igual que ocurre con la inteligencia tradicional, se sospecha que los servicios de inteligencia de los países realizan acciones en el ciberespacio y financian a organizaciones para que se las realicen. Estas organizaciones son conocidas como APT. Las APT[3] están formadas por un personal con muy altos conocimientos y con un alto nivel de financiación que proviene, presuntamente, de un Estado en base a sus objetivos. Los objetivos o intereses por los que se mueven hacen tener una ligera idea de los puntos de unión de estas organizaciones con Estados y su respaldo económico. Empresas de ciberinteligencia como Fireye o Symantec catalogan a estos grupos mediante un número —APTXX— o un término escogido según las campañas realizadas.

La labor de las empresas de inteligencia a la hora de descubrir las tácticas, técnicas y procedimientos ha sido fundamental a la hora de realizar una agrupación de las APT en base a sus objetivos y a las campañas en las que se han visto envueltas. Por ejemplo, APT28[4] es uno de los actores con más actividad en el ciberespacio. Es conocido como Tsar Team y sus objetivos son los países caucásicos, sobre todo Georgia y los países del este de Europa, teniendo también como objetivo países OTAN y otras organizaciones europeas relacionadas con la Defensa y la Seguridad. Estos indicios hacen sospechar que APT28 podría estar relacionada con Rusia. El software malicioso que utilizan tiene anotaciones en ruso y su actividad está centrada entre las 8 de la mañana y las 6 de la tarde, horario de trabajo en la mayoría de las ciudades de Rusia. Por todo esto, APT28 se podría atribuir, siempre supuestamente, a que tiene un fuerte apoyo económico del Gobierno ruso detrás.

[3] VILLALON HUERTA, A. *Amenazas Persistentes Avanzadas*, Nau Llibres, 2016.

[4] FIREYE, “Advanced Persistent Threats List”. Disponible en: https://www.fireeye.com/current-threats/apt-groups.html

Las APT realizan acciones de ciberguerra y ciberespionaje de una forma encubierta y sin una atribución certera a un determinado país. Es posible que el propio país quisiera influir en esa atribución a su propio país con el fin de provocar un efecto disuasorio en los demás. Esto que hasta ahora se realiza de manera sibilina, puede estar cambiando y podría escalar. Un ejemplo de esto, fueron las acciones realizadas por el grupo *The Shadow Brokers*[5]y pueden ser analizadas desde una perspectiva disuasoria.

En mayo de 2017, el mundo vivió uno de sus primeros ciberataques a nivel mundial conocido como *WannaCry*. En este ataque, llamado *ransomware*, un archivo malicioso cifra el contenido del disco y se extiende por la red realizando la misma acción en otros equipos. Además, pide al usuario una cantidad monetaria en criptomonedas si quiere descifrar sus archivos. *WannaCry* fue uno de los primeros ataques de *ransomware* realizados a nivel mundial, ataque que hoy en día es una de las mayores amenazas en el ciberespacio. *WannaCry* se aprovechó de una vulnerabilidad *Zero Day*, las cuales son vulnerabilidades que aún no son conocidas y que, en el caso de que se lanzara un ataque aprovechando dicha vulnerabilidad, no existiría medida de mitigación.

WannaCry hizo salir a la luz a un grupo de cibercriminales conocido como *The Shadow Brokers*, los cuales afirmaron haber hackeado a la *National Security Agency* (NSA) norteamericana y haber robado software malicioso, no más de diez piezas, que explotaban vulnerabilidades *Zero Day* y obtenían beneficio económico con su venta. Además, enunciaron que uno de los que habían vendido fue utilizado en el ataque de *WannaCry*. *The Shadow Brokers* declaró que solo pudo hacerse con el 10 % del software malicioso que tenía la NSA. Este hecho es una muestra manifiesta de poder cibernético de un país, pudiendo provocar una tremenda disuasión en los actores que están interesados en Estados Unidos. Si solo una pieza de software malicioso provocó un caos a nivel mundial, el poder potencial en el ciberespacio de la NSA podría ser muy grande. Se podría sospechar que la propia NSA podría estar detrás de *The Shadow Brokers* realizando una acción disuasoria de forma discreta.

[5] SEUNG H., KWANWOO K., SEUGWON S., "Poster: Knwoledge Seeking on the Shadow Brokers". Disponible en: http://nss.kaist.ac.kr/papers/ccs2018posterna.pdf

Comparativa con la disuasión provocada por submarinos en la II Guerra Mundial

La Primera Guerra Mundial fue uno de los primeros escenarios en los que los submarinos participaron de forma activa, aunque su uso fue principalmente defensivo. Una vez terminada la Primera Guerra Mundial, la firma del Tratado de Versalles en 1919 impedía a Alemania la construcción de buques de guerra de gran tonelaje y, por supuesto, la construcción de cualquier sumergible. Alemania debía construir, además, una flota homogénea, es decir, el mismo número de buques de cada clase. Este hecho que parece irrelevante tuvo unas consecuencias muy significativas en la Segunda Guerra Mundial.

La primera de ellas a favor de la ingeniería, ya que se comenzaron a construir buque con mucho ingenio. Un ejemplo de ello es lo que se llamó «acorazados de bolsillo» donde el más conocido de ellos es el *Graf Spee* por su participación en la batalla del Río de la Plata contra buques ingleses. El *Graf Spee* estaba catalogado como crucero pesado, pero apenas superaba las 15 000 toneladas, casi 10 000 toneladas menos que sus homólogos de otras naciones, cosa que lo hacia muy versátil y dinámico a la hora de entrar en combate. Una curiosidad de su ligereza fue la utilización de soldadura eléctrica en lugar del remache y la utilización de aleaciones ligeras de acero.

Otra consecuencia fue que Alemania comenzó a construir de forma clandestina submarinos, ya que era conocedora de que los submarinos podrían representar un papel importantísimo en caso de que una guerra tuviera lugar. Sin embargo, comenzó tarde a realizar su construcción. Según algunos historiadores, si Alemania se hubiese dedicado a construir submarinos y acorazados de bolsillo, el curso de la guerra habría sido bien distinto.

A lo largo de la Segunda Guerra Mundial, la flota alemana decidió utilizar sus submarinos[6] para atacar y desarrollar una estrategia muy común en las batallas navales clásicas que no es otra que el bloqueo de los recursos para los Aliados hundiendo los buques mercantes que les abastecían. Se dice que algunos submarinos alemanes hundieron 100 buques mercantes en un mes; hecho que, en algunos momentos de la guerra, asfixió a los Aliados. Las tácticas de los submarinos cambiaron de defensivas a ofensivas, realizando sus ataques de forma coordinada. Las conocidas como «manadas

[6] MATA, S. *U-BOOTE El arma submarina alemana durante la Segunda Guerra Mundial*, La esfera de los libros, 2016.

de lobos» atacaban convoyes de buques mercantes con una extraordinaria coordinación, pero que sin embargo el comandante de cada submarino solía realizar acciones ofensivas por su cuenta dentro de esa manada. De hecho, a pesar de intentar usar los submarinos como un grupo de combate, el espíritu submarinista es el de realizar misiones específicas en solitario, ya que de esta manera se preserva su discreción.

Un avance de ingeniería, por un lado, revierte en una reacción; y, por el contrario, se observan varios avances tecnológicos entre el final de la Primera Guerra Mundial y el final de la Segunda. Uno de ellos fue la detección de un objeto sumergido a través de los rayos sonoros en inmersión, en su origen llamado *Anti-Submarine Detection Investigation Committee* (ASDIC) y posteriormente conocido como SONAR (*Sound Detection and Ranging*) por analogía con el término de RADAR (*RADio Detection And Ranging*). De esta manera, los submarinos se sintieron mucho más hostigados en la Segunda Guerra Mundial que a finales de la primera.

Un hecho que ha favoreció a ambos bandos fue la aparición de la técnica LOFAR (*Low Frequency Analysis and Recording*)[7]. Esta técnica, ampliamente más utilizada por los submarinos, consigue no solo detectar un buque, sino también clasificarlo en función de sus frecuencias características que lo hacen único, además de aumentar la distancia de detección gracias a la mejora de la relación señal/ruido.

Al terminar la Segunda Guerra Mundial, el auge de los submarinos es total, comenzando una carrera armamentística por parte de las dos grandes potencias en ese momento, EE. UU. y Rusia. Asimismo, Francia y Reino Unido comenzaron la fabricación de estos buques considerados como un arma estratégica y como una medida de contener a los posibles enemigos.

En la actualidad, el uso del submarino, en su mayoría nuclear, con tecnología muy avanzada, con el posible uso torpedos supercavitantes lo convierte en una amenaza real y la tenencia de submarinos en su lista de buques hace a cualquier país ser tenido en cuenta a la hora de batirse o no con él por el domino del mar.

[7] ABRAHAM, D. “Underwater Acoustic Signal Processing: Modeling, Detection and Estimation (Modern Acoustics and Signal Processing)”, Springer, 2019.

Llegados a este punto: ¿Por qué comparar una APT con un submarino? Como primera aproximación, la técnica LOFAR, mencionada anteriormente, es lo más parecido a identificar las TTP de una APT. En ocasiones, un submarino en inmersión en cota profunda sin capacidad visual, gracias al LOFAR, es capaz de identificar el tipo de buque: si es de guerra o no, la clase e incluso el nombre según sus frecuencias. Lo mismo ocurre con las APT, donde la atribución se realiza principalmente en función de las TTP que utiliza y que pueden compararse con algunas ya conocidas por inteligencia.

Las características generales de una APT son su capacidad de permanecer anónima, su difícil detección (invisibilidad) y su resiliencia en el caso de ser detectadas. Estas características de las APT conjugan bastante bien con la premisa de «No se sabe ni cuántos son, ni dónde están». Análogamente, el submarino tiene tres principios fundamentales por este orden: seguridad, discreción y mantener la iniciativa.

La seguridad de la APT es aportada por su resiliencia, es decir, protegerse a sí misma y, en el caso de ser detectada, dejar alguna puerta trasera (*backdoor*) para volver en algún momento o simplemente realizar un exfiltrado de datos de emergencia y abandonar rápidamente la red. En el caso de los submarinos, cuando se percatan de que han sido detectados, lanzan un torpedo hacia la detección (normalmente, pueden haber recibido un *ping* sonar) y se sumergen a cota profunda, abriendo distancia, donde no puedan ser detectados.

En cuanto a la discreción, es más que evidente que la esencia del submarino es permanecer indetectado (salvo excepciones que serán comentadas más adelante). Tanto es así que la simple sospecha de la presencia de un submarino no controlado en un ejercicio o maniobras provoca que el ejercicio sea inmediatamente suspendido y que se realice una búsqueda exhaustiva para intentar identificar dicho objeto submarino. De igual forma, las APT tratan de permanecer indetectadas, incluso inician su actividad meses o años después de haber conseguido entrar en una red.

En cuanto al anonimato, existen puntos en común, pero con algunos matices. El anonimato es el conjunto de técnicas utilizadas por una APT para no ser detectadas. Mientras una APT puede esconder sus acciones a través de proxys, servicios de *cloud* (como Amazon Web Service o Google Cloud) o a través de la *dark web*; análogamente un submarino es capaz de esconderse si su cota está por debajo de la profundidad de capa. Explicado de manera sencilla, la velocidad de los rayos sonoros en el agua varía fundamentalmente en función de la profundidad y la temperatura del agua y, en menor medida, de la salinidad. La velocidad del sonido en el agua aumenta hasta cierta profundidad, donde empieza a disminuir drásticamente. Esta profundidad se conoce como profundidad de capa por debajo de la cual los submarinos son prácticamente indetectables, aunque tampoco tendrán capacidad de detección. Por lo tanto, existe un compromiso entre la capacidad de detección y la necesidad de ocultación, análogo a las APT.

Por último, si se habla de invisibilidad, las técnicas de las APT son múltiples. El término de invisibilidad está referido a que la APT no sea identificada a nivel local, mientras que anonimato esta más referido a nivel de comunicaciones con el exterior o la manera de acceder a la red para no ser identificado. La inyección en procesos legítimos, el uso de tareas programadas o la utilización de herramientas legítimas del sistema operativo (conocidas como LOLbins[8]) son algunas de las técnicas utilizadas por las APT. La posibilidad de ser invisible para un submarino está influida por multitud de factores, algunos de ellos no controlados (como la meteorología) y se reduce a muy pocas técnicas. Una de ellas es la posibilidad de posarse en el fondo o la reducción del ruido en inmersión.

¿En que ocasiones puede interesar que se rompa alguna de las características de los submarinos? Supongamos una situación donde se les está impidiendo a unas fragatas acceder a un puerto mediante el hostigamiento de otros buques, ya sean fragatas o patrulleros. La aparición de un submarino en escena modifica completamente las prioridades del otro bando. Si un submarino aliado de las fragatas llega a la zona, hace superficie y, a continuación, hace inmersión, aunque abandone la zona, sembrará la duda en el otro bando ante una amenaza tan grave como esa. ¿Podría ocurrir esto con las APT?

[8] LOLBins – Living-of-the-land binaries.

De la mitigación de la amenaza submarina a la mitigación de la amenaza cibernética

Las técnicas para la detección de amenazas en el ciberespacio están evolucionando[9] de una forma exponencial en los últimos años debido al aumento de complejidad en las acciones de los actores amenaza, sobre todo de las APT, haciendo que las tareas de un *Security Operations Center* (SOC) para detectarlos queden prácticamente obsoletas. La defensa pasiva, esperando a que una alerta pueda saltar en el *Security and Information Event Management* (SIEM)[10] ha dejado de ser efectiva a la hora de detectar una posible intrusión de actores amenaza avanzados. Un concepto relativamente nuevo, *Threat Hunting* (TH), empieza a ser relevante en el marco de la detección. Curiosamente, en el argot naval, la detección de un submarino se denomina «la caza de un submarino» y los submarinos también «cazan» barcos de superficie.

El TH está considerado el último paso del SOC y es un aliado indivisible del concepto de *Cyber Threat Intelligence* (CTI). TH es la búsqueda proactiva de amenazas dentro de una red y es muy útil a la hora de buscar su persistencia o permanencia sin tener que volver a infectar la red. Anticiparse a un ataque supone un auténtico reto para el personal que defiende una red y esto no podría ser posible sin la labor de CTI, cuyas principales funciones son la búsqueda en fuentes abiertas y el estudio de nuevas técnicas de intrusión que pudiesen ser utilizadas en la red propia.

Llegados a este punto, resulta interesante estudiar en qué punto se encuentra ahora mismo el equilibro entre detección e intrusión de una APT. El análisis puede ser enfocado desde un punto de vista militar. La guerra en el ciberespacio, como tal, no está regulada. Recientemente, la OTAN publicará un documento que será considerado un hito en la historia de la ciberguerra, el AJP 3.20 (*Allied Joint Publication*) donde aparecerán términos como operaciones militares en el ciberespacio, o cataloga al ciberespacio como uno de los dominios de guerra (*Warfare domains*) junto con tierra, aire y espacio y mar, siendo el ciberespacio un dominio casi infinito donde las fronteras no están definidas, no existe un control de armas, hay infinidad de actores y el marco legal es bastante

[9] STRAND, J. “Offensive Countermeasures: The Art of Active Defense”, *CreateSpace*, 2017.

[10] MURDOCH, D., “Blue Team Handbook: SOC, SIEM, and Threat Hunting: A Condensed Guide for the Security Operations Team and Threat Hunter”, 2019.

complejo. Varias preguntas surgen a raíz de esto en referencia al ciberespacio: ¿Existen derechos a la legítima defensa?, ¿qué es un combatiente legítimo?, ¿qué se puede catalogar como un intento hostil?, ¿cuándo se puede realizar el uso de la fuerza? o ¿qué es un ataque proporcional en el ciberespacio? Hasta ahora, los únicos documentos de referencia eran los manuales de Tallin, documentos con relativa legitimidad a nivel internacional, ya que no han sido reconocidos por muchos Estados.

La pregunta sería, comparando las APT con la evolución de los submarinos, ¿en qué momento histórico nos encontramos? La respuesta es compleja y con muchos matices, pero tratando de hacer una aproximación lo más certera posible, el momento en el que nos encontramos frente a las APT es muy parecido al final de la Segunda Guerra Mundial en el panorama de los submarinos. Mientras que con un SONAR se era capaz entonces de detectar un objeto en movimiento, pero si el submarino detenía su propulsión se hacía indetectable; hoy en día sistemas como el Detector de Anomalías Magnéticas (MAD, por sus siglas en inglés) o el despliegue de sonoboyas activas han resuelto esta carencia. Análogamente, en la actualidad, los Estados no son capaces de detectar de forma preventiva si una APT ha infectado sus redes o no. Podemos ver diariamente en la prensa cómo los Estados y las empresas realizan grandes esfuerzos en mitigar los ataques y evitar que el ataque se vuelva a producir.

Reflexionando, si el dominio de la ciberguerra se convierte en un dominio legítimo de combate, las APT (u otro nombre que se le quiera dar) podrían convertirse en organismos legítimos. *A priori* parece una idea descabellada, pero si lo analizamos, existen analogías en la actualidad que respaldan, de forma aproximada, esta teoría. El primer axioma es que en el mundo actual las Fuerzas Armadas se usan en gran medida de forma disuasoria. Si existiese la posibilidad de que hubiera una ciberguerra, nadie se atrevería a ciberatacar a un Estado que tuviese, por ejemplo, 15 APT reconocidas. Otra analogía, sería utilizar el conocimiento de vulnerabilidades *Zero Days* y la capacidad de ser explotadas como medida disuasoria.

Ciertamente, el revelar que se tiene conocimiento de vulnerabilidades *Zero Days* y software malicioso capaz de explotar dicha vulnerabilidad en su «ciberarsenal», podría hacer a algún Estado pensarse si utilizar alguna de sus APT con la impunidad que se utilizan hoy en día, por miedo a cualquier represalia por parte del Estado que cuenta con ese conocimiento de vulnerabilidades *Zero Days* o que se sabe que tiene APT más potentes. Con esto no se quiere decir que no existan grupos que realicen operaciones de inteligencia en el ciberespacio, ya que hoy en día existen grupos reconocidos de inteligencia en cualquier ámbito. Organismos reconocidos internacionalmente como la CIA (Central Intelligence Agency) de Estados Unidos o el CNI (Centro Nacional de Inteligencia) español no genera ningún tipo de revuelo social salvo cuando se produce alguna exfiltración de información. A la hora de realizar las acciones en el ciberespacio, se deberá velar, más si cabe, por mantener las características básicas de las APT, análogas a las del submarino: anonimato (mantener la iniciativa), invisibilidad (discreción) y resiliencia (seguridad).

Conclusión

Al igual que el uso de submarinos se convirtió desde la Segunda Guerra Mundial en un medio de disuasión por parte de los Estados; en la guerra en el ciberespacio, primero asimétrica *per se* e incluida de manera inherente en el campo de la guerra híbrida se utilizará la capacidad de potencial de realizar acciones ofensivas en el ciberespacio y se insinuará de manera más intensa la tenencia de grupos tipo APT que harán a los Estados replantearse su estrategia de operaciones, especialmente en el ciberespacio. Por tanto, llegará un momento que los Estados utilizarán la presunción de poder realizar ciertas acciones ofensivas en el ciberespacio o la tenencia de grupos APT o el conocimiento de vulnerabilidades *Zero Days* como medio de disuasión, siendo necesario ser tenido en cuenta de manera irremediable en el marco de la guerra híbrida de los próximos años.

La tecnología avanza de una manera vertiginosa y las técnicas de ataque de la presente década van a diferir completamente de las técnicas utilizadas hoy en día. El TH y la CTI deberán ser capaces de avanzar a la misma velocidad, aunque siempre irán un paso por detrás de los atacantes. Legitimar los grupos que realizan acciones en el ciberespacio —que pueden llamarse APT o no— podría abrir un panorama en el campo de la ciberguerra cuyas consecuencias son, de momento, desconocidas. El hecho de plantear esa posibilidad solo demuestra que existe y que, si llega a ocurrir, es un elemento más de un Estado a la hora de hacer las capacidades potenciales de sus Fuerzas Armadas en cualquier campo de batalla, incluido el ciberespacio.

*Gabriel Sánchez-Román Urrutia**
Teniente de navío de la Armada
Analista de Ciberseguridad del MCCD