ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

03/2018 8 de enero de 2018

*Manuel R. Torres Soriano**

El dilema de interpretación en el ciberespacio

El dilema de interpretación en el ciberespacio

Resumen:

Una de las principales fuentes que alimentan la conflictividad armada es el llamado dilema de interpretación, el cual ocurre cuando un Estado debe interpretar las intenciones subyacentes de las acciones puestas en marcha por competidores, rivales o enemigos. Este fenómeno se alimenta de la dualidad y el carácter ambiguo de las estrategias de seguridad y defensa, pero también de la falta de información a la hora de analizar sus motivaciones. El dilema de interpretación se ha visto potenciado como consecuencia de la eclosión del ciberespacio, y la proyección de las relaciones de poder en esta nueva dimensión. Este documento tiene como objetivo analizar los problemas adicionales a los que se enfrenta un Estado cuando debe evaluar el comportamiento de otros actores en el ciberespacio, siendo los más importantes: la existencia de ensayos agresivos, los requerimientos operacionales del desarrollo de cibercapacidades y la existencia de sesgos cognitivos en el análisis de la información.

Palabras clave:

Ciberconflictos, ciberinteligencia, dilema de seguridad, internet, estudios estratégicos.

The interpretation dilemma in cyberspace

Abstract:

One of the main sources of armed conflict is the so-called interpretation dilemma, which occurs when a State must interpret the underlying intentions of actions undertaken by competitors, rivals or enemies. This phenomenon is fueled by the duality and ambiguity of security and defence strategies, but also by the lack of information when analysing their motivations. The dilemma of interpretation has been heightened as a consequence of the emergence of cyberspace, and the projection of power relations in this new dimension. This article aims to analyse the additional problems faced by a State when assessing the behaviour of other actors in cyberspace, the most important being: the existence of aggressive test, operational requirements for the development of cyber-capabilities and the existence of cognitive biases in the analysis of information.

Keywords:

Cyber-conflicts, cyber-intelligence, security dilemma, internet, strategic studies.

Una de las principales fuentes que alimentan la conflictividad armada es el llamado dilema de seguridad[1]. La teoría estratégica moderna hace hincapié en un matiz de este proceso al que denomina dilema de interpretación, el cual ocurre cuando un Estado debe interpretar las intenciones subyacentes de las acciones puestas en marcha por competidores, rivales o enemigos. El desarrollo y despliegue de capacidades militares o el incremento de la recolección de inteligencia, pueden ser concebidos por sus autores como medidas orientadas a incrementar su seguridad, pero también pueden ser percibidos por la otra parte como el preludio de una acción hostil. El dilema de interpretación se alimenta, por tanto, de la dualidad y el carácter ambiguo de muchas de las medidas que los Estados implementan en el ámbito de las políticas de seguridad y defensa, pero también de la falta de información a la hora de evaluar sus motivaciones.

El dilema de interpretación se ha visto potenciado como consecuencia de la eclosión del ciberespacio, y la proyección de las relaciones de poder en esta nueva dimensión[2]. El espectro de las agresiones en el ciberespacio abarca desde el robo de información, hasta los daños en infraestructuras y personas. Sin embargo, en su génesis, cualquiera de estos actos son indistinguibles desde un punto de vista técnico, y solo es posible especular sobre la intencionalidad última de quienes los llevan a cabo. Este documento tiene como objetivo analizar algunos de los principales problemas a los que se enfrentan los Estados cuando deben evaluar las acciones puestas en marcha por sus adversarios en el ciberespacio, siendo los más importantes: la existencia de ensayos agresivos, los requerimientos operacionales del desarrollo de cibercapacidades y la existencia de sesgos cognitivos en el análisis de la información.

Ensayos agresivos

El desarrollo de planes operativos en el ámbito de la defensa depende de un conocimiento profundo de las capacidades militares, doctrinas y procedimientos de movilización de otros ejércitos. Una de las fuentes de conocimiento más útiles es el estudio de su respuesta ante determinados eventos que interpretan como actos de agresión. Con el objetivo de aumentar la frecuencia de estos episodios, algunos países recurren a provocaciones militares limitadas para desencadenar una respuesta que les

[1] JORDÁN Javier. “Dilema de seguridad, disuasión y diplomacia coercitiva”, en JORDÁN, J. (Coord.), *Manual de Estudios Estratégicos y Seguridad Internacional*, Madrid, Plaza y Valdés, 2013, 179-204.
[2] BUCHANAN Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*, London, Hurst, 2017.

permita mejorar su comprensión de las fortalezas y debilidades del oponente. Esa es la lógica subyacente, por ejemplo, de los múltiples incidentes aéreos que durante la Guerra Fría tuvieron lugar entre Estados Unidos y la Unión Soviética. A través de breves incursiones en territorio enemigo se pretendía activar sus mecanismos de defensa antiaérea, lo que permitía conocer en detalle la efectividad de sus sistemas de radares, los protocolos de respuesta, la cadena de mando y control o el proceso de toma de decisiones por parte del liderazgo militar y político. A pesar de su utilidad desde el punto de vista de obtención de inteligencia, las provocaciones suponen un elemento desestabilizador que alimenta el recelo entre las partes. En un entorno activo de tensión, este tipo de prácticas pueden ser interpretadas erróneamente como el preludio de una agresión bélica a gran escala. El dilema de interpretación se basa en la subjetividad de sus protagonistas: mientras que el provocador piensa que es obvio el carácter inocuo de sus transgresiones, no sucede igual desde la perspectiva del agredido, el cual interpreta estos eventos condicionado por la ausencia de información, por su lectura parcial del contexto en el cual se produce y por una serie de precedentes y prejuicios que le llevan a otorgar una relevancia muy distinta.

Figura 1: Captura de pantalla de un equipo infectado por *Wannacry*
Fuente: http://www.malware-traffic-analysis.net/2017/05/15/index2.html

En el ciberespacio también existen las acciones agresivas de testeo que, debido a una serie de incentivos adicionales, tienen lugar con una mayor frecuencia e intensidad. Por un lado, el ciberespacio elimina las limitaciones geográficas, lo que explica que las víctimas de estas intrusiones no se limiten a los actores con los cuales se comparte frontera o se encuentran dentro del alcance del despliegue militar de un país. Cualquier estado tienen la capacidad potencial de proyectar sus operaciones de testeo a la totalidad de los países del planeta, lo que sitúa dentro del ámbito de interés estratégico a países que anteriormente recibían una atención marginal debido a su lejanía física o a las limitaciones logísticas.

Por otro lado, en el ciberespacio se produce una multiplicación de objetivos que pueden ser objeto de una evaluación agresiva. Los mecanismos de respuesta no solo se estudian incidiendo sobre objetivos militares o gubernamentales, sino también sobre una amplia variedad de actores del ámbito social, económico y cultural cuya disrupción tiene un enorme impacto. La naturaleza privada de la mayor parte de las infraestructuras y redes que operan en el ciberespacio multiplica la probabilidad de que se produzcan este tipo de provocaciones ya que, a diferencia de lo que sucede con las agresiones externas contra el ámbito institucional, la respuesta política no suele ser tan severa con este otro tipo de víctimas[3]. Tras cada agresión es inevitable que surjan controversias en torno a cuál es el nivel de responsabilidad de la empresa atacada por no haber protegido suficientemente sus sistemas, o por prácticas negligentes que han incrementado la incidencia de estos ataques. Este es el caso, por ejemplo, de lo sucedido en mayo de 2017 tras la expansión a escala mundial del *ransomware* conocido como *WannaCry* el cual, haciendo uso de una vulnerabilidad presente en las versiones más antiguas del sistema operativo *Windows*, consiguió paralizar la actividad de grandes empresas y organismos públicos en 150 países. Tras el shock inicial, y una vez recobrada la normalidad, se produjo un cruce de acusaciones en torno a si otros actores distintos a los perpetradores del ataque tenían que asumir parte de la culpa[4]: ¿debían rendir cuentas las grandes empresas que facilitaron la propagación por no haber adoptado en

[3] NYE Joseph S. "Deterrence and Dissuasion in Cyberspace", *International Security*, vol. 41, nº 3 (Winter 2016/17), 44–71.

[4] FOX-BREWSTER Thomas. "Microsoft Just Took A Swipe At NSA Over The WannaCry Ransomware Nightmare", *Forbes* (14/5/2017), disponible en: https://www.forbes.com/sites/thomasbrewster/2017/05/14/microsoft-just-took-a-swipe-at-nsa-over-wannacry-ransomware-nightmare/#2b41c9c53585 Fecha de la consulta 04.12.2017.

sus equipos las versiones más recientes (y seguras) de *Windows*?, ¿era la propia empresa *Microsoft* la responsable por no haber detectado y parcheado con anterioridad este fallo de seguridad?, ¿o era la Agencia de Seguridad Nacional (NSA) de Estados Unidos la responsable por haber perdido el control sobre un vector de ataque que ahora estaba siendo empleado en su contra? En definitiva, la existencia de una responsabilidad diluida puede servir de argumento absolutorio para aquellos Estados que no desean (o no les resulta posible) articular una represalia contra el agresor.

En ocasiones, efectuar una atribución sólida de responsabilidad requiere aportar datos que provienen de fuentes de inteligencia de carácter clandestino. Hacer público sus resultados termina «quemando» mecanismos de obtención cuya efectividad dependen de que los objetivos desconozcan que su información o actividades han sido penetradas por un actor externo. Es entendible que los Estados se muestren reacios a sacrificar estos recursos escasos y en ocasiones insustituibles, algunos de los cuales solo generan fruto después de años de un trabajo intenso orientado a detectar y explotar las vulnerabilidades que permitan acceder al núcleo de decisión de un Estado. Puede comprenderse que solo bajo condiciones excepcionales el Estado esté dispuesto a degradar sus capacidades de obtención para construir una acusación contundente, la cual le permitiría movilizar a la opinión pública y la comunidad internacional a favor de una represalia de cierta entidad. Resulta menos probable que asuma este coste por la defensa de intereses privados, si el Estado no desea adoptar como propia esa causa, lo que explica que buena parte de estas provocaciones queden impunes. En el caso de *WannaCry* podemos encontrar también un ejemplo de esta resistencia del Estado a comprometer sus recursos de inteligencia. Tanto Estados Unidos como Reino Unido filtraron a la prensa[5] de manera «oficiosa» que su evaluación apuntaba a Corea del Norte como el causante de este ataque. Sin embargo, en dicha acusación no se aportaba ningún tipo de evidencia empírica, sino simplemente una vaga mención a que «las técnicas, procedimientos y objetivos» de este ataque eran similares a otros efectuados en el pasado por los hackers del régimen de Kim Jong Un.

[5] NAKASHIMA Ellen.“The NSA has linked the WannaCry computer worm to North Korea”, *The Washington Post* (14.06.2017), disponible en: https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?tid=ss_tw&utm_term=.b8037b204120 Fecha de la consulta 04.12.2017.

Por último, el ciberespacio permite reducir el coste político de este tipo de acciones agresivas a través de la ocultación o difuminación de la autoría. A diferencia de lo que sucede en el ámbito militar convencional, donde no es posible ocultar la procedencia de las aeronaves, embarcaciones o sistemas de armas que se emplean en estas provocaciones, en el ciberespacio existe un amplio margen técnico para ocultar la autoría estatal, creando para ellos actores interpuestos, recurriendo a *proxies*[6], o atribuyendo falsamente la autoría a otros Estados u organizaciones. De igual modo, el riesgo operativo que se asume en el ciberespacio, es muy inferior al que se produce en el ámbito físico. Que una ciberoperación quede comprometida puede producir una pérdida temporal del acceso a un objetivo o la inutilización de algunos procedimientos debido a la adopción de contramedidas. Sin embargo, los impulsores de estas acciones no tendrán que asumir ni el coste humano y material de la pérdida de operativos y armamento, ni la crisis política y diplomática que supone la existencia de fallecidos, prisioneros o sistemas de armas que han caído en manos del enemigo. En este sentido, los fracasos en el ciberespacio son meras contingencias que difícilmente afectan a la orientación estratégica de un país.

Requisitos operacionales

El desarrollo de cibercapacidades implica la necesidad de sostener en el tiempo una serie de actividades que pueden ser interpretadas como los actos preparatorios de una agresión. Tanto la capacidad de proyectar un ataque, como la de obtener inteligencia, requieren de un trabajo previo de reconocimiento, mapeo y penetración de las redes y sistemas que serán objeto de explotación. Si bien el interés operacional de algunos objetivos resulta obvio (lo que explica que se trabaje sobre ellos de manera prolongada y persistente), no sucede igual con otros cuya utilidad futura resulta difícil de prever. La necesidad de contar con un amplio catálogo de opciones para implementar un ciberataque y cubrir necesidades futuras de inteligencia, lleva a algunos Estados a adoptar un enfoque indiscriminado a la hora de seleccionar los potenciales objetivos a penetrar. Se trata de un planteamiento operativo que desborda los recursos materiales y humanos de cualquier actor, de ahí que también se recurra a herramientas que realizan

[6] TORRES Manuel R. "Guerras por delegación en el ciberespacio", *Revista del IEEE*, nº 9 (junio 2017), 15-36, disponible en: http://revista.ieee.es/index.php/ieee/article/view/309/473 Fecha de la consulta 04.12.2017.

de manera autónoma estas labores de mapeo e infiltración. En este sentido, la concentración de ciberataques sobre un mismo objetivo en un corto espacio de tiempo, no supone necesariamente el indicador de un mayor interés. En ocasiones, la causa se haya en la existencia de una brecha de seguridad que ha sido detectada y está siendo explotada de manera intensiva, sin necesidad de que se produzca una interacción humana.

Esta labor permanente de infiltración incide directamente sobre el dilema de interpretación. Los Estados se ven sometidos a la necesidad permanente de evaluar en profundidad la relevancia de los incidentes que padecen a diario. El análisis técnico no sustituye a la necesidad de interpretación, ya que las acciones enfocadas a la obtención de ciberinteligencia, son indistinguibles de los actos preparatorios de un ciberataque destinado a causar un daño físico. En este sentido, lo que inicialmente ha podido ser concebido como una operación de ciberinteligencia destinada a obtener acceso a las redes y sistemas de otro país, puede mutar en el tiempo, y convertirse en una operación «kinética». Es el caso, por ejemplo, de los ciberataques contra las centrifugadoras nucleares de Irán en 2010. Aunque la atención pública se dirigió hacia el virus informático conocido como Stuxnet, este vector de ataque forma parte de una campaña más amplia de recolección de información conocida como *Olympic Games*, que tuvo su inicio varios años antes de que empezasen a producirse el sabotaje del programa nuclear iraní[7]. De ahí que resulte muy difícil dilucidar la motivación del atacante, cuando en ocasiones, ni siquiera está definida de antemano, sino que esta va evolucionando según el contexto político y las nuevas ventanas de oportunidad operacionales que se van abriendo a medida que la infiltración va resultando exitosa.

Sesgos cognitivos

El dilema de interpretación se ve sometido a los mismos sesgos cognitivos que dificultan en términos generales el trabajo del analista de inteligencia[8]. Sin embargo, el ciberespacio como objeto de estudio tiene una serie de particularidades que aumentan la probabilidad de cometer errores en la interpretación de la realidad.

[7] ZETTER Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, London, Crown Publishers, 2014.
[8] HEUER Richards J. *Psychology of Intelligence Analysis*, New York, Novinka Books, 2006.

La visión mayoritaria entre analistas y decisores políticos es que la balanza ataque-defensa en el ciberespacio está claramente inclinada a favor de la primera[9]. Según esto, llevar la iniciativa a través de una postura ofensiva es la mejor estrategia para obtener seguridad. Este planteamiento, no solo incrementa la desconfianza entre adversarios, sino que también introduce un poderoso sesgo en el proceso de evaluación e interpretación de los ciberincidentes, empujando de menara instintiva hacia las hipótesis más alarmistas.

La inclinación intelectual hacia el peor de los escenarios posibles, no solo se produce a la hora de interpretar la intencionalidad, sino que se ve reforzada en los diferentes niveles de análisis de las ciberamenanaza. Así, por ejemplo, en el nivel táctico, las operaciones de ciberinteligencia tienen una naturaleza eminentemente engañosa[10]. El ocultamiento de la verdad no solo es un requisito operativo para obtener el acceso y control de los sistemas y la información del objetivo, sino también una condición que debe mantenerse a lo largo del tiempo, para que el desarrollo de estas operaciones alcance sus objetivos. El proceso cognitivo de las personas no está condicionado únicamente por la disponibilidad de información, sino también por la valoración que estas efectúan sobre la verosimilitud y calidad de la misma. Si los decisores dudan de la información que tienen a su alcance, es inevitable que a esa desconfianza se extienda a su evaluación del mundo que les rodea. El estrés cognitivo puede llevar no solo a magnificar la relevancia de determinados ciberincidentes, sino a interpretar su ausencia, como un indicador de que estos se están produciendo, pero han pasado inadvertidos. Ese era el razonamiento, por ejemplo, de Richard Clarke, la primera persona que ejerció el puesto de coordinador de ciberseguridad de la Casa Blanca, cuando afirmaba: «Hay dos tipos de empresas estadounidenses, aquellas que han sido hackeadas, y aquellas que no saben que han sido hackeada»[11]. Esta afirmación no era sino una adaptación aún más pesimista de lo afirmado por el director del FBI, Robert Mueller, un año antes cuando dividía las empresas americanas entre las que habían sido hackeadas y las que aún no, aunque

[9] SLAYTON Rebecca. "Why Cyber Operations Do Not Always Favor the Offense", *Belfer Center Policy Brief*, February 2017, disponible en: https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense Fecha de la consulta 04.12.2017.

[10] LIN Herbert & ZEGART Amy. "Introduction to the special issue on strategic dimensions of offensive cyber operations", *Journal of Cybersecurity*, vol. 3, nº 1 (March 2017), 1–5, disponible en: https://academic.oup.com/cybersecurity/article/3/1/1/3060285 Fecha de la consulta 04.12.2017.

[11] HYLAND Duane. "Richard A. Clarke Talks Cybersecurity at AIAA AVIATION 2013", *AIAA* (2013), disponible en https://www.aiaa.org/SecondaryTwoColumn.aspx?id=19463 Fecha de la consulta 04.12.2017.

pensaba que finalmente todas ellas convergerían en una única categoría: «las empresas que han sido hackeadas y las que serán hackeadas de nuevo»[12].

La integración de las ciberarmas dentro de las operaciones militares convencionales contribuye a aumentar la «niebla de la guerra« que dificulta el proceso de toma de decisiones. Los diferentes desarrollos doctrinales sobre cómo debería producirse el aporte «ciber» tienden a coincidir a la hora de contemplarlo como un instrumento para anular o adulterar los sistemas de mando y control del enemigo, arrastrando a la parálisis o al aislamiento a las diferentes unidades militares, mientras estas son objeto de un ataque convencional. Un indicador temprano de que se está siendo sometido a un ciberataque preparatorio podría ser el fallo simultáneo de los diferentes sistemas de comunicación y control, o la existencia de un comportamiento anómalo o errático de los sistemas informáticos. Sin embargo, este tipo de contingencias también pueden producirse por causas aleatorias. Esta ambivalencia y la presión temporal suponen un nuevo motor para el dilema de interpretación, el cual puede ser aún más problemático cuando afecta a la disuasión nuclear[13]. La militarización del ciberespacio ha supuesto un elemento que incide profundamente en el equilibrio nuclear, en la medida en que se abre la posibilidad hipotética de que un Estado pierda la capacidad momentánea de comunicarse y transmitir órdenes sobre sus arsenales nucleares, o esté recibiendo una información adulterada sobre el despliegue y uso de medios nucleares por parte de un actor hostil. La combinación de recursos ciber y nucleares vuelve a situar como una opción la posibilidad de un primer ataque que destruya por completo a un enemigo al que se le priva del acceso a la información y el control sobre sus mecanismos de represalia.

Otro sesgo cognitivo es atribuir una unicidad inexistente. Cuando se analiza el comportamiento de las acciones puestas en marcha por un Estado se le atribuye de manera inconsciente los atributos propios de un actor unitario que se comporta en todos sus actos de manera coherente y coordinada. Sin embargo, en cualquier Estado, incluyendo aquellos en los que se practica un gobierno autocrático y personalista,

[12] MUELLER Robert S. “Remarks by Robert S. Mueller, III at RSA Cyber Security Conference San Francisco, CA”, *FBI* (1.03.2012), disponible en https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies Fecha de la consulta 04.12.2017.

[13] GARTZKE Erik & LINDSAY Jon R. “Thermonuclear cyberwar”, *Journal of Cybersecurity*, vol. 3, nº 1 (March 2017), 37–48, disponible en: https://academic.oup.com/cybersecurity/article/3/1/37/2996537 Fecha de la consulta 04.12.2017.

encontraremos que su actuación exterior es fruto de la tensión permanente entre múltiples agencias y grupos de poder que rivalizan entre sí por ganar protagonismo, recursos e imponer sus propios prioridades. Obviar este hecho, puede llevar al error de interpretar un conjunto de iniciativas desconectadas y a veces contradictorias, como si formasen parte de un mismo plan de acción diseñado por un único centro de decisión. El uso del ciberespacio como escenario para el conflicto acentúa la falta de unicidad en la acción exterior del Estado[14]. La segurización de esta dimensión se ha producido en ausencia de un desarrollo doctrinal que delimite de manera clara la atribución de responsabilidades y cometidos entre actores públicos y privados. La falta de concreción ha propiciado que diferentes organismos se sientan llamados a realizar las mismas misiones. Eso explica, por ejemplo, cómo compitiendo por la atención del presidente ruso, Vladimir Putin, las inteligencias militar (GRU) y civil (FSB) terminasen actuando de manera solapada y sin coordinación contra las redes del Partido Demócrata de Estados Unidos. O explica, por ejemplo, cómo en la acción exterior china conviven al menos dos visiones contradictorias sobre el robo de propiedad intelectual a través de Internet: la del Ejército chino (PLA), que la concibe como una herramienta para avanzar en el desarrollo industrial y militar del país y reducir la brecha de poder con sus competidores[15], y la del Ministerio de Exteriores, que la percibe como una acción que socava las relaciones diplomáticas con Occidente, y dificulta que el país puede desempeñar un papel de liderazgo en los foros y organismos internacionales.

La medición y catalogación, aunque necesaria, tampoco anula el dilema de interpretación. La incertidumbre es el entorno habitual donde los decisores políticos y militares deben tomar decisiones. Uno de los elementos que más inseguridad genera es la percepción de que un rival está inmerso en una carrera armamentística que pretende alterar a su favor el equilibrio de poder existente. Cuando hablamos de armamento «convencional», el esfuerzo presupuestario genera resultados (nuevas instalaciones militares, reclutamiento de personal, nuevos buques y aeronaves, etc.) que pueden ser percibidos de manera tangible. Cuando un adversario debe interpretar la magnitud de esta amenaza, puede recurrir a datos empíricos que, aunque imperfectos, contribuyen a

[14] LINDSAY Jon R. “Cyber Espionage”, en CORNISH P. (ed.), *The Oxford Handbook of Cyber Security*, Oxford, Oxford University Press, (en prensa), disponible en: https://docs.google.com/viewer?a=v&pid=sites&srcid=am9ucmxpbmRzYXkuY29tfHd3d3xneDo2NDI4MjU2YWI4ZDM4MmI4. Fecha de la consulta 04.12.2017.

[15] INKSTER Nigel “Cyber Espionage”, *Adelphi Series,* vol. 55, nº 456 (2016), 51- 82.

reducir la incertidumbre. Sin embargo, cuando debe interpretarse la existencia de carrera armamentística en el ciberespacio, existen muy pocos elementos sobre los cuales apoyar un enfoque cuantitativo[16]. Existe una escasa o nula transparencia sobre las partidas presupuestarias que se dedican al desarrollo de estos recursos. En el caso de poder acceder a esos datos, tampoco existe una correlación directa entre más gasto, y más capacidades, sino que su adquisición obedece a factores difícilmente mesurables como la calidad de su capital humano, su creatividad, o la cultura organizativa. Una muestra de la dificultad para medir y comparar a nivel agregado puede apreciarse en las palabras del general Paul Nakasone, jefe del Ciber Comando del Ejército de los Estados Unidos cuando afirmaba en un evento público sobre ciberseguridad: «He estado en diferentes unidades del ejército. Trato de pensar: ¿hay un francotirador que haya conocido, o un piloto, o un conductor de submarino, o cualquier otra persona en el ejército que sea 50 veces mejor que su compañero? Es difícil de imaginar. Pero les diré que algunos de los programadores que tenemos son 50 veces mejores que sus compañeros»[17].

Como resultado, la valoración sobre si se está produciendo un incremento amenazante de cibercapacidades por parte de un adversario, tiene un componente eminentemente subjetivo. En este sentido, la liberación de información sobre su naturaleza y alcance (aunque se produzca de manera no deseada) produce efectos paradójicos. Este es el caso, por ejemplo, de la publicación de documentos de NSA por parte del contratista Edward Snowden[18]. Esta fuga masiva no solo generó un enorme problema de imagen para el Gobierno estadounidense, sino que afectó muy negativamente a la efectividad de los servicios de inteligencia del país, que vieron cómo buena parte de sus procedimientos y fuentes quedaron comprometidos. Sin embargo, las filtraciones de Snowden también proyectaron una poderosa imagen sobre las extraordinarias capacidades de los Estados Unidos en el ámbito ciber, lo que en última instancia genera un efecto disuasorio ante posibles rivales y competidores.

---

[16] CRAIG Anthony & VALERIANO Brandon. “Conceptualising Cyber Arms Races”, en PISSANIDIS N., RÕIGAS H. and VEENENDAAL M. (Eds.) *8th International Conference on Cyber Conflict and Cyber Power,* Tallinn, NATO CCD COE Publications, 2016, 141-158.

[17] TUCKER Patrick. “A Fight Is Brewing between Congress and the Military over Cyber War”, *Defense One* (16.11.2017), disponible en http://www.defenseone.com/technology/2017/11/fight-brewing-between-congress-and-military-over-cyber-war/142616/ Fecha de la consulta 04.12.2017.

[18] EPSTEIN Edward Jay. *How America Lost Its Secrets: Edward Snowden, the Man and the Theft,* New York, Knopf, 2017.

Conclusiones

La interpretación del adversario requiere entender sus objetivos e intereses, pero también la forma en la que sus distintos recursos de poder se integran y actúan. Las ciberoperaciones de un mismo actor sobre diferentes países adoptan múltiples formas porque su enfoque y objetivos son distintos en cada caso. Cuando se aborda un incidente de ciberseguridad, es habitual que el análisis táctico-técnico (qué vectores y procedimientos se utilizan) monopolice la discusión, ya que la obtención de este tipo de datos resultan mucho más asequibles y «objetivables» que la indagación sobre las motivaciones de sus perpetradores. Sin embargo, este tipo de aproximaciones, aunque necesarias, son manifiestamente insuficiente para comprender el contexto estratégico y la lógica subyacente de este tipo de incidentes.

Este es el caso, por ejemplo, del sofisticado ciberataque sufrido por la emisora de televisión francesa *TV5 Monde* en abril de 2015, el cual consiguió paralizar sus emisiones durante casi dos días y según su director «casi destruye» la cadena, ya que el *software* empleado tenía como objetivo inutilizar todo equipamiento conectado a Internet[19]. Solo el azar, a través de la presencia accidental de un técnico que de manera fortuita desconectó el equipo desde el cual se estaba iniciando el ataque, evitó que los atacantes alcanzasen su propósito. A través del *defacement* de los perfiles de la cadena en redes sociales de Internet, el sabotaje fue supuestamente reivindicado por el llamado «Cybercaliphate», un grupo de *hacktivistas* vinculado con la organización terrorista Estado Islámico. Sin embargo, meses más tarde un grupo de investigadores de la empresa *FireEye*[20] llegaron a la conclusión de que el ciberataque había sido orquestado desde Rusia por un grupo de operadores vinculados al Gobierno del país. Este grupo había hecho uso de infraestructuras, procedimientos y técnicas similares a los empleados por ellos mismos en otros ciberataques del pasado contra objetivos públicos y privados en Estados Unidos y Europa, de ahí que en el ámbito de las empresas de ciberseguridad se les reconociese como APT28, Pawn Storm, Tsar Team, Fancy Bear o Sednit[21]. La judicatura francesa oficializó la hipótesis rusa en su investigación, al asumir

[19] CORERA Gordon. “How France's TV5 was almost destroyed by 'Russian hackers'”, *BBC News* (10.10.2016), disponible en: http://www.bbc.com/news/technology-37590375. Fecha de la consulta 04.12.2017.

[20] PAGANINI Pierluigi. “FireEye claims Russian APT28 hacked France’s TV5Monde Channel”, *Security Affairs* (10.06.2015), disponible en: http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html. Fecha de la consulta 04.12.2017.

[21] BRANGETTO Pascal & VEENENDAAL Matthijs A. “Influence Cyber Operations: The Use of

la supuesta reivindicación yihadista como una mera forma de enmascarar la verdadera autoría del ciberataque.

El análisis técnico evidenció la presencia de una «falsa bandera« y la pista rusa, sin embargo, no despejó las principales incógnitas en torno al significado de esta agresión. ¿Es una acción destinada a testear capacidades? ¿Es un acto de represalia por alguna decisión del Gobierno francés? ¿Busca aumentar la capacidad de disuasión de Rusia haciendo una demostración tácita de sus capacidades en el ciberespacio? ¿Su objetivo es generar miedo en la sociedad francesa para desviar su atención de otras cuestiones, o pretende reorientar su posicionamiento sobre determinadas políticas y alianzas internacionales?

Figura 2: *Defacement* en el perfil de Facebook de la cadena de televisión TV5 Monde.
Fuente: https://arstechnica.com/information-technology/2015/04/french-tv-network-blames-an-islamist-group-for-11-station-blackout/

El estudio del código informático tampoco resulta suficiente para responder a otras interrogantes de carácter táctico. No permite desvelar, por ejemplo, si tras la elección del objetivo y el método empleado existe un impulso en el nivel político, u obedece a una

Cyberattacks in Support of Influence Operations", en PISSANIDIS N., RÕIGAS H. and VEENENDAAL M. (Eds.) *8th International Conference on Cyber Conflict and Cyber Power*, Tallinn, NATO CCD COE Publications, 2016, 113-126.

iniciativa de sus ejecutores. Tampoco si la comprensión de la lógica interna del ataque requiere ponerlo en relación con otros incidentes previos, si es un hecho aislado, o simplemente es el punto de partida de una campaña de futuros ciberataques. De igual modo, no aporta muchas evidencias sobre si el momento elegido obedece a un cálculo de oportunidad política, o es una mera cuestión de cuándo era viable técnicamente ejecutar el sabotaje. Incluso la adopción de una apariencia yihadista requiere de interpretación: ¿se ha recurrido al «sospechoso habitual» para que el ocultamiento resulte creíble, o atribuyendo falsamente al terrorismo esas capacidades se pretende generar un determinado efecto en la opinión pública? Que a nivel técnico haya sido posible realizar una atribución hacia Rusia[22]: ¿es resultado de la falta de pericia de sus autores?, o por el contrario, ¿se perseguía ofrecer un rastro ambiguo para que, aun siendo plausible la negación por parte del Gobierno ruso, todo el mundo tuviese clara la verdadera autoría?

En definitiva, abordar estas y otras cuestiones que inciden directamente en el núcleo del dilema de interpretación requiere de ciberinteligencia. Pero esta, lejos de verse reducida al mero análisis forense del código, debe ser entendida en su sentido más amplio: como un proceso holístico destinado a reducir la incertidumbre. Un objetivo que requiere no solo la recolección y análisis de los datos que se generan en el ciberespacio, sino también de su integración en el contexto estratégico que rodea estas interacciones, en el cual sigue ocupando un lugar central el comportamiento humano y las relaciones de poder.

*Manuel R. Torres Soriano**
Profesor titular de Ciencia Política. Universidad Pablo de Olavide (Sevilla)
Miembro del Grupo de Estudios en Seguridad Internacional (GESI)

[22] BARTHOLOMEW Brian & GUERRERO-SAADE Juan Andres. "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks", *Virus Bulletin Conference* (October 2016), disponible en: https://cdn.securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf. Fecha de la consulta 04.12.2017.