Capacidades ofensivas, disuasión y ciberdefensa

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

Tema

Los países democráticos están adoptando medidas ofensivas para disuadir a los países y grupos que realizan ciberataques de hacerlo o, al menos, que se arriesguen a pagar un precio. La cuestión es saber si el remedio de la disuasión es peor que la enfermedad de la impunidad.

Resumen

Las operaciones militares en el ciberespacio son el último recurso de la seguridad nacional, al igual que ocurre en cada uno de los demás dominios de tierra, mar, aire y espacio donde operan las fuerzas armadas. Pero las fuerzas armadas no sólo deben adoptar acciones defensivas para disuadir a los posibles agresores, sino también ofensivas. A esta conclusión se ha llegado en los últimos meses cuando las medidas defensivas, civiles y militares no han bastado para contener el crecimiento de ciberataques y, además, éstos se han patrocinado o consentido por algunos actores estatales. En consecuencia, las estrategias de ciberseguridad nacional se han ido abriendo a la planificación de capacidades ciberofensivas (defensa activa) que permitan disuadir a los posibles agresores o, al menos, hacerles pagar un coste elevado. Este ARI resume el estado de la disuasión y las ventajas e inconvenientes que plantean las operaciones ofensivas en el dominio del ciberespacio.

Análisis

La protección del ciberespacio se ha volcado en medidas defensivas para proteger las infraestructuras críticas de los países o los despliegues de sus fuerzas en teatros de operaciones. De las primeras se han venido ocupando las Administraciones Públicas y el sector privado corresponsables de la ciberseguridad, mientras que de las segundas se han encargado los mandos y fuerzas de ciberdefensa. Hasta el pasado inmediato, las acciones defensivas han primado sobre las ofensivas (*offensive cyber capabilities*, OCC) por la dificultad de identificar a los atacantes (atribución), por la falta de regulación del derecho a la legítima ciberdefensa o por los riesgos que implica una devolución de ataques (*hacking-back*). No obstante, en los últimos años se está produciendo un cambio desde la lógica de la resiliencia hacia la lógica de la disuasión, es decir, desde la prioridad de resistir y reponerse cuanto antes de los ciberataques a la de tomar medidas de represalia contra las mismas para evitarlas.

La disuasión funciona sobre la base de intenciones y capacidades. Su existencia aumenta la incertidumbre del posible agresor, porque corre el riesgo de que sus ciberataques desencadenen acciones de represalia. Y, cuanto menos conozca sobre ellas, mayor será su incertidumbre, porque complicará su cálculo de riesgos. Por el contrario, no disponer de capacidades ofensivas de contraataque o no estar dispuesto

a usarlas genera un efecto contrario a la disuasión que incentiva los ciberataques ante la certidumbre de que no encontrarán respuesta. Esta lógica de la disuasión se ha ido abriendo paso a medida que la proliferación de ciberataques ha puesto a prueba la postura defensiva de los países y dado paso a la proliferación de declaraciones y capacidades ofensivas explícitas.

El cambio de lógica tiene un amplio respaldo en la sociedad civil, porque son las instituciones políticas, económicas y sociales las que más sufren los efectos de los ciberataques. Por ejemplo, el sector privado de los Estados Unidos solicitó a la Administración en 2018 que adoptara medidas para protegerlo de los ciberataques porque el coste de las medidas defensivas que asumían comenzaba a ser insoportable. Pidió que desarrollara una política de disuasión que redujera su exposición a los ataques, procedieran estos de las organizaciones criminales o de los servicios de inteligencia de algunos países. Se trataba de acabar con la impunidad reinante y asegurar que los responsables, directos o indirectos, pagarían un precio por los ciberataques. Algunos de esos ataques procedían de amenazas no estatales, como las organizaciones criminales que buscan el robo, rescates o la suplantación de la identidad con fines delictivos y lucrativos. Pero otros tenían detrás una clara intencionalidad estatal, como el ataque norcoreano a los estudios Sony en 2014, o forman parte del enfrentamiento geopolítico en curso entre países como Irán y Corea del Norte, que atacan las infraestructuras financieras de Estados Unidos en represalia por las decisiones de su Administración[1].

En el caso de los países europeos, menos acostumbrados a crear y utilizar el poder militar que las grandes potencias, el cambio de lógica ha obedecido a la multiplicación de ciberataques sobre países, instituciones, procesos electorales e intereses vitales para la seguridad nacional. La constatación del reto ha obligado a la Unión Europea y a algunos de sus Estados miembros a combinar su prioridad normativa de regular el ciberespacio y fomentar la protección de las infraestructuras digitales del mercado único para abrir la puerta a capacidades más ofensivas, como las incluidas en el inventario de medidas diplomáticas de respuesta de la UE y el desarrollo de una ciberdefensa europea.

Las iniciativas anteriores han desarrollado capacidades y estructuras de ciberdefensa más ofensivas, pero no han resuelto las reservas de fondo sobre su utilidad y funcionamiento. El debate en torno a la disuasión en el ciberespacio sigue planteado, pero la acumulación de capacidades e intenciones lo eleva a un nivel de complejidad superior. De entrada, su introducción entre los instrumentos de respuesta afecta a la lógica de la disuasión tradicional, centrada en las armas nucleares y, sobre todo, en las convencionales, por lo que los analistas estratégicos tendrán que analizar su impacto

[1] David E. Simon (2017), "Raising the Consequences of Hacking American Companies", Centre for Strategic and International Studies, octubre de 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171012_Simon_RaisingConsequencesOfHacking_Web.pdf?za8vAFjk85a40wpIFvvd_FzyTg9haqEY; Erika Borghard (2019), "Protecting Financial Institutions Against Cyber Threats: A National Security Issue", Carnegie Endowment for International Peace, https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324.

(cont.)

sobre otros modos de disuasión[2]. Las capacidades ofensivas por sí solas no garantizan la disuasión en el ciberespacio y necesitan que su posesión se acompañe de capacidades defensivas adecuadas y de un desarrollo doctrinal que asocie su empleo a blancos adecuados y a cambios de conducta concretas. Mientras, el número de los países que disponen (Estados Unidos, China, Rusia, Israel, Reino Unido, Irán o Corea del Norte) o desean disponer de capacidades ofensivas (Bélgica, Alemania, Francia, Finlandia o India, entre otras) va creciendo (más de 30 países en 2016, según fuentes estadounidenses) y algunos países, como Estados Unidos, el Reino Unido o Australia, las han empleado contra el Estado Islámico en Oriente Medio[3].

La disuasión en la ciberseguridad

Entre otros hitos importantes para el desarrollo de las capacidades ofensivas, se encuentra el reconocimiento por la OTAN del ciberespacio como un dominio para las operaciones militares en su Cumbre de Varsovia, en 2016. Entre los países occidentales, el liderazgo corresponde a los Estados Unidos. Según la información disponible en fuentes abiertas, la preocupación por las capacidades ofensivas se remonta a 2012, cuando tuvieron constancia de que la Federación Rusa sondeaba las infraestructuras críticas de Estados Unidos para descubrir sus puntos débiles e introducir *software* malicioso en ellas con el fin de poder activarlas algún día si escala la tensión entre ambos países. Desde entonces, las Administraciones han buscado la forma de disuadir al Kremlin de llevar a cabo actuaciones en el ciberespacio que pongan en peligro la seguridad nacional o la democracia en los Estados Unidos.

En coherencia con lo anterior, la nueva Estrategia de Ciberdefensa de los Estados Unidos responde a esta mayor agresividad que demanda la confrontación geopolítica con China y Rusia y en ella se pide al Departamento de Defensa que "compita, disuada y gane" en el dominio del ciberespacio[4]. Se pide a las fuerzas de ciberdefensa que se preparen para la guerra y construyan una fuerza más letal, que establezcan alianzas y partenariados y que compitan y disuadan activamente a sus rivales. La nueva Estrategia amplía el campo de la disuasión a la protección de las infraestructuras críticas, lo que se entiende que afecta a las acciones ofensivas, porque de las defensivas ya se encarga el Departamento de Seguridad Interior. La ampliación forma parte de un proceso de maduración de las capacidades del Departamento de Defensa desde la Estrategia de 2015, que cuenta ahora con un mando de ciberdefensa único, más de un centenar de equipos plenamente operativos y una experiencia de combate[5]. La madurez de las capacidades ofensivas ha permitido a la Administración estadounidense una mayor

[2] Ellen Nakashima y Miss Ryan (2016), "U.S. military has launched a new digital war against the Islamic State", *The Washington Post*, 15/VII/2016.

[3] Max Smeets y Herbert S. Lin (2018), "Offensive Cyber Capabilities: To What Ends", NATO CCD COE, 2018.

[4] Departamento de Defensa de los EEUU, "Cyber Strategy" (resumen), septiembre de 2018.

[5] Nina Kollars y Jacqueline Schneider (2018), "Defending forward: the 2018 Cyber Strategy is here", *War on the Rocks*, 20/IX/2018.

(cont.)

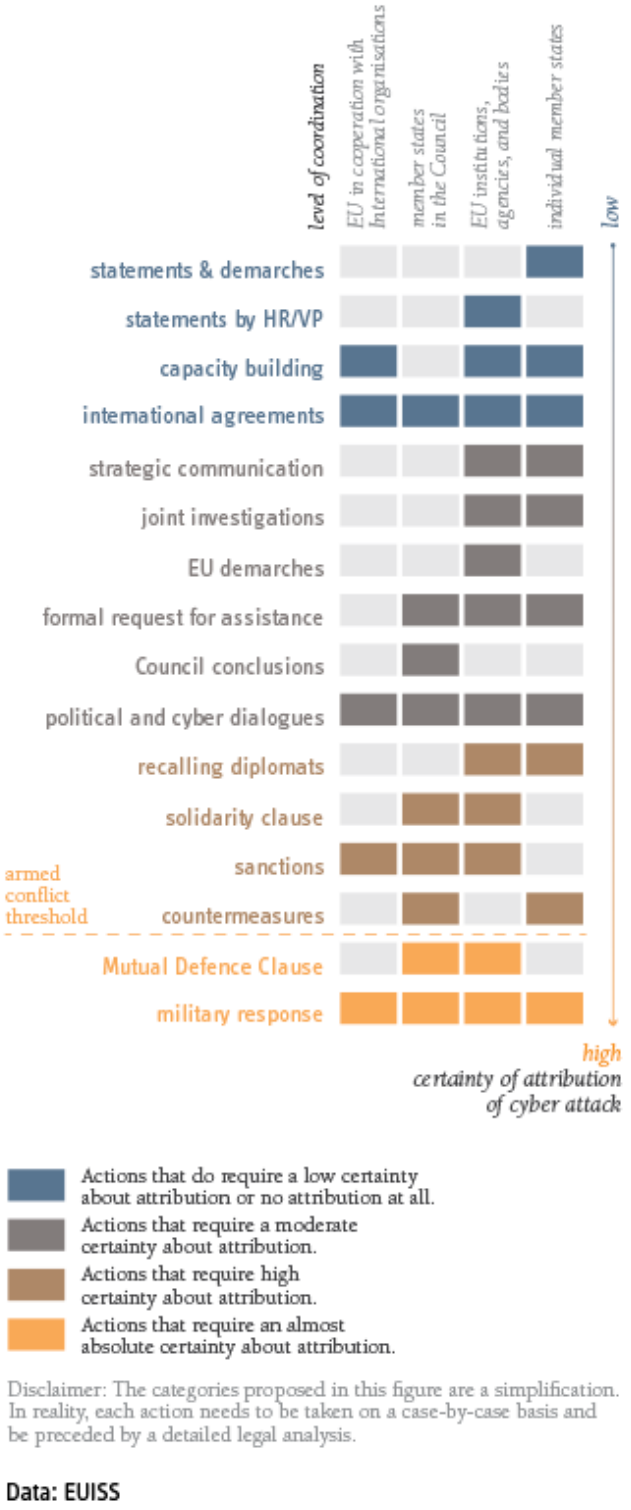
variedad y flexibilidad de instrumentos en su conflicto con Irán, recurriendo a operaciones ofensivas encubiertas para mantener controlada la escalada militar[6].

Ajena a la competición geopolítica entre China y Estados Unidos, la Unión Europea ha tenido que sopesar la necesidad de desarrollar capacidades de ciberdefensa bajo las evidencias y continuidad de las acciones ofensivas de la Federación Rusa. La sucesión de ciberataques contra Ucrania y los países bálticos o las intromisiones en procesos electorales han forzado a las instituciones europeas a recurrir a la disuasión. Hasta ahora, las medidas adoptadas por la UE se limitan a las menos agresivas del espectro[7] dentro de la lógica de su cultura estratégica cooperativa y se han limitado a reforzar las infraestructuras de la Política Exterior y de Seguridad Común y los despliegues de la Política Común de Seguridad y Defensa, así como a desarrollar un catálogo de medidas diplomáticas (que recoge la figura 1) para responder a todo el espectro de agresiones en función de la mayor o menor certeza en su atribución.

[6] Julian Barnes y Thomas Gibbons-Neff (2019), "U.S. Carried Out Cyberattacks on Iran", *The New York Times*, 22/VII/2019.

[7] Secretaría General del Consejo, "Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities", doc. 13007/17, de 9 de octubre.

Figura 1. Instrumentos de respuesta diplomática de la UE en función de la seguridad de la atribución y el nivel de coordinación entre sus Estados miembros



Fuente: Moret y Pawlak, European Union Institute for Security Studies (EUISS)[8].

[8] Erica Moret y Patryk Pawlak (2017),"EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", *Brief Issue* 24, European Union Institute for Security Studies (EUISS), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

En la figura se muestra el reparto posible de respuestas entre la UE, sus agencias y los Estados miembros, en los que las respuestas colectivas son más factibles cuanto más lejos se encuentran del umbral militar de respuesta. Entre las medidas adoptadas, algunas se han dirigido a contrarrestar la injerencia rusa en los procesos electorales y a combatir la desinformación. Hasta ahora, estas medidas *blandas* no han conseguido madurar suficientemente debido a la renuencia europea a legislar materias controvertidas y a la falta de eficacia de medidas como el Sistema de Alerta Rápida, que debería haber protegido las elecciones de mayo de 2019[9]. Sin embargo, a pesar de la voluntad europea de prevenir la conflictividad en el ciberespacio, la intencionalidad y proliferación de los ciberataques registrados han ido elevando la presión para que las capacidades e intenciones de la ciberdefensa europea progresen hacia ese umbral, empezando por el Parlamento Europeo, que desearía que la UE y sus Estados miembros contaran con capacidades ofensivas disuasorias en su inventario[10].

Francia, por su parte, se ha postulado como una potencia cibernética completa, con capacidad para combinar acciones defensivas y ofensivas, desde su Libro Blanco de la Defensa de 2008 hasta su Revisión Estratégica de la Ciberdefensa de 2018, aunque ha sido recientemente cuando ha elaborado –o revelado– detalles sobre sus elementos doctrinales ofensivos ("*Eléments publics de doctrine militaire de lutte informatique offensive*") y defensivos ("*Politique ministérielle de lutte informatique defensive*")[11].

El Reino Unido sigue la tradición anglosajona de ubicar sus capacidades ofensivas dentro del ámbito de la inteligencia (Government Communication Headquarters, GCHQ), con la colaboración –pero no en dependencia– de las Fuerzas Armadas en el National Offensive Cyber Program (NOCP). No dispone de una doctrina explícita que revele sus capacidades ofensivas, pero sí han trascendido sus operaciones contra el Estado Islámico. Su capacidad de realizar contraataques en el ciberespacio de forma unilateral es distinta de la capacidad de ciberdefensa activa (*Active Cyber Defence*, ACD) que desarrolla en el ámbito de la ciberseguridad para la protección de activos civiles. En este ámbito, la Estrategia Nacional de Ciberseguridad 2016-2021 limita la defensa "activa" a disuadir de los ciberataques que no conllevan riesgo de una escalada militar[12].

Algunos países europeos, como Alemania o España, también se han visto obligados, contra su cultura estratégica defensiva, a considerar la necesidad de contramedidas ofensivas para proteger su seguridad. En el primer caso, la Estrategia de Ciberseguridad de 2016 marcó el punto de inflexión desde una ciberseguridad basada en la protección

[9] Matt Apuzzo (2019), "Europe Built a System to Fight Russian Meddling. It's Struggling", *The New York Times*, 6/VII/2019.

[10] Parlamento Europeo, "Report on Cyber-Defence", doc. A8-0189/2018, de 25 de mayo, http://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.pdf.

[11] Ministerio de Defensa, "Comunicado sobre la doctrina militar ofensiva", 18/I/2019, https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-de-florence-parly/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.

[12] Tim Stevens y otros (2019), "UK Active Cyberdefence", The Policy Institute, King's Collegue, enero de 2019, https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf.

(cont.)

civil de las infraestructuras críticas a otra de ciberdefensa que incluía medidas ofensivas. Bajo esa nueva orientación, Alemania ha ido construyendo su Mando de Ciberdefensa y dotándolo de capacidades tecnológicas, personal y formación para desarrollar operaciones militares defensivas y ofensivas en el dominio del ciberespacio[13]. En el caso español, la Estrategia Nacional de Ciberseguridad de 2019 reconoce la necesidad de implantar medidas de ciberdefensa activa para ir más allá de las medidas de autoprotección que los ciudadanos, autónomos y empresas puedan tomar, y el Concepto de Ciberdefensa incluye medidas de defensa, explotación y ataque[14].

Los riesgos de la disuasión

El empleo de las capacidades ofensivas para respaldar la disuasión tiene abiertos varios frentes de debate. El primero surge de la tensión entre su legalidad y su eficacia. A diferencia de otros dominios, el uso de la guerra en el ciberespacio carece de una regulación internacional y parece poco probable que las grandes potencias se avengan a participar en una gobernanza internacional mientras les favorezca la falta de regulación. En su defecto, la eficacia es un parámetro más adecuado para medirla. Hasta ahora, se conocen pocos casos de empleo y no existe información en fuentes abiertas para evaluar cuáles eran los objetivos buscados y cuáles los conseguidos. Los datos conocidos entre 2000 y 2016 reflejan muy pocas operaciones ofensivas de gran calado y no hay evidencias empíricas que demuestren con rigor que esas operaciones eviten los ataques ni que los provoquen[15]. La dificultad para medir la eficacia desde fuera de los sistemas nacionales de ciberdefensa es mayor que en otros dominios y capacidades militares debido a su reducida trasparencia, sea deliberada para preservar la disuasión u obligada por el estadio preliminar de la conceptualización teórica. La intuición general parece coincidir en que es mejor contar con capacidades ofensivas que no contar con ellas, aunque no se puede medir cuánto mejoran la capacidad de disuasión[16].

A falta de trasparencia y medición de su eficacia, la decisión de contar o no con este tipo de capacidades ofensivas depende de un conjunto aleatorio de factores. Seguir la tendencia general es un factor importante que explicaría la multiplicación de países que se apuntan a la tendencia dominante, independientemente de su relevancia estratégica. De no seguirla, sus Gobiernos tendrían que explicar las razones de su renuencia en el debate político y, lo que es peor, arriesgarse a hacerlo en caso de que se vean más afectados por los ciberataques que otros usuarios más decididos. Otro factor procede de la socialización de las élites político-militares con esas capacidades ofensivas en el marco de la defensa o la seguridad colectiva. La formación, el adiestramiento y el desarrollo de capacidades colectivas en los marcos de la OTAN o la UE facilitará con el tiempo la maduración de los conceptos, doctrinas, estrategias y estructuras de

[13] Matthias Schultze y Sven Herpig (2018), "Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them", *Council on Foreign Relations* (blog), 3/XII(2018.

[14] Ministerio de Defensa, "Concepto de Ciberdefensa" (resumen ejecutivo), 18/IX/2018.

[15] Brandon Valeriano y Benjamin Jansen (2019), "The Myth of the Cyber Offense", *CATO Policy Analysis* 862, 15/I/2019.

[16] James A. Lewis (2015), "The Role of Offensive Cyber Operations in NATO's Collective Defence", *Tallin Paper* 8, 2015.

ciberdefensa de los distintos países, pero a corto plazo casi todas las iniciativas se encuentran en período de prueba.

Un obstáculo a esta vía de socialización, que ayuda a explicar la mencionada falta de trasparencia, es la necesidad de restringir el conocimiento de las intenciones y capacidades concretas de cada país. Los Estados son reacios a explicitar las capacidades ofensivas de las que disponen –incluso a sus aliados–, porque descubrir sus cartas les haría perder la ventaja comparativa de la que disponen. Descubrir sus procedimientos operativos, sus infraestructuras de ataque, sus fuentes de inteligencia o las ventajas y limitaciones de sus capacidades ofensivas proporcionaría una información demasiado valiosa a terceros. En consecuencia, las acciones ofensivas son fundamentalmente nacionales y es difícil que puedan llevarse a cabo ejercicios de adiestramiento u operaciones conjuntas de carácter ofensivo, porque todos los participantes tendrían acceso a las capacidades de los países más avanzados[17].

Otro obstáculo para la consolidación de la disuasión tiene que ver con la falta de regulación internacional o nacional. A falta de ella, la delegación de poder que se traslada a los mandos de ciberdefensa para anticiparse o responder a los ciberataques escapa al control parlamentario y pende de la discrecionalidad de los presidentes y de los gabinetes de seguridad nacional. Hasta la Guerra Fría, los Parlamentos tenían la prerrogativa de declarar las guerras, y después muchos han reclamado el control de los desplazamientos de tropas al exterior en las operaciones y misiones de posguerra fría. El desarrollo de las operaciones ofensivas encubiertas complica el control parlamentario y aumenta el riesgo de que a partir de ellas se produzca una escalada que desemboque en un conflicto armado no autorizado. La agresividad de Rusia y China podría justificar la delegación, pero una vez admitida será difícil remover las capacidades ofensivas de los inventarios militares y evitar que se utilicen en casos menos justificados. Por eso, el desarrollo de las capacidades ofensivas debe complementarse con un marco regulatorio y doctrinal que establezca las asunciones de empleo y el reparto de responsabilidades entre los distintos decisores. La regulación es, además, imprescindible para prevenir su empleo por actores privados que no tengan una evaluación –o interés– sobre las posibles consecuencias, deseadas o no, para terceros. Esta preocupación se refleja, por ejemplo, en la doctrina militar francesa de ciberdefensa (“*Eléments Publics”*), en la que se regulan los mecanismos de supervisión de todos los riesgos asociados a las operaciones ofensivas y defensivas, aunque su operación se encomiende al Mando de Ciberdefensa (Commandement de la cyberdéfense, COMCYBER).

La delegación debe realizarse con controles, porque se corre el riesgo de que las capacidades ofensivas se empleen de forma sesgada o automática. Por un lado, es posible que algunos presidentes con amplios poderes utilicen los nuevos instrumentos sin conocer sus especificidades de empleo. Este podría ser el caso de los presidentes de Estados Unidos, que han usado –y abusado de– sus poderes de guerra para que sus Fuerzas Armadas intervengan en conflictos no declarados. En este sentido, el Memorándum Presidencial del 13 de septiembre de 2015 flexibilizó las normas de empleo de las capacidades ofensivas vigentes ampliando las opciones de sus Fuerzas Armadas y del Consejo de Seguridad Nacional, muy proclives a utilizar la fuerza en sus

[17] Jack Waiting (2019), “Allies in the Multi-Domain Task Force”, *RUSI Defence Systems* 21(1), 5/IV/2019.

relaciones internacionales. Por otro, es necesario evitar que la falta de conocimiento y experiencia respecto a las acciones ofensivas aliente el mito de que pueden evitar los ciberataques o de que el ciberespacio favorece las acciones ofensivas, por lo que es importante que el desarrollo conceptual y doctrinal de la defensa activa no quede exclusivamente en manos de sus usuarios finales (en el caso británico, la supervisión corresponde al Comité de Inteligencia y Seguridad del Parlamento).

Conclusiones

Las capacidades ofensivas en el ciberespacio han llegado para quedarse. Las grandes potencias han abierto el camino para utilizarlas en su competencia geopolítica directa y los demás las están siguiendo para no descolgarse del nuevo modo de disuasión. Ni todas las expectativas que se crean están justificadas ni todos los reparos que se conocen están demostrados. Ante la dificultad de la evaluación, que llegará con el tiempo, los consejos de seguridad nacional y los mandos de ciberdefensa han creído que era mejor disponer de esas capacidades ofensivas que no tenerlas. Su disponibilidad debe completarse cuanto antes con un marco regulatorio que evite que las condiciones de empleo dependan exclusivamente de las autoridades militares o de seguridad. Su aplicación en el ámbito de la ciberdefensa conlleva riesgos poco conocidos, pero, si la maduración de las operaciones y medidas se acompaña de contención, sus resultados podrían aplicarse al ámbito de la ciberseguridad. Ya que no es posible devolver el genio de las capacidades ofensivas a la lámpara que lo contenía, habrá que meditar con prudencia los deseos que se le pidan.