ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

83/2022 27 de septiembre de 2022

*Christian Dieterich**

El aumento del uso del ciberespacio como vector de ataque en conflictos

El aumento del uso del ciberespacio como vector de ataque en conflictos

Resumen:

El ciberespacio se ha convertido en un lugar común, determinante en cualquier conflicto bélico. Georgia en 2008 y toda la literatura referente a la guerra híbrida parecen hacer honor a esta argumentación. Así pues, ¿estamos ante un cambio de paradigma en el que el ciberespacio será el dominio más determinante en los conflictos actuales y futuros?

Este artículo ofrece una visión general de los diferentes vectores de ataque en el ciberespacio, la situación global de los ataques patrocinados por el Estado en la última década y los retos a los que se enfrentan atacantes y defensores en el ciberespacio. Además, se examinará la cuestión de si el ciberespacio se ha convertido en el instrumento estatal más importante en los conflictos desde 2008.

Por último, la consideración de los aspectos legales y éticos de las operaciones ofensivas en el ciberespacio arroja una mirada sobre un factor del uso estatal del ciberespacio que ha tendido a ser subestimado hasta ahora.

Palabras clave:

Conflicto híbrido, geopolítica, actores estatales, operación ciberespacial ofensiva.

The increased use of cyberspace as a vector of attack in conflicts

Abstract:

Cyberspace has become a commonplace, a determining factor in any war. Georgia in 2008 and all the literature on hybrid warfare seem to live up to this argument. So, are we facing a paradigm shift in which cyberspace will be the most decisive domain in current and future conflicts?
This article provides an overview of the different attack vectors in cyberspace, the global state of state-sponsored attacks over the last decade and the challenges facing attackers and defenders in cyberspace. In addition, the question of whether cyberspace has become the most important state instrument in conflicts since 2008 will be examined.
Finally, consideration of the legal and ethical aspects of offensive operations in cyberspace sheds light on a factor in state use of cyberspace that has tended to be underestimated until now.

Keywords:

Hybrid conflict, geopolitics, state actors, offensive cyberspace operation.

Cómo citar este documento:

DIETERICH, Christian. *El aumento del uso del ciberespacio como vector de ataque en conflictos*. Documento de Opinión IEEE 83/2022.
https://www.ieee.es/contenido/noticias/2022/09/DIEEEO83_2022_CHRDIE_Ciberespacio.pdf
y/o enlace bie[3] (consultado día/mes/año)

Introducción

La imagen de la guerra que ciertamente sigue prevaleciendo en la mente de la mayoría de la gente es el concepto clásico en el sentido de la guerra clausewitziana: la lucha armada entre dos o más naciones con el objetivo de obligar al adversario a cumplir su propia voluntad. La imagen de ejército contra ejército, de gran violencia física y de escombros humeantes.

Aunque esto todavía se aplica en parte a los conflictos actuales, la guerra ha cambiado. Sigue adaptándose a las condiciones políticas, sociales y económicas cambiantes en cada caso concreto. Por otra parte, se está produciendo una desregulación cada vez mayor de la guerra, ya que cada vez más a menudo entran en ella actores que no se adhieren a las normas de guerra establecidas (Reglamento de La Haya, Convenciones de Ginebra, etc.) o utilizan diversas zonas sujetas a normas poco claras para llevar a cabo sus operaciones[1].

Esto se refiere no solo a los llamados «modos de lucha asimétricos» de los grupos terroristas, que implican cada vez más a la población civil en las operaciones de combate, en parte como cobertura y en parte como apoyo logístico, sino también a los Estados que hacen uso de la «guerra híbrida» para lograr sus objetivos[2,3].

El origen del concepto de guerra híbrida se remonta a los dos oficiales estadounidenses James N. Mattis y Frank Hoffman[4], que ampliaron el llamado modelo de «guerra en tres bloques»[5] del general Charles Krulak[6] añadiendo una cuarta dimensión, la psicológica y el espacio informativo.

En 2013, este modelo fue retomado por el general ruso Valery Gerasimov y perfeccionado bajo el nombre de «conflicto de nueva generación» (véase figura 1). También él asume que los límites entre la guerra y la paz son cada vez más borrosos y siguen pautas desconocidas. A medida que estas normas han cambiado, «el papel de

[1] MÜNKLER, H. *Die neuen Kriege*. Editado por Landeszentrale für politische Bildung Baden-Württemberg (Der Bürger im Staat), 54(4), 2004, pp. 179-184.
[2] Ibid.
[3] BILBAN, C. y GRININGER, H. (eds.). *Mythos "Gerasimov-Doktrin": Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung? Eine Analyse der Rezeptionen in Europa und China*. Schriftenreihe der Landesverteidigungsakademie, Wien, Republik Österreich, Bundesministerium für Landesverteidigung, 2019, Band 2.
[4] MATTIS, J. N. y HOFFMAN, F. «Future Warfare: The Rise of Hybrid Wars». *Proceedings-United States Naval Institute*. US Naval Institute, 2005, 132(11).
[5] Este modelo parte de la base de que los conflictos modernos son escenarios muy complejos en los que los combates tienen lugar en un bloque, la ayuda humanitaria en el siguiente, y las partes del conflicto tienen que volver a separarse en el siguiente, pero se refería principalmente a los combates en terreno urbano.
[6] KRULAK, C. C. «The Strategic Corporal: Leadership in the Three Block War», *Marines Magazine*. 1999, pp. 1-7.

los medios no militares en la consecución de objetivos políticos y estratégicos está aumentando y, en muchos casos, superando el poder de las armas en su eficacia»[7].

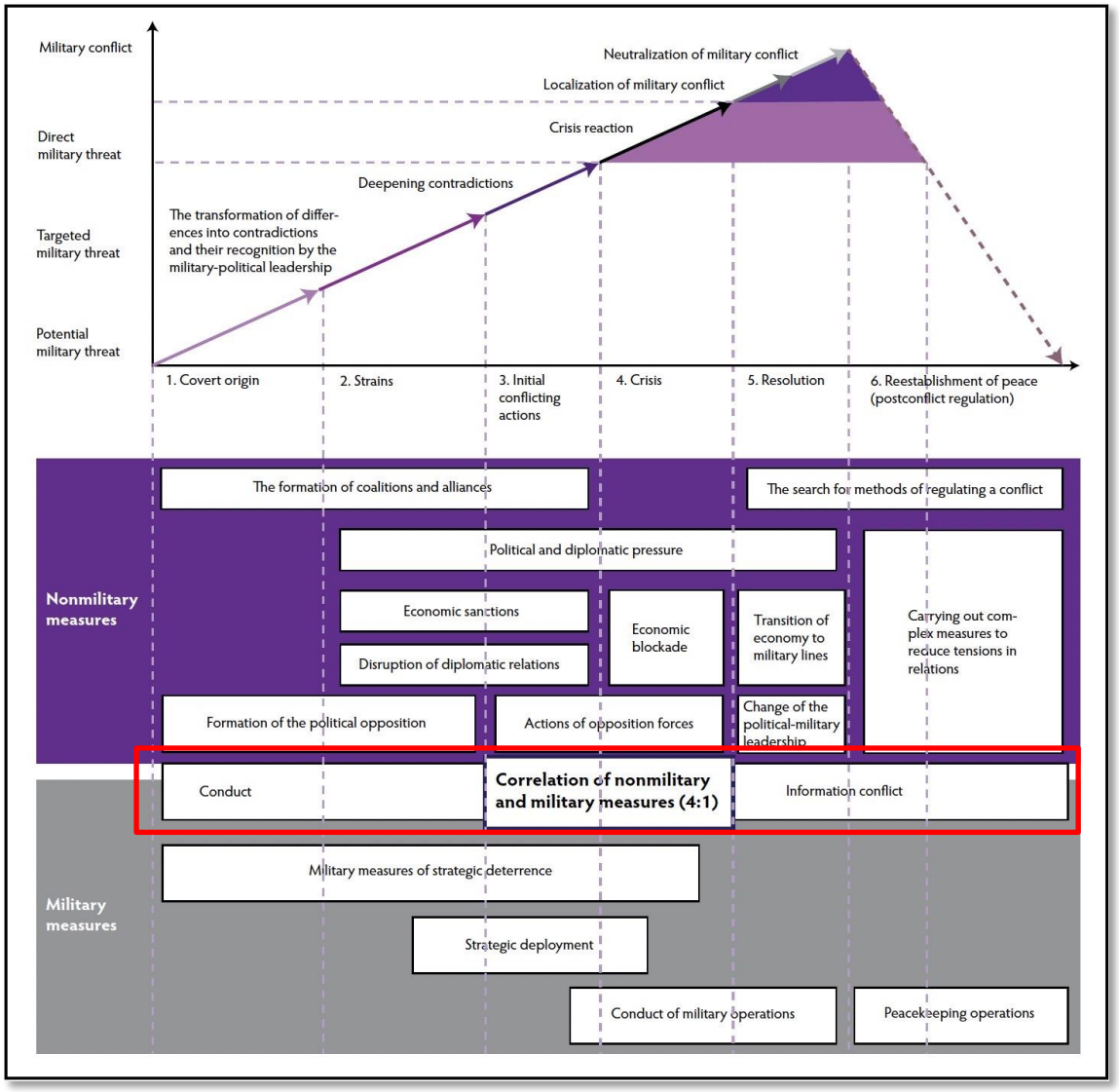

Figura 1. Gráfico del artículo de Gerasimov en el *Voenno-Promyšlennyj Kur'er*, 26 de febrero de 2013, traducido por Charles Bartles[8]

Uno de los dominios de la guerra híbrida es el ciberespacio, una sección de la zona de conflicto que está en gran medida «no regulada» para su uso militar, también llamada zona gris (véase figura 2). En este caso, no hay conflicto armado, pero el conflicto ya está en marcha. Los actores buscan allí ventajas «sin exponerse a los costes y riesgos

[7] COALSON, R. «Russian Military Doctrine article by General Valery Gerasimov». *facebook.com*. 2014. Disponible en: https://www.facebook.com/notes/10224211182773273/ (consulta 10/2/2022).
[8] BARTLES, C. K. «Getting Gerasimov Right», *Military Review,* 96(1). Department of the Army Headquarters, Fort Leavenworth, 2016, pp. 30-38.

de la guerra»[9]. Por tanto, puede afirmarse que, si la «guerra híbrida» es un método, la «zona gris» es un lugar[10].

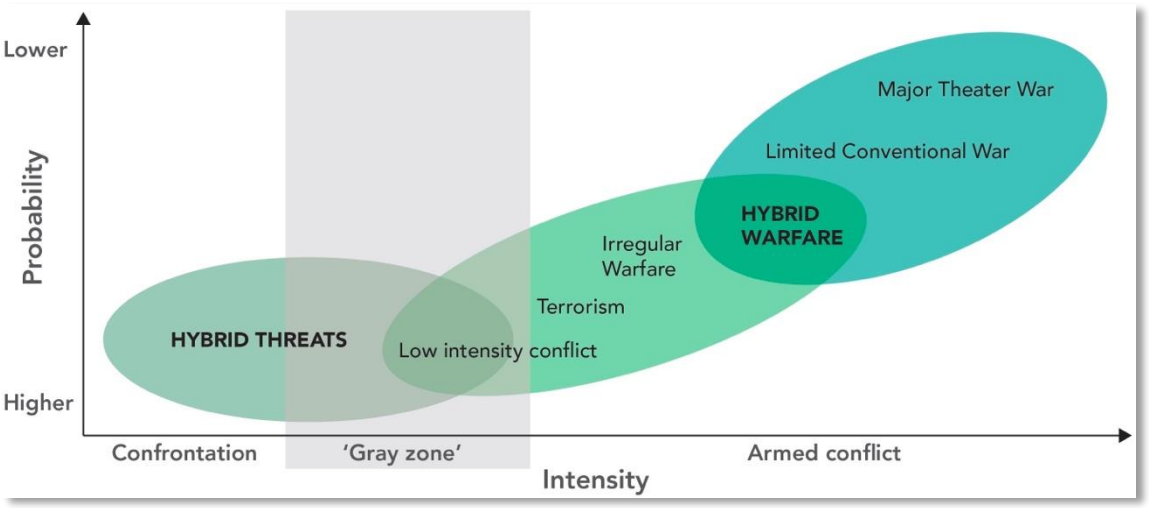

Figura 2. Amenazas híbridas y guerra híbrida en un continuo de conflictos[11]

Si se amplía un poco la mirada, se descubre que la ciberguerra es una «forma continua y omnipresente de geopolítica»[12]. La creciente importancia del ciberespacio es el resultado de la *informatización*[13] de nuestra sociedad, economía y ejército. Por ello, muchos Estados han empezado a incluir la ciberguerra en su «código geopolítico» desde la década de 2000. Desde entonces, el uso del ciberespacio con fines ofensivos ha tenido múltiples repercusiones en la geopolítica *física*[14] y la ha modificado posteriormente de forma permanente.

Con la aparición del ciberespacio, la geopolítica como interacción dinámica entre territorios (en particular, los Estados) se ha ampliado para incluir el componente de las redes globales. Si el uso de estas redes sigue creciendo al mismo ritmo, los Estados tendrán que replantearse su concepción tradicional de la geopolítica, en la que enemigos y aliados, amenazas y oportunidades solo podían ser otros Estados.

[9] ROBERTS, B. «Neue Herausforderungen erfordern neue Ideen: Elemente einer Theorie des Sieges in modernen strategischen Konflikten». *SIRIUS – Zeitschrift für Strategische Analysen*, 4(4). 2020, pp. 410-434 y p. 430. doi:10.1515/sirius-2020-4004.

[10] BACHMANN, S. D., DOWSE, A. y GUNNERIUSSON, H. «Competition Short of War–How Russia's Hybrid and Grey-Zone Warfare Are a Blueprint for China's Global Power Ambitions», *Australian Journal of Defence and Strategic Studies*, 1(1). 2019.

[11] MONAGHAN, S. «Countering Hybrid Warfare», *PRISM,* (2). 2022, pp. 82-99.

[12] FLINT, C. *Introduction to geopolitics*. 4ª ed. Abingdon, Oxon; Routledge, New York, 2022, p. 200.

[13] La informatización se entiende aquí como el proceso de generar y utilizar información para poder generar más información a partir de ella.

[14] Un ejemplo bien conocido es el ataque a las redes de los Estados bálticos por parte de Rusia tras la retirada de un monumento ruso.

Uso del ciberespacio como vector de ataque

Para comprender mejor el combate en el ciberespacio es necesario conocer las diferentes herramientas de que disponen los actores, así como su motivación para emplearlas.

En principio, los atacantes pueden utilizar diferentes «vectores de ataque»[15, 16] de forma individual o combinada, aprovechando las brechas de seguridad o las vulnerabilidades de los sistemas informáticos. Aunque estos ataques pueden ser realizados por cualquiera y también son muy utilizados por los delincuentes, los ataques de los agentes estatales, en particular, se caracterizan por un alto grado de profesionalidad y complejidad.

También se puede distinguir entre métodos ciberespaciales no intrusivos e intrusivos[17]. Mientras que los métodos no intrusivos no acceden directamente a los sistemas objetivo, sino que solo influyen negativamente en su funcionalidad mediante diversas medidas, los métodos intrusivos penetran en los sistemas en cuestión. El objetivo aquí es la salida, modificación o infiltración de la información[18].

La figura 3 muestra la complejidad de las amenazas en el ciberespacio e «ilustra la creciente correlación entre la complejidad de los ataques, el creciente grado de interconexión y la disminución de la comprensión de la arquitectura del sistema»[19]. Además, la amenaza sigue aumentando con el tiempo a medida que se desarrollan más y más vectores de ataque, algunos de los cuales se muestran en la figura en el eje naranja.

[15] Un *vector de ataque* se refiere tanto a una ruta de ataque como a una técnica de ataque mediante la cual un atacante lleva a cabo con éxito un ataque a un sistema o servicio informático.
[16] POHLMANN, N. «Glossar Cyber-Sicherheit». 2020. Disponible en: https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/ (consulta 31/1/2022).
[17] KEBER, T. O. y ROGUSKI, P. N. «lus ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis», *Archiv des Völkerrechts*, 49(4). Mohr Siebeck GmbH & Co. KG, 2011, pp. 399-434.
[18] DETHLOFF, N., NOLTE, G. y REINISCH, A. (eds.). *Freiheit und Regulierung in der Cyberwelt: Rechtsidentifikation zwischen Quelle und Gericht.* Berichte der Deutschen Gesellschaft für Internationales Recht, Band 47, Heidelberg: C. F. Müller, 2016.
[19] SCHROEFL, J. «Cyber Power between Fiction and Reality», *The Defence Horizon Journal*. 25 de marzo de 2021. Disponible en: https://www.thedefencehorizon.org/post/cyber-power-between-fiction-and-reality-1?lang=de (consulta 6/9/2021).

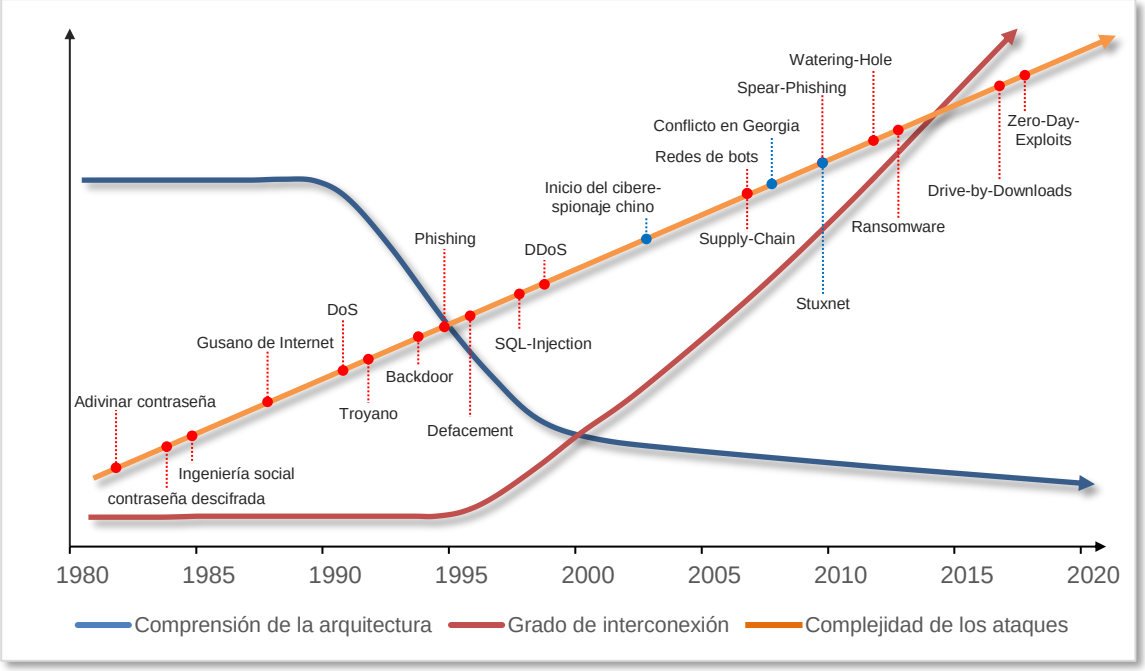

Figura 3. Complejidad de las amenazas en el ciberespacio (elaboración propia a partir de Schroefel)[20]

Advanced Persistent Threats

Un tipo especial de amenaza en el ciberespacio son las llamadas «amenazas persistentes avanzadas» (APT). Se diferencian de otras amenazas de ciberseguridad por los motivos y métodos de los atacantes y suelen ser ataques a largo plazo que se llevan a cabo con gran esfuerzo sobre objetivos seleccionados individualmente. Los ataques APT no se utilizan con fines delictivos, sino para obtener información y, si es necesario, sabotear el objetivo[21].

Las siglas APT son una combinación de tres palabras (en inglés):

- **Avanzado** (advanced): los atacantes de APT suelen estar bien financiados y tienen acceso a las herramientas y técnicas necesarias para llevar a cabo un ataque sofisticado. Una de estas estrategias avanzadas es el uso de múltiples vectores de ataque para lanzar y mantener el ataque.
- **Persistente** (persistent): los atacantes de APT son persistentes y persiguen sus objetivos. Intentan permanecer en un sistema el mayor tiempo posible una vez que se han infiltrado en él. Emplean diversas estrategias defensivas para

[20] Ibíd.
[21] BSI. *Die Lage der IT-Sicherheit in Deutschland 2021*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2021. Disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.html (consulta: 8/6/2022).

evitar ser detectados por los sistemas de detección de intrusos de su objetivo. Para aumentar su tasa de éxito, adoptan un enfoque «lento y constante».

- **Amenaza** (threat): los ataques APT suelen provocar la pérdida de datos sensibles o el compromiso de componentes o misiones vitales. Muchas instituciones y organizaciones nacionales que cuentan con defensas avanzadas para proteger sus misiones y/o datos son cada vez más vulnerables a estas amenazas.

En la actualidad, este tipo de ataques está reservado exclusivamente a los actores estatales o, al menos, patrocinados por el Estado en el ciberespacio, ya que solo pueden ser llevados a cabo por grupos de *hackers* profesionales debido al esfuerzo que suponen[22].

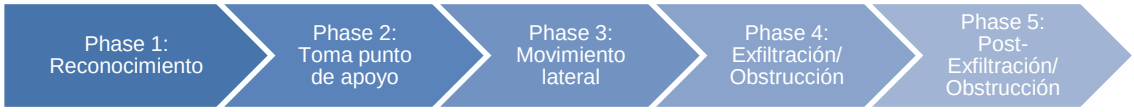

Figura 4. Desarrollo de un ataque APT (elaboración propia)

La figura 4 muestra una secuencia típica de un ataque APT[23]. Tras un reconocimiento inicial, el atacante se hace con un punto de apoyo en el sistema, se desplaza lateralmente si es necesario, y entonces comienza la fuga de datos o la modificación de los datos en el sistema objetivo. Después, se puede permanecer en el sistema o cubrir las propias huellas.

Los retos del ciberespacio

En el uso (militar) del ciberespacio, surgen algunos retos clave[24] para atacantes y defensores:

1. **La fusión de los espacios militares y civiles:** al compartir gran parte de la infraestructura digital, prácticamente todos los ámbitos de la vida (pública) pueden convertirse en un objetivo. La *guerra* en sí puede librarse con medios civiles, pero sus efectos pueden afectar tanto a la esfera militar como a la civil.

[22] ALSHAMRANI, A., MYNENI, S., CHOWDHARY, A. y HUANG, D. «A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities», *IEEE Communications Surveys & Tutorials*, 21(2). 2019, pp. 1851-1877.
[23] Ibíd.
[24] WERKNER, I. J. «Cyberwar – die Digitalisierung der Kriegsführung? Eine Einführung». En: Werkner, I. J. y Schörnig, N. (eds.). *Cyberwar – die Digitalisierung der Kriegsführung*. Springer VS Fragen zur Gewalt, Wiesbaden Heidelberg, 2019, pp. 1-14.

2. **Alta asimetría de efectos:** una característica especial del ciberespacio es que incluso pequeños ataques con muy poco esfuerzo técnico y bajos costes pueden tener un efecto devastador. También es asimétrica la «tolerancia a los fallos»[25]. Mientras que un atacante puede normalmente hacer varios intentos, de los cuales solo uno debe tener éxito, los defensores del ataque solo tienen este único intento y deben tener éxito protegiendo sus sistemas.
3. **Atribución:** el atacante de un ciberataque normalmente solo puede ser identificado con gran retraso y esfuerzo informático forense, si es que lo hace[26]. Esto se debe a varias razones: (1) la *volatilidad* de los rastros en Internet, (2) la facilidad con la que se pueden manipular los propios rastros, (3) la *brecha hombre-máquina*, que en el mejor de los casos identifica el sistema de origen, pero no a la persona que lo origina, y (4) la mundanidad de la herramienta de ataque (PC, memoria USB, etc.).
4. **No hay tiempos de aviso:** no importa la rapidez de un ataque militar convencional: un «primer ataque digital» se produce en fracciones de segundo.

Situación global

En todo el mundo, actores estatales de diversos países realizan ataques en o desde el ciberespacio casi a diario, que son documentados en Internet por diversas instituciones y bases de datos una vez que se conocen. Uno de estos directorios es el proporcionado por el Centro de Estudios Estratégicos e Internacionales[27], aunque solo recoge 820 ciberataques clasificados como *significativos*[28] desde 2003. Como ya se puede ver en la figura 5, los ataques significativos han aumentado considerablemente, especialmente desde 2016.

[25] GAYCKEN, S. «Die vielen Plagen des Cyberwar», en: Schmidt-Radefeldt, R. y Meissler, C. (eds.). *Automatisierung und Digitalisierung des Krieges: Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik*. Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden. 2012, pp. 87-117. doi:10.5771/9783845238227-87

[26] Esta es una de las razones por las que las autoridades policiales dan mucha importancia a la retención de datos.

[27] CSIS. *Significant Cyber Incidents Since 2006*. Center for Strategic and International Studies, 2022. Disponible en: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (consulta: 17/2/2022).

[28] Ciberataques a gobiernos u organizaciones gubernamentales, industrias de defensa, empresas de alta tecnología, así como ataques que superen el importe de los daños de un millón de dólares.

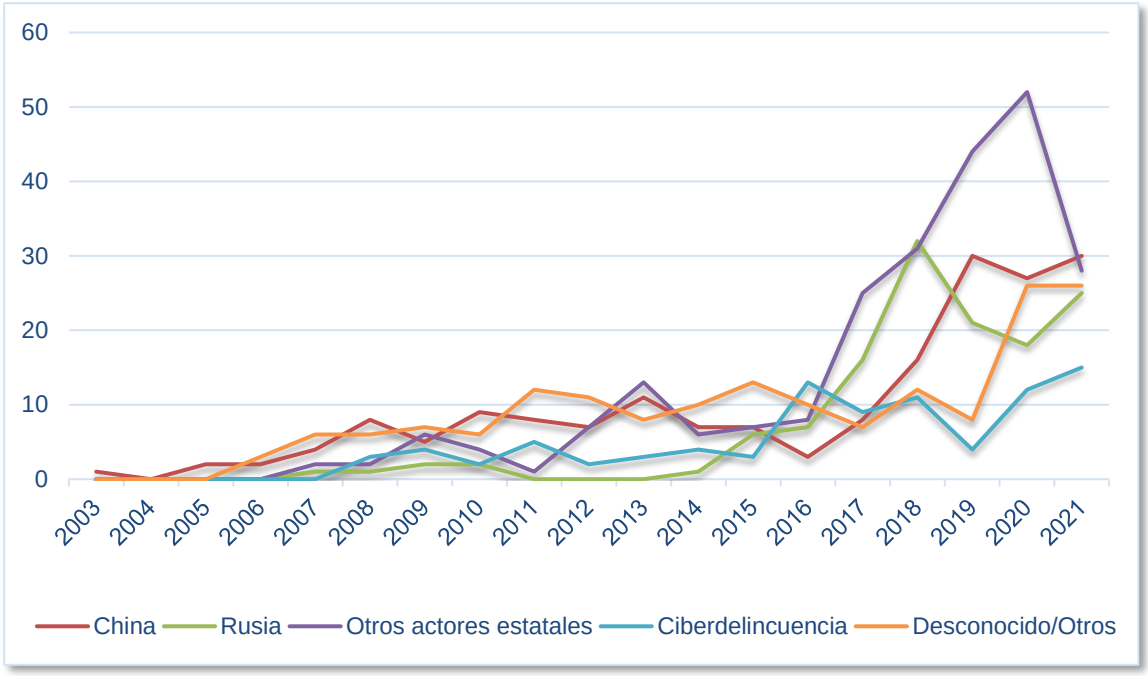

Figura 5. Desglose de casos por actor (elaboración propia)

El análisis de los datos del CSIS (figura 5) permite sacar algunas conclusiones relevantes:

- Aunque la clasificación incluye también a los agentes no estatales, la selección de los objetivos considerados parece indicar que son atacados preferentemente por agentes estatales. Esto parece comprensible dado el *botín* esperado (secretos de Estado y datos gubernamentales, espionaje industrial y grandes sumas de dinero).
- La ciberdelincuencia, que, como es de esperar, debería representar la mayor parte de las acciones ofensivas en el ciberespacio, está infrarrepresentada debido a las limitaciones del conjunto de datos. Solo unos pocos acontecimientos de gran repercusión y alcance entraron en la lista.
- Aunque los demás actores estatales que figuran en la base de datos no están más desglosados, Corea del Norte, Irán, EE. UU., India y Pakistán representan la mayor parte. En el caso de Corea del Norte, en particular, la motivación es principalmente financiera[29], aunque los ataques sean llevados a cabo por el Estado.

[29] SPIEGEL. «Nordkorea soll laut Uno-Bericht Raketenprogramm mit Krypto-Raubzügen finanzieren», *Der Spiegel*. 7 de febrero de 2022. Disponible en: https://www.spiegel.de/netzwelt/netzpolitik/nordkorea-soll-laut-uno-bericht-raketenprogramm-mit-krypto-raubzuegen-finanzieren-a-54bd6901-27f0-4fd8-813a-ddf3f9c6e982 (consulta: 8/6/2022).

- Hasta 2017, los ataques chinos se mantuvieron en un nivel constante (alto). La motivación era casi siempre el espionaje, ya sea contra Estados o industrias. A partir de 2018, las actividades ciberespaciales chinas han aumentado bruscamente. Por un lado, esto podría estar relacionado con el inicio de la presidencia de Donald Trump y su retórica más dura hacia China, que llevó a China a rescindir unilateralmente el acuerdo ciberespacial entre los presidentes Barack Obama y Xi Jinping (Farley, 2018). Por otra parte, también podría estar relacionado con el aumento de la confianza en sí mismo y la búsqueda de la estrategia china «Made in China 2025»[30].
- El número comparativamente alto de actores desconocidos puede atribuirse al mencionado problema de atribución.
- Hasta 2014, Rusia solo apareció con algunas operaciones ciberespaciales ofensivas. Posteriormente, Rusia comenzó a utilizarlas en relación con la anexión de Crimea, violando el derecho internacional. Posteriormente, estos ataques han seguido aumentando. El objetivo seguía siendo predominantemente Ucrania, y la motivación eran las campañas de desinformación o los ataques a las infraestructuras ucranianas (críticas). Los demás casos están relacionados en su mayoría con actividades de espionaje contra otros Estados, como Estados Unidos y países de la UE. Parece que Rusia ha añadido las operaciones ciberespaciales ofensivas a su conjunto de herramientas estatales y militares.

Ampliando la perspectiva

La situación global en el ámbito de las operaciones ciberespaciales ofensivas queda aún más clara cuando se utiliza una base de datos (Hackmageddon.com) que registra un número significativamente mayor de ciberataques, algo más de 15.000 casos[31]. Si se representan ambos conjuntos de datos en un gráfico tras filtrar los actores estatales (figura 6), se observa que el aumento global de 2011 a 2021 es muy similar. Esto indica que ambos conjuntos de datos describen los incidentes en el ciberespacio de forma similar, pero difieren en los criterios de selección. También hay que tener en cuenta que existe un número considerable de casos no denunciados. Estos casos suelen referirse a

[30] La estrategia china «Made in China 2025» es una estrategia de China para cerrar la brecha tecnológica con otros países en diez áreas clave o incluso superarlos. Un medio para ello es el uso masivo del ciberespionaje.
[31] PASSERI, P. *Hackmageddon - Homepage*. Hackmageddon. 2022. Disponible en: https://www.hackmageddon.com/ (consulta: 8/6/2022).

ámbitos gubernamentales, militares o incluso industriales sensibles en los que ninguna de las partes implicadas tiene interés en que se haga público.

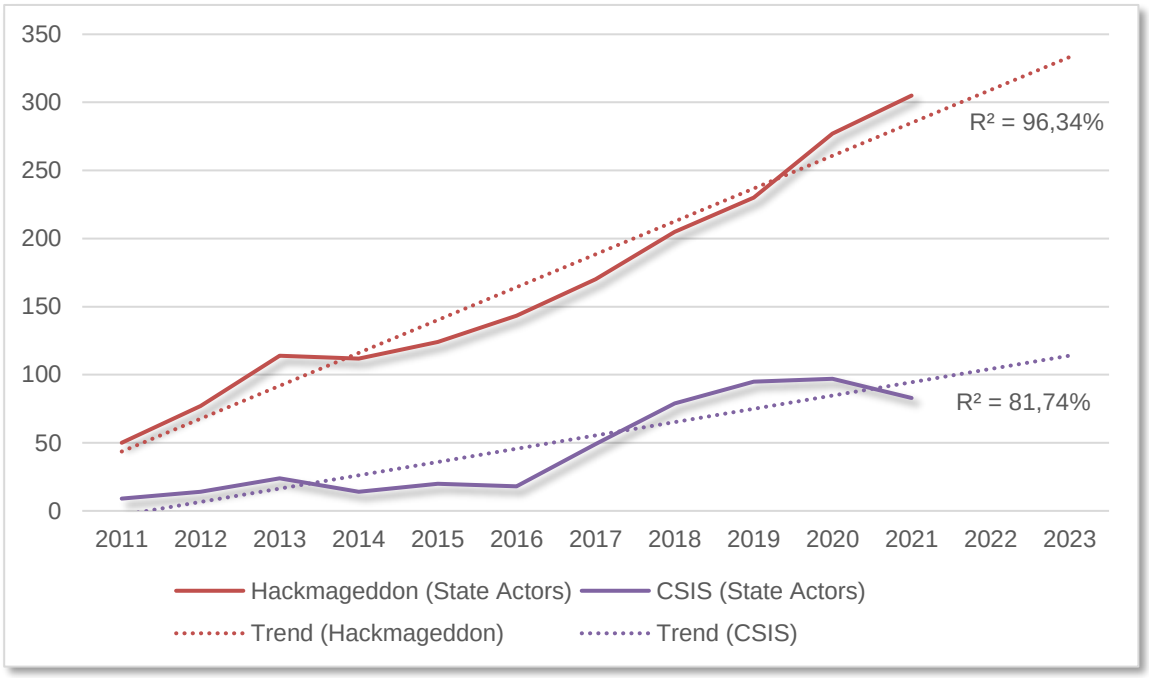

Figura 6. Comparación de los conjuntos de datos de Hackmageddon y CSIS

En resumen, se puede decir lo siguiente: mientras que el porcentaje de operaciones ciberespaciales estatales se mantiene constante a nivel mundial en torno al 10 % de los casos, el número total se ha multiplicado en los últimos 10 años. Los motivos son, entre otros, la obtención de divisas, la realización de campañas de desinformación, el apoyo a operaciones militares o el apoyo a objetivos estratégicos y políticos.

A pesar de este creciente uso del ciberespacio, el uso de operaciones ciberespaciales ofensivas por parte de los actores estatales no siempre tiene como objetivo sustituir los ataques convencionales. Porque, en contra de las representaciones populares, las operaciones ciberespaciales ofensivas (militares) no son un arma polivalente, ya que —al igual que las armas convencionales— están sujetas a numerosas limitaciones, ya sean de carácter político, estratégico, operativo o incluso táctico.

Ámbitos de las amenazas híbridas

Aunque el ciberespacio es solo uno de los muchos dominios dentro de las amenazas híbridas (figura 7), el uso del ciberespacio «desempeña un papel excepcional y muy específico en las amenazas híbridas actuales, entre otras cosas porque todo lo que

importa en el mundo real (incluidos todos los conflictos políticos y militares) también tiene lugar en el ciberespacio»[32].

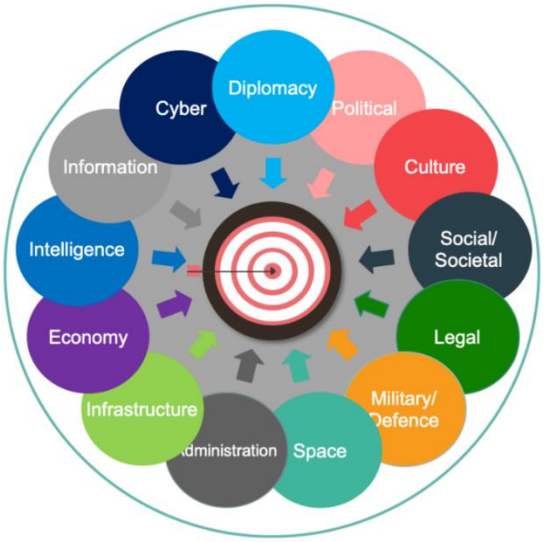

Figura 7. Ámbitos de las amenazas híbridas

A pesar de que las amenazas a la seguridad de los Estados no han cambiado fundamentalmente, el ciberespacio ofrece nuevas posibilidades de uso en cuanto a la velocidad de ejecución, el mecanismo de transmisión y la alta prevalencia e impacto potencial de los ataques[33, 34]. Además, el ciberespacio ofrece la mencionada posibilidad de uso encubierto y de mayor anonimato. No en vano, y debido a la combinación de costes comparativamente bajos y una gran asimetría de efectos, las operaciones ciberespaciales ofensivas son también un medio adecuado para los Estados que no tienen el estatus de gran potencia, como Irán, Corea del Norte, Israel o Pakistán.

Sin embargo, las ciberoperaciones ofensivas también están sujetas a limitaciones y no son adecuadas para todos los escenarios de despliegue de amenazas híbridas dentro de la zona gris (véase figura 2). Una evaluación de Giannopoulos *et al*.[35] demostró que el dominio ciberespacial es una opción o herramienta viable solo en 10 de los 40 escenarios operativos[36], por lo que se encuentra más bien en el medio campo. Para algunos otros escenarios, también es concebible el uso de operaciones ciberespaciales (ofensivas) en relación con el dominio de la información. Entre ellas se encuentran la manipulación del discurso migratorio, el uso de narrativas contradictorias, el descrédito

[32] GIANNOPOULOS, G., SMITH, H. y THEOCHARIDOU, M. *The landscape of hybrid threats: a conceptual model: public version.* Publications Office of the European Union, Luxemburg, 2021, p. 28. Disponible en: https://data.europa.eu/doi/10.2760/44985 (consulta: 6/9/2021).
[33] Ibíd.
[34] MONAGHAN, S. «Countering Hybrid Warfare», *PRISM*, (2). 2022, pp. 82-99.
[35] GIANNOPOULOS, G., SMITH, H. y THEOCHARIDOU, M. *The landscape of hybrid threats: a conceptual model: public version.* Publications Office of the European Union, Luxemburg, 2021. Disponible en: https://data.europa.eu/doi/10.2760/44985 (consulta: 6/9/2021).
[36] Estos son: (1) operaciones físicas contra la infraestructura; (2) creación y explotación de dependencias de la infraestructura; (3) inversión extranjera directa; (4) espionaje industrial; (5) ciberespionaje; (6) operaciones ciberespaciales; (7) explotación de lagunas e incertidumbres en la ley; (8) explotación de normas, procesos, instituciones y argumentos legales; (9) campañas de desinformación y propaganda; y (10) operaciones electrónicas (interferencia de satélites y *spoofing*).

o el apoyo a actores políticos y candidatos, o el control e influencia de los medios de comunicación.

Dominio	Número de menciones
Political	23
Social/Societal	21
Military/Defense	17
Administration	16
Diplomacy	15
Economy	14
Infrastructure	11
Cyber	10(+4)
Culture	9
Space	9
Intelligence	9
Information	9
Legal	6

Tabla 1. Dominios de actividades de amenazas híbridas (elaboración propia)

A pesar de todas las ventajas mencionadas del dominio ciberespacial, algunas herramientas importantes de las amenazas y los conflictos híbridos no pueden (o solo pueden insuficientemente) ser influenciadas por el ciberespacio. En este contexto, es importante señalar que «lo híbrido es siempre una combinación de herramientas, pero no todas las combinaciones son híbridas»[37]. Así, una sola herramienta no es suficiente para cumplir los criterios de una amenaza híbrida (operaciones en la zona gris) o incluso de un conflicto híbrido (la zona entre el conflicto armado irregular y el regular).

Por lo tanto, el hecho de que el uso del ciberespacio se convierta en el instrumento más importante en la resolución de conflictos interestatales, y en qué medida, varía de un país a otro, dependiendo de la motivación o del objetivo político y/o estratégico del actor. No es el caso de Rusia y China, aunque las operaciones ciberespaciales ocupan un lugar destacado en su caja de herramientas. Para EE. UU. la situación no está tan clara. A pesar de todo, se tiende a negar esto porque, al menos superficialmente, otros instrumentos enumerados en la figura 7 (por ejemplo, la diplomacia, la economía, el ejército) parecen ser más relevantes.

En consecuencia, si se utilizan operaciones ciberespaciales ofensivas, los atacantes deben estar muy seguros de que el ataque tendrá realmente éxito y no causará daños colaterales. Los ataques mal ejecutados o incorrectos implican un alto riesgo de escalada. Además, los ataques más complejos requieren un alto grado de conocimientos técnicos y de coordinación[38].

[37] GIANNOPOULOS, G., SMITH, H. y THEOCHARIDOU, M. *The landscape of hybrid threats: a conceptual model: public version.* Publications Office of the European Union, Luxemburg, 2021 p. 33. Disponible en: https://data.europa.eu/doi/10.2760/44985 (consulta: 6/9.2021).

[38] SCHULZE, M. «Militärische Cyber-Operationen: Nutzen, Limitierungen und Lehren für Deutschland», *SWP-Studie*. 2020, doi:10.18449/2020S15

Sin embargo, las ciberoperaciones militares ofensivas limitadas pueden ser útiles para acompañar secuencialmente los ataques convencionales contra adversarios altamente tecnificados. Sin embargo, los Estados obtienen el mayor beneficio del ciberespionaje más que de los efectos militares disruptivos o destructivos.

Consideraciones legales y éticas

Un aspecto que a menudo se subestima es la evaluación legal y ética de las acciones ofensivas en el ciberespacio.

Desde la perspectiva estatal, la cuestión de cuándo un ciberataque puede equipararse a un ataque armado es de importancia central, ya que de ello podría derivarse un derecho de autodefensa[39] securitizado. Los expertos concluyen que el derecho internacional clásico también se aplica en el ámbito ciberespacial[40,41]. Sin embargo, no todo acto perjudicial puede entenderse como un «acto de guerra» en todos los casos, lo que desencadenaría automáticamente el derecho a la autodefensa.

Aunque la inmensa mayoría de los ciberataques no superan este umbral definido, los Estados se reservan, no obstante, el derecho a la autodefensa también en el ciberespacio. Al mismo tiempo, es casi imposible hacer una evaluación diferenciada de las operaciones ciberespaciales estatales, ya que su naturaleza no transparente significa que están en gran medida alejadas de un discurso sobre el derecho internacional[42].

La primera consideración ética de las operaciones ciberespaciales ofensivas fue realizada por primera vez por Randall Dipert[43]. Formuló tres aspectos desafiantes: (1) el problema de la atribución, (2) la defensa contra las operaciones ciberespaciales ofensivas es propensa a los errores, compleja y costosa, y (3) dichas operaciones no tienen componentes exóticos o exclusivos que puedan impedir eficazmente su proliferación. Por estas razones, y porque el derecho internacional existente no podía ser

[39] Un grupo de expertos nombrado por la ONU ha confirmado explícitamente en dos informes que la totalidad de la Carta de la ONU y el derecho internacional vigente también se aplican en el ciberespacio (cf. documento de la ONU A/68/98 [24 de junio de 2013], párrafo 20 y A/70/174 [22 de julio de 2015], en particular el párrafo 28c).
[40] SCHÖRNIG, N. «Gewalt im Cyberraum – ein politikwissenschaftlicher Blick auf Begriff und Phänomen des Cyberkrieges». En: Werkner, I. J. y Schörnig, N. (eds.). *Cyberwar–die Digitalisierung der Kriegsführung.* Springer VS (Fragen zur Gewalt), Wiesbaden, 2019, pp. 39-61.
[41] KREUZER, L. «Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffe». En: Werkner, I. J. y Schörnig, N. (eds). *Cyberwar–die Digitalisierung der Kriegsführung*. Springer VS (Fragen zur Gewalt), Wiesbaden, 2019, pp. 63-86.
[42] Ibíd.
[43] DIPERT, R. R. «The Ethics of Cyberwarfare», Journal of Military Ethics, 9(4. 2010, pp. 384-410. doi:10.1080/15027570.2010.536404

transferido 1:1 a las ciberoperaciones ofensivas, Dipert predijo una especie de «guerra fría» de larga duración en el ciberespacio.

Para resolver este problema legal y ético, sería necesario que las naciones líderes en el ámbito del ciberespacio se sentaran a la mesa y se impusieran mutuamente normas, que luego se aplicarían como directrices éticas y legales sostenibles para toda la comunidad internacional.

Ahora bien, debido a la actual situación mundial tras la invasión rusa de Ucrania en 2022, actualmente es muy poco probable que los actores mencionados se pongan de acuerdo en unas directrices vinculantes a nivel internacional. Por lo tanto, los dilemas y desafíos legales y éticos mencionados anteriormente seguirán sin resolverse por el momento.

Conclusiones

En los primeros días de Internet, eran predominantemente actores no estatales los que explotaban los puntos débiles de los sistemas y las operaciones ciberespaciales ofensivas, tal y como las conocemos hoy, apenas tenían lugar, si es que las había. Esto solo cambió con el aumento de las redes informáticas en la década de 1990. Sin embargo, debido al alto nivel de complejidad, la comprensión de la arquitectura de las redes siguió disminuyendo. Esto facilitó no solo a los ciberdelincuentes, sino también a los agentes estatales, la realización de ciberoperaciones militares de gran alcance mediante ataques cada vez más complejos.

Al mismo tiempo, este nuevo tipo de ataque se ancló explícitamente en las doctrinas militares de muchos Estados, lo que profesionalizó aún más el uso de estos ataques. Se crearon unidades dedicadas cuya única tarea es llevar a cabo este tipo de operaciones de acuerdo con los respectivos principios operativos formulados. En el proceso, resultó que las operaciones ciberespaciales a veces hicieron posibles ataques que de otro modo no habrían podido tener lugar, o solo con gran riesgo. Un ejemplo destacado de ello es el conocido ataque Stuxnet a las plantas de enriquecimiento de uranio iraníes.

Para China, por ejemplo, no había alternativa a las operaciones ciberespaciales para lograr sus objetivos políticos y estratégicos. Pero también en los ataques más recientes, que se están produciendo actualmente en Ucrania 2022, los ciberataques de diversas formas desempeñaron un papel importante, que, sin embargo, aún no puede evaluarse de forma concluyente. Sin duda, otros Estados observarán de cerca los últimos

acontecimientos para sacar sus conclusiones tanto del efecto como de las reacciones internacionales.

En definitiva, hay que decir que el escenario de amenazas en el ciberespacio es cada vez mayor. La creciente complejidad de las operaciones ciberespaciales ofensivas, la disminución de la comprensión de la arquitectura combinada con la interconexión cada vez más avanzada se yuxtapone con una situación global que no ha sido tan conflictiva desde hace mucho tiempo. Es muy probable que gran parte de esto tenga lugar también en el ciberespacio.

*Christian Dieterich**
Teniente coronel Ejército del Aire alemán
Alumno del Curso de Estado Mayor de las Fuerzas Armadas en España