Documento
Opinión

24/2023 7 de marzo de 2023

María De Álvaro Mizzian *

El ciberespacio en tiempos de guerra: la IT Army ucraniana

El ciberespacio en tiempos de guerra: la IT Army ucraniana

Resumen:

La agresión rusa a Ucrania en febrero de 2022 trajo consigo la vuelta de la guerra a Europa: una guerra que ya no solo se libra en el campo de batalla, sino que también se desarrolla en escenarios como el ciberespacio. Estos nuevos escenarios implican la participación de nuevos actores en los conflictos. La posibilidad de una ciberguerra se lleva teorizando una década, pero nunca se ha estudiado como parte de un conflicto mayor. La rápida respuesta del Gobierno ucraniano para la protección del ciberespacio, con la creación de la IT Army y la movilización de otros actores cibernéticos, provee por primera vez un ejemplo que permite observar el alcance de las amenazas digitales para los Estados.

Este documento se abre con una breve introducción al ciberespacio, repasa los intentos de regulación de las actividades dañinas que se llevan a cabo en él y analiza el caso de la IT Army ucraniana para entender el lugar que la ciberguerra ocupa hoy en día en el marco de los conflictos internacionales.

Palabras clave:

Ciberguerra, ciberespacio, Anonymous, Ucrania, IT Army, *hackers,* hacktivismo.

Cyberspace in times of war: the Ukrainian IT Army.

Abstract:

The Russian aggression to Ukraine in February 2022 brought back war to Europe, a war that doesn't take place only in the battlefield but also in new scenarios like cyberspace. Along with these new sceneries, a number of new actors who take part in said conflicts can also be found. The possibility of cyberwarfare has been theorized for a decade but it was never possible to study it as part of a greater warlike conflict. The rapid response of the Ukrainian government for the protection of their cyberspace by creating the IT Army and the mobilization of other cybernetic actors provide, for the first time, an example to observe the scope of digital threats for states.

This document presents an introduction to cyberspace, the attempts made for the regulation of damaging activities in it and analyses the case of the Ukrainian IT Army to understand the place cyberwarfare holds in international conflicts.

Keywords:

Cyberwarfare, Cyberspace, Anonymous, Ukraine, IT Army, hackers, hacktivism.

Cómo citar este documento:

DE ÁLVARO MIZZIAN, María. *El ciberespacio en tiempos de guerra: la IT Army ucraniana*. Documento de Opinión IEEE 24/2023.
https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO24_2023_MARALV_Ciberespacio.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

Cuando el 24 de febrero de 2022 las tropas rusas comenzaron las maniobras de invasión del territorio ucraniano, el presidente ucraniano Volodímir Zelenski hizo un llamamiento a la defensa del país: una defensa que protegiese la soberanía ucraniana en todos los espacios, incluyendo el digital. La sociedad internacional respondió con sorpresa a la inclusión del ciberespacio en la estrategia nacional de defensa a la agresión, puesto que, hasta el momento, la guerra siempre se había considerado como puramente militar.

El ciberespacio representa una herramienta de uso diario en los países desarrollados y a la vez es un gran desconocido. En ocasiones este se ha descrito como un espacio común global, abierto y dinámico, que queda fuera de la jurisdicción. A pesar de que el ciberespacio podría encajar con la definición tradicional de un espacio común, quizás sea más apropiado calificarlo como una heterotopía. Las heterotopías[1] son espacios que se dibujan en la institución social y que pueden ser descritos como lugares fuera de la sociedad aunque sean efectivamente localizables. La noción de ciberespacio podría ajustarse a esta última definición si lo consideramos un espacio creado por la sociedad en el que participamos a diario, pero que no se ajusta a la soberanía y la jurisdicción que otros espacios sí tienen. A efectos de este artículo, el ciberespacio se define como un «entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos mediante redes informáticas»[2].

Dentro de la intangibilidad descrita, encontramos lo que puede considerarse el mayor problema del ciberespacio: la falta de control. Y es que no existe una autoridad mundial que controle lo que ocurre en este dominio y vigile las actividades ilícitas que en él se puedan desarrollar. Así, ha surgido un movimiento de ataques y amenazas a la seguridad de las personas a través de diversos delitos cibernéticos. Los delitos cibernéticos son aquellas acciones antijurídicas que se llevan a cabo a través de internet[3]. Entre los múltiples delitos recogidos por esta definición figuran ataques que pueden dañar seriamente a la población, pues permiten dañar infraestructuras básicas y frenar el

[1] FOUCAULT, M. «Des espaces autres», *Empan*, 54. 2002, pp. 12-19. Disponible en: https://doi.org/10.3917/empa.054.0012 [consulta: 14/11/2022]
[2] SCHMITT, M. N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2.ª ed).: Cambridge University Press, Cambridge, 2007.
[3] XIII CONGRESO SOBRE PREVENCIÓN DEL DELITO Y JUSTICIA. «Delito cibernético». Doha, del 12 al 19 de abril de 2015. Disponible en: https://www.un.org/es/events/crimecongress2015/cibercrime.shtml [consulta: 14/11/2022]

funcionamiento de ciudades enteras. Así nació lo que hoy se conoce como ciberguerra, una guerra que no se ajusta a los principios clásicos de un conflicto y que escapa a cualquier regulación, una guerra en la que pueden participar actores de todo tipo y, a primera vista, salir indemnes.

La sociedad internacional respondió con sorpresa a la estrategia para la protección del ciberespacio iniciada por el ministro de Transformación Digital ucraniano a raíz de los acontecimientos del 24 de febrero de 2022. Hasta entonces la ciberdefensa había sido una tarea encargada a cuerpos de militares expertos, en especial en el caso de Ucrania, que había sufrido ataques continuos desde los meses anteriores al comienzo de la agresión rusa[4,5]. Así pues, ante la amenaza de un aumento de estos ataques, la participación en dichas maniobras de defensa se amplió a voluntarios y a personal especializado del ámbito civil, con lo que se difuminaron los límites conocidos hasta el momento entre los combatientes y las personas protegidas[6].

El ciberespacio y su uso para actividades ilegales: la ciberguerra

Las operaciones cibernéticas se engloban dentro del concepto de amenazas híbridas. En un mundo en una continua competición entre actores, previa al estallido de un conflicto armado convencional, encontramos la denominada como zona gris[7,8]. En esta zona gris se ponen en marcha ataques y amenazas no convencionales, como los ciberataques, y se inicia lo que se conoce como guerra híbrida. En ocasiones estas

[4] MILLER, C. «Throwback attack: Russia breaches Wolf Creek Nuclear Power facility», *Industrial Cybersecurity Pulse*. 24 de febrero de 2022. Disponible en: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-russian-breaches-wolf-creek-nuclear-power-facility/

[5] POLITYUK, P. y HOLLAND, S. «Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war». Reuters, 14 de enero de 2022. Disponible en: https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/

[6] Los límites mencionados son los presentes en el Convenio de Ginebra (1949), relativo a la protección debida en tiempo de guerra a las personas civiles, un estatus cuya aplicación se podría poner en duda en el caso de los voluntarios de la IT Army.

[7] LÓPEZ-LAGO LÓPEZ-ZUAZO, M. «La competición en el continuum» (Documento de Opinión, n.º 56). IEEE, 2021. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO56_2021_MANLOP_Competicion.pdf [consulta:16/11/2022].

[8] U.S. MARINE CORPS. *Competing* (MCDP 1 4). Estados Unidos, 2020. Disponible en: https://www.marines.mil/Portals/1/Publications/MCDP%2014.pdf?ver=fGwjmqkxGvv0GPe0mPgdqw%3d%3d [consulta: 10/11/2022].

amenazas no convencionales se extienden más allá del umbral de violencia[9] y son usadas como estrategia junto con acciones cinéticas convencionales.

Tanto estudios privados[10] como gubernamentales[11] identifican una tendencia al alza en el número de ciberofensas a empresas y entidades públicas. Estos datos obligan a prestar mayor atención a esas nuevas amenazas y, en especial, a las implicaciones legales para los individuos que en ellas participan. La motivación para llevar a cabo operaciones cibernéticas puede ser distinta para cada individuo: económica, relacionada con la búsqueda de poder o simplemente destructiva. No obstante, este trabajo se centra en los ciberataques con una finalidad dañina, porque la simple intención de causar daños afecta a las repercusiones que los atacantes puedan sufrir, especialmente si sus acciones se producen en el marco de un conflicto mayor.

Una particularidad de los ataques realizados en el ciberespacio es su difícil atribución[12]. La naturaleza del ciberespacio permite que los atacantes se escondan tras el anonimato gracias a un amplio conocimiento del sistema y de su funcionamiento. Por ejemplo, para muchos de ellos cambiar la dirección IP del ordenador desde el que se lanza la ofensa conforma un conocimiento básico. Este problema de atribución constituye la mayor dificultad para redactar y aplicar una legislación equivalente a la existente para otras amenazas. La mayor parte de las atribuciones de ciberataques que se han podido hacer son especulativas, pero apuntan a dos tipos diferenciados de actores. El primer tipo son grupos y personas respaldados por entes estatales, como la IT Army ucraniana que estudia este artículo. Estos actores son menos numerosos debido a las implicaciones en el derecho internacional de las acciones ilegítimas llevadas a cabo por agentes estatales o por representantes de ellos. El segundo tipo son grupos organizados y personas que actúan de manera independiente, sin mandato o control directo de un Estado. Estos grupos, aunque independientes, pueden participar en la asistencia a un Estado o a su población, suelen actuar por iniciativa propia con una motivación ideológica, religiosa o

[9] LÓPEZ-LAGO LÓPEZ-ZUAZO, M. *Op. cit.*
[10] RISK BASED SECURITY INC. *2021 Year End Report*. Estados Unidos, 2022. Disponible en: https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf [consulta: 17/11/2022].
[11] DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT. *Cyber Security Breaches Survey 2022*. Londres, 2022. Disponible en: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 [consulta: 17/11/2022].
[12] Comprendida como la presencia de una conducta activa o pasiva y la posibilidad de atribuir esa conducta a un determinado sujeto.

patriótica y son conocidos como hacktivistas[13].

A pesar de las dificultades, la sociedad internacional ha sido capaz de identificar el peligro de la falta de jurisprudencia relativa a los ataques cibernéticos y la ciberguerra. Es importante que, a la par que se realizan avances legislativos nacionales en lo que respecta a estas amenazas —por ejemplo, la Estrategia Nacional para la Ciberseguridad española de 2019—[14], se intente alcanzar una aproximación internacional al problema. Mientras que algunas organizaciones consideran que el derecho internacional clásico se aplica a esta dimensión[15], otros actores dudan de la utilidad de él debido a la generalidad de sus principios[16]. Con carácter global, las Naciones Unidas pusieron en marcha un estudio sobre el problema del ciberespacio a través su Comité Primero, encargado del desarme y la seguridad internacional. El tema es tratado dentro de la organización por dos entidades: un grupo de agentes gubernamentales y un grupo de trabajo abierto.

Con carácter regional, la Unión Africana acometió un intento legislativo cuando en 2014 se aprobó la «Convención sobre ciberseguridad y protección de datos personales»[17]. En la Unión Europea (UE) se aprecian avances en la legislación del ciberespacio: en 2020 se aprobó la «Comunicación conjunta sobre la estrategia de ciberseguridad de la UE para la década digital»[18], el primer intento de establecer unos mínimos en ciberseguridad comunes a los veintisiete Estados miembros.

Sin embargo, hoy en día la estrategia legislativa que puede ser considerada más avanzada en materia de ciberseguridad y regulación del ciberespacio es la propuesta por la Organización del Tratado del Atlántico Norte (OTAN). Mediante la creación del Centro de Excelencia para la Ciberdefensa Cooperativa, la organización dedicó recursos a

[13] SCHMITT, M. N. *Op. cit.*
[14] DEPARTAMENTO DE SEGURIDAD NACIONAL. *Estrategia nacional de ciberseguridad 2019*. Presidencia de Gobierno, Madrid, 2019. Disponible en: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf
[15] ORGANIZACIÓN DE LAS NACIONES UNIDAS. «Informe del grupo de expertos gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional del 24 de junio de 2013 (A/68/98)». Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/69/PDF/N1337169.pdf?OpenElement
[16] WRIGHT, J. «Cyber and International Law in the 21st Century» (comunicación). Chatham House Royal Institute for International Affairs, Londres, 23 de mayo de 2018. Disponible en: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century .
[17] UNIÓN AFRICANA. African Union Convention on Cyber Security and Personal Data Protection. 27 de junio de 2014. Disponible en https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[18] COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO. «La estrategia de ciberseguridad de la UE para la década digital (JOIN/2020/18 final)». 12 de diciembre de 2020.

cualquier ámbito que pudiese estar relacionado con la ciberdefensa: la educación, los análisis, la investigación e incluso el desarrollo de propuestas legislativas para la regulación del ciberespacio.

Gracias a este centro, la OTAN ha podido diferenciar dos grandes corrientes legislativas en lo que se refiere a la ciberseguridad[19]: la primera, un aumento de la adopción de estrategias nacionales, tal y como se ha mencionado; la segunda, la existencia de un debate teórico sobre la aplicación del derecho internacional a las operaciones cibernéticas, porque, a pesar de que algunas amenazas son controlables y sancionables de forma nacional, cuando estas se producen a través del ciberespacio pueden convertirse muy rápidamente en transfronterizas y susceptibles de desestabilizar el equilibrio internacional. Dentro de esta segunda corriente se encuadra la iniciativa del *Manual de Tallin,* un proyecto de aplicación de las normas del derecho internacional al ciberespacio. Su primera edición fue publicada en 2013 y se centraba en ataques que podían ser analizados como ejemplo del uso de la fuerza, es decir, como posibles quebrantamientos del principio estructural del derecho internacional (art. 2.4 de la Carta de las Naciones Unidas). Una revisión de este manual vio la luz en 2017 con la publicación del *Manual de Tallin 2.0,* que recoge un espectro más amplio de ataques, incluso aquellos que no superan el umbral del uso de la fuerza.

Hasta el momento se han sentado las bases de un marco puramente teórico sobre el ciberespacio y sus intentos de regulación, pero pocas veces se ha estudiado de manera práctica una situación real. Por eso este análisis se centra en el caso específico de la creación de la IT Army ucraniana, para intentar comprender la importancia de la situación actual de cara al futuro de los conflictos mundiales.

La IT Army ucraniana

El 26 de febrero de 2022, solo dos días después del comienzo de la agresión rusa, el ministro ucraniano Mijailo Fedorov anunciaba a través de su cuenta de Twitter un movimiento inesperado para la defensa nacional. Fedorov, que ostenta la cartera de Transformación Digital, anunciaba la creación de una *IT army,* centrada en las amenazas

[19] TALIHÄRM, A. M. «Towards Cyberpeace: Managing Cyberwar through International Cooperation», *UN Chronicle*, vol. L, n.º 2. Nueva York, 2013. Disponible en: https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

en el ciberespacio, y llamaba a la participación de profesionales de todo el mundo en ella[20]. La iniciativa suponía un movimiento inédito en la ciberseguridad mundial, puesto que, por primera vez, se proponía la creación de un cuerpo gubernamental *ad hoc* dedicado a la defensa y el ataque en el ciberespacio y se pedía la participación de civiles. Con ello se imprimía un claro giro a lo que hasta el momento se había visto en otros países que cuentan con cuerpos para la defensa del ciberespacio en el marco de sus fuerzas armadas[21]. Pero no solo el campo de actuación de este «ejército» causó sorpresa, también lo hizo su composición, pues se animó a la participación a ciudadanos de todo el mundo y no solo de Ucrania. Con el fin de facilitar la conexión con los interesados, en el tuit de Fedorov también aparecía el vínculo a un canal de Telegram, desde el cual se harían llegar tareas a los participantes en la IT Army.

La existencia de agencias y grupos especializados en ciberataques de origen ruso[22] es una realidad conocida desde antes de que se produjera la agresión a Ucrania. Han sido relacionados con Rusia ciberataques como el de BlackEnergy en 2015, que interrumpió la electricidad en zonas de Ucrania [23]; el *ransomware* WannaCry, lanzado en 2018 y que afectó a las infraestructuras informáticas de múltiples empresas y servicios públicos europeos, e incluso el ciberataque a la Colonial Pipeline de Estados Unidos en 2021, que frenó el suministro de carburantes a diversas zonas del país[24]. Así pues, la lucha contra los efectos de estos ataques resulta comprensible. No obstante, la respuesta institucionalizada y abierta al público supuso una sorpresa importante para la sociedad

[20] FEODOROV, M. (@FedorovMykhailo). «We are creating an IT army. We need digital talents. All operational tasks will be given here: https://t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists». Twitter, 26 de febrero de 2022. Disponible en: https://twitter.com/FedorovMykhailo/status/1497642156076511233?s=20&t=mF7nE7Z9tZq90eL2N2L5ew

[21] Un ejemplo claro fue la creación del Mando Conjunto del Ciberespacio español en 2013, a través de la «Orden del Ministerio de Defensa 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa» (https://www.boe.es/eli/es/o/2013/10/30/def2012). Otro ejemplo es el United States Cyber Command, creado en 2010 por el Gobierno estadounidense. Ambos casos reflejan la existencia de cuerpos militares dedicados al ciberespacio, distintos de la IT Army, abierta a la participación a expertos civiles.

[22] La atribución de ciberataques a un país o grupo de *hackers* es una de las cuestiones de mayor dificultad a la hora de legislar sobre el tema. Este párrafo hace referencia a la atribución de esos ataques por parte de organismos públicos de los Estados afectados a grupos de *hackers* de origen ruso.

[23] PAKHARENKO, G. «Cyber Operations at Maidan: A First-Hand Account», en GEERS, K. (ed.), *Cyber war in perspective: Russian aggression against Ukraine.* CCDCOE, 2015, pp. 60-65. Disponible en: https://web.archive.org/web/20161202005747/https:/ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

[24] BING, C. y KELLY, S. «Cyber attack shuts down U.S. fuel pipeline "jugular", Biden briefed». Reuters, 8 de mayo de 2022. Disponible en: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ [consulta: 6/11/2022]

internacional.

Poco ha sido desvelado por parte del Gobierno ucraniano sobre la verdadera estructura de esta organización. Sí se conoce, sin embargo, la colaboración en la ciberdefensa ucraniana de Yegor Aushev y de distintas compañías. Aushev es conocido dentro de este mundo por ser confundador de la compañía de ciberseguridad Hacken y de una ciberescuela en Ucrania. En entrevistas ha comentado que, horas después de que comenzara la agresión, el Ministerio de Defensa ucraniano se puso en contacto con él para que participara en la movilización de la comunidad *hacker* ucraniana contra los ciberataques rusos[25]. También se atribuye a Aushev la redacción del primer llamamiento a la ciberresistencia ucraniana, que apareció en múltiples foros de la comunidad *hacker* del país[26].

Según la información dada por Aushev, la IT Army se dividiría en un grupo de defensa y un grupo de ataque y estaría formada por profesionales respaldados por expertos en la materia[27]. Esta idea de la participación exclusiva de expertos se opondría a las prácticas del ministro Fedorov cuando compartió el *link* a un canal público donde se publicarían «misiones» para los colaboradores. Sin embargo, la información suministrada por un participante anónimo de la IT Army deja ver que el grupo está liderado por un equipo de veinticinco profesionales de origen ucraniano[28]. Y es que la IT Army, además de con un amplio número de profesionales y especialistas, cuenta con un grupo importante de lo que expertos como Aushev llaman *script kiddies*[29]: un conjunto de participantes en la actividad del grupo sin experiencia profesional en el sector IT, que, en el caso del ciberejército ucraniano, se cree que provienen de todo el mundo. Las comunicaciones de la IT Army realizadas a través de canales públicos, como Telegram, Twitter y su propia página web, se dirigen a este último sector.

La importancia de este grupo de *script kiddies* radica en la naturaleza de los ataques que pretendería llevar a cabo la IT Army ucraniana. La actividad del grupo se centra en

[25] SCHECTMAN, J. y BING, C. «EXCLUSIVE: Ukraine calls on hacker underground to defend against Russia». Reuters, 25 de febrero de 2022. Disponible en: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ [consulta: 6/11/2022].
[26] *Idem*.
[27] DELCKER, J. "Inside Ukraine's Cyber Guerrilla Army". *DW*, 24 de marzo de 2022. https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527. [Consultado el 6/11/ 2022]
[28] SCHECTMAN Y BING, *Op. cit.*
[29] DELCKER, J. *Op. cit*.

ataques de denegación de servicio distribuido (DDoS) a distintas entidades rusas. Estos ataques se llevan a cabo a través de un aumento del tráfico que reciben los servidores de los objetivos, con lo que la red se sobrecarga y se provoca una caída del servicio[30]. Los números que aporta la globalización de la lucha cibernética ucraniana ayudan de manera importante al éxito de dichas maniobras. Las razones expuestas por los participantes extranjeros en este ejército digital son variadas, pero todos mencionaban la necesidad de prestar ayuda a la población ucraniana cuando se hicieron públicas las imágenes de la situación del país[31]. El ejército voluntario está formado en su mayoría por jóvenes que son nativos digitales y que a lo largo de su vida han adquirido conocimientos de programación y *software.* A través de diversas entrevistas se ha conocido que la distribución geográfica de los voluntarios es extensa, desde Dinamarca a los Países Bajos[32], pasando por Suiza y Nueva York[33].

Pero la IT Army no está sola en la ciberdefensa de Ucrania. Múltiples organizaciones de *hackers* que existían previamente se han unido a la causa. La actividad del ciberejército no podía centrarse solamente en el ataque, eran necesarias campañas informativas para cosechar el apoyo de la opinión pública a la causa. Por eso la organización Squad303, un colectivo de origen polaco ligado al conocido Anonymous, abandera una importante campaña de información en los dispositivos de origen ruso[34]. Esta también se beneficia de la acción de voluntarios de todo el mundo, quienes, a través de la página web de Squad303, pueden enviar mensajes a través de múltiples plataformas digitales.

Pero no es posible hablar del mundo cibernético sin mencionar el posicionamiento de Anonymous. Desde su creación en 2004[35], este colectivo ha participado en algunas de

[30] CYBERSECURITY AND INFRASTRUCTURE SECUTITY AGENCY (CISA). *Understanding Denial-of-Service Attacks. Security Tip (ST04-015)*. Washington, 2009. Disponible en: https://www.cisa.gov/uscert/ncas/tips/ST04-015 [consulta: 19/11/2022]

[31] STOKEL-WALKER, C. y MILMO, D. «"It's the Right Thing to Do": The 300,000 Volunteer Hackers Coming Together to Fight Russia». *The Guardian*, 15 de marzo de 2022. Disponible en: https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia .

[32] DELCKER, J. *Op. cit.*

[33] STOCKEL-WALKER, C. y MILMO, D. *Op. cit.*

[34] SQUAD303 (@squad3o3). «Who are we? Just an anonymous people... Why are we? To #fightforUkraine #OpRussia #UkraineUnderAttack #UkraineRussianWar». Twitter, 6 de marzo de 2022. Disponible en: https://twitter.com/squad3o3/status/1500566343770329090?s=20&t=9X8d-G1x5NaJQEFc9cy_OQ

[35] LANDERS, C. «Serious Business», *Citypaper Online Columns.* 4 de febrero de 2008 (archivado desde el original el 8 de abril de 2008). Disponible en: https://web.archive.org/web/20080408092335/http://www.citypaper.com/columns/story.asp?id=15543

las campañas de hacktivismo más importantes de los últimos años[36]. Desde el bloqueo a la participación *online* de la organización terrorista Dáesh[37] a operaciones de apoyo a los movimientos populares de Túnez[38] y Egipto[39] durante las Primaveras Árabes, Anonymous se ha convertido en el actor más importante en el mundo digital. Antes de la invasión, Anonymous había comenzado la llamada Samantha Smith Operation, en la cual, entre otras acciones, se utilizaban webs de empresas chinas para advertir sobre las consecuencias del aumento de las tensiones en Ucrania y para instar a las Naciones Unidas al despliegue de unidades pacificadoras en el Donbás[40].

Una vez comenzó la agresión contra Ucrania, Anonymous declaró la ciberguerra a Rusia y lanzó una ofensiva contra numerosas webs de su Gobierno[41]. A lo largo de la guerra los *hackers* de Anonymous han llevado a cabo distintas acciones contra Rusia y han compartido su conocimiento y experiencia con los miembros de la IT Army ucraniana para el desarrollo de ataques cibernéticos.

A pesar de que la situación de los grupos mencionados pueda antojarse parecida, existe una gran diferencia entre sus miembros: la consciencia de la ilegalidad de las acciones. Los miembros de Anonymous y Squad303 son conscientes de la ilegalidad de los ciberataques y de las consecuencias que estos pueden tener. En múltiples ocasiones han sido detenidos *hackers* relacionados con Anonymous y la organización es consciente de ello. Sin embargo, por lo que las entrevistas dejan ver, los *hackers* voluntarios o *script kiddies* que participan en los ataques DDoS son conscientes de la dudosa legalidad de las actividades pero no consideran que puedan sufrir repercusiones. Y, sobre todo, la situación especial puede producir que las acciones cibernéticas se lleven a cabo en el marco de un conflicto armado internacional.

---

[36] Se considera *hacktivismo* la serie de actividades de desobediencia civil que se lleva a cabo utilizando herramientas cibernéticas (SCHMITT, M. N. *Op. cit*).
[37] COTTEE, S. «The Cyber Activists Who Want to Shut Down ISIS», *The Atlantic.* 8 de octubre de 2015. Disponible en: https://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312/
[38] ANONYMOUS. «OPERATION TUNISIA — A Press Release». Disponible en: https://youtu.be/BFLaBRk9wY0
[39] SOMAIYA, R. «Hackers Shut Down Government Sites», *The New York Times*. 2 de febrero de 2011. Disponible en: https://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html?_r=1
[40] EVERINGTON, K. «Anonymous posts Taiwan flag, Peng Shuai on CCP website». Taiwan News, 7 de febrero de 2022. Disponible en: https://www.taiwannews.com.tw/en/news/4434420
[41] PURTILL, J. «Hacker collective Anonymous declares “cyber war” against Russia, disables state news website». ABC News, 25 de febrero de 2022. Disponible en: https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160

Múltiples Estados modernos ponen restricciones o incluso prohíben la participación de nacionales en conflictos armados extranjeros, especialmente en conflictos en los que lucharían contra un Estado amigo[42]. Las legislaciones que prohíben la participación militar en conflictos extranjeros son demasiado antiguas para contemplar la idea de un ejército digital. Un ejemplo especialmente claro es la Foreign Enlistment Act[43] británica, que regula la participación de nacionales en conflictos extranjeros, aprobada en 1870 y revisada por última vez en 2008, cuando aún era impensable una guerra digital.

Pero la falta de regulación no solo afecta a la legalidad de las acciones, sino también a la posible necesidad de protección de los participantes en la ciberguerra. Si la IT Army hubiese sido considerada un grupo armado dentro del conflicto, se produciría un vacío en la cobertura legal de sus miembros y si se les aplicarían las normas del derecho internacional humanitario. No considerar a este cuerpo como un combatiente no deja de ser una decisión debatida, puesto que de manera efectiva la coordinación de las acciones corre a cargo del Ministerio de Transformación Digital ucraniano. Esto implicaría que el grupo no puede beneficiarse de las ventajas que el derecho internacional humanitario concede a las personas en los conflictos, en especial si sufrieran represalias por parte de *hackers* rusos. En algunos casos podrían llegar a ser considerados y juzgados en calidad de participantes en las hostilidades.

Sin embargo, parece que el momento para abordar las cuestiones jurídicas concernientes a la ciberguerra no tiene por qué ser este. A pesar del miedo que existía en febrero de 2022 a una ciberguerra que pusiese en peligro a la población, a noviembre de 2022 parece que no se han llevado a cabo grandes acciones[44]. Aunque sí se han producido numerosos ataques que han afectado momentáneamente a entidades de ambos bandos[45], el flujo de ciberataques no ha llegado al nivel esperado por la sociedad

[42] En inglés, «state at peace». Debido a dificultades de traducción, en este caso se considera «Estado amigo» no aquel con el que se mantiene una buena relación, sino aquel que en el momento de la ofensa mantiene una relación de paz con el Estado de origen del combatiente.
[43] Foreign Enlistment Act 1870, s. 4. Disponible en: https://www.legislation.gov.uk/ukpga/Vict/33-34/90/contents [consulta: 25/11/2022]
[44] GAVRILA, A. «La gran ciberguerra de Ucrania que no ocurrió» (Documento de Opinión, n.º 99). IEEE, 2022. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf [consulta: 30/11/2022].
[45] ESET. *Threat Report T1, 2022*. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

internacional[46,47]. Por consiguiente, en lo que respecta a los conflictos armados actuales, los métodos clásicos de acción militar siguen siendo los preferidos y las nuevas herramientas, como la guerra cibernética, se mantienen en la zona gris.

Conclusiones

Todo análisis de lo que ocurre actualmente en Ucrania debe ser tomado con precaución, debido a la incertidumbre que sigue rodeando al conflicto. Sin embargo, esto no quita la necesidad de estudiar los pasos más importantes que se han dado en el marco de la agresión. Dejando a un lado las acciones que se hayan llevado a cabo finalmente, con la creación de un grupo cuya función inicial consistía en brindar protección ante las amenazas cibernéticas se materializaba una idea presente en los estudios geopolíticos de los últimos años: el ciberespacio se ha convertido en un nuevo campo de batalla. Se abre así una nueva vía de necesaria consideración en cualquier nueva escalada bélica, pues la defensa de este espacio prueba ser un eje importante para los suministros básicos de un país.

A medida que el siglo XXI transcurre, se puede ver cómo diversas tecnologías, como el *Internet of things*[48], avanzan en todos los ámbitos de la vida. Hemos podido apreciar los efectos de ataques cibernéticos a redes eléctricas y medios de comunicación. No obstante, es importante tomar en consideración los efectos que podrían derivarse de la aplicación de estos ataques a vehículos, electrodomésticos e incluso dispositivos médicos. Ante la imposibilidad de prever los avances tecnológicos que se producirán, para una defensa *a priori,* es necesario que esta no vaya tres pasos por detrás del desarrollo tecnológico.

Como se ha podido apreciar a lo largo del artículo, la ciberguerra se lleva a cabo a distintos niveles: desde los grupos no gubernamentales, que *motu proprio* lanzan

[46] GAVRILA, A. *Op. cit*.
[47] CUBEIRO CABELLO, E. «El ciberespacio en la guerra de Ucrania» (Documento de Opinión, n.º 32). IEEE, 2022. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf [consulta: 12/1/2023].
[48] Para una definición de «Internet of things», cfr. SHAFIQ, M. *et al.* (2022) «The rise of "internet of things": Review and open research issues related to detection and prevention of IOT-based security attacks», *Wireless Communications and Mobile Computing*. 2022, pp. 1-12. Disponible en: https://doi.org/10.1155/2022/8669348

estrategias para atacar a quienes son considerados enemigos, a los organismos de defensa nacionales dedicados a la ciberseguridad que contrarrestan ataques. Lo que queda claro de la situación observable en Ucrania es que la ciberdefensa, hoy en día, exige un gran nivel de coordinación entre el personal profesional gubernamental, la industria tecnológica y, en ocasiones, actores que pueden ser considerados delictivos.

A pesar de que, como se ha mencionado, la gran ciberguerra esperada tras el comienzo de la agresión rusa no haya ocurrido, no se puede esperar que esta situación se repita. El caso de la IT Army ucraniana es solo un ejemplo que invita a la reflexión sobre el futuro de la protección del ciberespacio, en tiempos de guerra o paz. Tanto a nivel nacional como en el seno de organizaciones internacionales como las Naciones Unidas y la Unión Europea, se necesitan políticas para organizar una defensa en este ámbito que prevenga y disuada futuras crisis. No faltan propuestas para buscar una solución a esta laguna jurídica internacional[49]. No obstante, es patente la dificultad en la colaboración entre Estados para proponer una legislación conjunta que se ajuste a los intereses de todos[50]. La sociedad internacional actual se encuentra más dividida que nunca por la ruptura de la hegemonía existente desde el final de la Guerra Fría. La formación de mayorías consensuadas, como exige la redacción de normas internacionales, es muy difícil de conseguir. Sin embargo, la existencia de propuestas de legislación, aunque poco desarrolladas aún, conforma un buen punto de partida para la elaboración de un futuro tratado internacional que regule el ciberespacio.

Actualmente se encuentra abierto el plazo de revisión del *Manual de Tallin 2.0;* la publicación de una tercera versión está planeada para 2026. También se encuentra en sesión el Grupo de Trabajo Abierto de las Naciones Unidas sobre la Seguridad de las Tecnologías de la Información y las Comunicaciones y su Uso, que tiene hasta 2025 para presentar a la Asamblea General sus conclusiones y estudios en la materia. Por las fechas fijadas para ambas iniciativas, parece que quedan años para poder hablar de una verdadera regulación de las actividades en el ciberespacio.

[49] ROBLES CARILLO, M. «El régimen jurídico de las operaciones en el ciberespacio: estado del debate» (Documento de Opinión, n.º 101). IEEE, 2019. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO101_2019MARROB_legalciber.pdf [consulta: 12/1/2023]

[50] *Idem.*

*María De Álvaro Mizzian**
Politóloga
Máster en Relaciones Internacionales y Diplomacia