Capítulo 1

El ciberespacio como un entorno de interacciones*

DOI: https://doi.org/10.25062/9786287602137.01

Steven Jones-Chaljub
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Citación APA: Jones-Chaljub, S. (2022). El ciberespacio como un entorno de interacciones. En Jones-Chaljub, S., *Conceptualización del ciberespacio humano* (pp. 15-29). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602137.01

Conceptualización del ciberespacio humano
ISBN impreso: 978-628-7602-14-4
ISBN digital: 978-628-7602-13-7
DOI: https://doi.org/10.25062/9786287602137

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2022

* Este libro presenta los resultados del proyecto de investigación "Fortalecimiento de las capacidades cibernéticas para Colombia" del grupo de investigación "Masa Crítica" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por Minciencias y con código de registro COL0123247. Los puntos de vista pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

El concepto de *ciberespacio* está lejos de ostentar una definición universal, y no precisamente por falta de consenso, sino porque es "algo" relativamente nuevo, que la humanidad todavía está intentando comprender en su máxima expresión, lo cual es sumamente paradójico. Lo es porque cuando se lee algo de historia es posible darse cuenta, desde una visión en retrospectiva, de que lo considerado hoy ciberespacio es una creación de nuestra especie, y muy seguramente lo seguirá siendo en los años venideros.

Los esfuerzos por definir al ciberespacio, así como muchas otras palabras que representan un reto ontológico (por ejemplo, terrorismo), se han limitado a dar significado a partir de posibles componentes o partes; no es posible saber qué es, aunque sí cómo está compuesto. Así, es común encontrar que este término es reducido, en general, al simple conjunto de redes, *hardware*, *software*, datos, infraestructura física y usuarios, como se muestra en la tabla 1. Esta aproximación es ilustrativa, pero deja la puerta abierta para ambigüedades e interpretaciones equívocas, que pueden limitar enormemente nuestra habilidad para tomar decisiones.

El presente libro, contrario a la tendencia descrita, entiende, a todos sus efectos, el ciberespacio como un entorno intangible, donde los individuos, así como las colectividades a las cuales estos pertenecen, interactúan para satisfacer diferentes intereses. Esta definición, si bien tiene un enfoque netamente antropológico, no sugiere que siempre deben estar dos o más personas sentadas en tiempo real frente a una pantalla.

Tabla 1. *Definiciones de ciberespacio en diferentes países*

	País	Fuente	Definición
1	Francia	*Seguridad y Defensa de los Sistemas de Información: Estrategia de Francia* (2011, p. 21).	Espacio de las comunicaciones creado por la interconexión mundial de equipos de procesamiento de datos digitales.
2	Rusia	*Concepto de Estrategia para la Ciberseguridad de la Federación Rusa*, p. 2.	Esfera de actividad en el interior del espacio de la información, formado por el conjunto de canales de comunicación de internet y otras redes de telecomunicaciones, la infraestructura tecnológica que garantiza su funcionamiento y cualquier forma de actividad humana en ella (individuos, organizaciones y Estados).
3	Reino Unido	*La Estrategia de Ciberseguridad del Reino Unido: Protegiendo y promoviendo el Reino Unido en un mundo digital* (2011, p. 11).	Dominio interactivo compuesto de redes digitales, y que es usado para almacenar, modificar y comunicar información. Este incluye internet, pero también, otros sistemas que información que soportan nuestros negocios, nuestra infraestructura y nuestros servicios.
4	Reino Unido	*La Estrategia de Ciberseguridad del Reino Unido: Protección, seguridad y resiliencia en el ciberespacio* (2009, p. 7).	El ciberespacio abarca todas las formas de actividades digitales en red; esto incluye el contenido y las acciones realizadas a través redes digitales.
5	Estados Unidos	*La estrategia nacional para asegurad el ciberespacio* (2003, p. 7).	El ciberespacio se compone de cientos de miles de computadores, servidores y routers interconectados, así como de switches y cables de fibra óptica, que permiten el funcionamiento de nuestra infraestructura crítica.
6	Estados Unidos	• *Diccionario de términos militares y asociados del Departamento de Defensa* (2011, p. 92). • Glosario de términos clave de la seguridad de la información del NIST (2013, p. 58). • Concepto operacional del ciberespacio y plan de capacidades del Ejército de Estados Unidos 2016-2028 (2010, p. 6).	Dominio global, dentro del ambiente de la información, y que consiste en la red interdependiente de infraestructuras de tecnologías de la información, incluyendo internet, las redes de telecomunicaciones, los sistemas de cómputo, los procesadores y los controladores integrados.

	País	Fuente	Definición
7	Alemania	• *Estrategia de Ciberseguridad de Alemania* (2011, p. 9). • Oficina Federal para la Seguridad de la Información (BSI): Glosario.	El ciberespacio es el espacio virtual de todos los sistemas de tecnologías de la información conectados en el ámbito de los datos a escala global. La base del ciberespacio es internet, como una conexión universal y accesible al público, así como una red de transporte que puede complementarse y ampliarse mediante cualquier número de redes de datos adicionales; los sistemas informáticos en un espacio virtual aislado no forman parte del ciberespacio.
8	Israel	Resolución N.º 3611: Avanzando en las capacidades nacionales en el ciberespacio (2011, p. 1).	Los dominios físicos y no físicos que son creados o compuestos por una parte de los siguientes componentes, o todos ellos: sistemas mecanizados y computarizados; computadores y redes de comunicaciones; programas; información computarizada; contenido transmitido por computadores, y los datos, su tráfico y quienes los utilizan.
9	Japón	*Estrategia de Ciberseguridad: Hacia un ciberespacio de liderazgo mundial, resiliente y vigoroso* (2013, p. 5).	Ciberespacio: espacio virtual global, como internet, compuesto de sistemas de información, redes de comunicaciones de información y sistemas similares, en los que circulan grandes cantidades de una amplia variedad de información, y el cual se ha expandido rápidamente y ha comenzado a permear el mundo real.
10	Japón	Estrategia Nacional de Seguridad (2013, p. 9).	Ciberespacio: un dominio global compuesto de sistemas de información, redes de telecomunicaciones y otros; proporciona los cimientos para actividades sociales, económicas y militares, entre otras.
11	España	Estrategia Nacional de Ciberseguridad (2013, p. 9).	Ciberespacio es el nombre que designa el dominio global y dinámico compuesto por las infraestructuras de tecnología de la información —incluido internet—, las redes y los sistemas de información y de telecomunicaciones.
12	Bélgica	Estrategia Nacional de Ciberseguridad, (2012, p. 12).	El ciberespacio es el ambiente global para la interconexión de sistemas de información y comunicaciones.
13	Canadá	*Estrategia de Ciberseguridad para una más fuerte y prospera Canadá* (2010, p. 2).	El ciberespacio es un mundo electrónico creado por redes interconectadas de tecnología de la información, y la información de esas redes.

	País	Fuente	Definición
14	República Checa	Borrador de acto legislativo sobre ciberseguridad (2014, p. 2).	El ciberespacio significa un ambiente digital, facilitador en la creación, el procesamiento y el intercambio de información, y creado por sistemas de información y servicios y redes de comunicación electrónica.
15	Hungría	Anexo N.° 1 de la decisión gubernamental N.° 1139/2013 frente a la estrategia nacional de ciberseguridad de Hungría, 2013, p. 3.	Ciberespacio significa el fenómeno combinado de sistemas descentralizados y crecientes de información electrónica, así como los procesos sociales y económicos que aparecen en y a través de dichos sistemas, en la forma de datos e información.
16	Italia	*Marco estratégico nacional para la seguridad del ciberespacio* (2013, p. 9).	El ciberespacio es un dominio construido por el hombre, y compuesto, esencialmente, de nodos de TIC, redes, *hosting* y procesamiento, y con una riqueza siempre creciente de datos de importancia estratégica para los Estados, las firmas, y los ciudadanos por igual, así como para todos los tomadores de decisiones políticas, sociales y económicas.
17	Montenegro	*Estrategia nacional de ciberseguridad para Montenegro 2013-2017* (2013, p. 5).	El ciberespacio es más que internet: incluye no solo el *hardware*, el *software* y los sistemas de información, sino también, las personas y las interacciones sociales dentro de estas redes.
18	Holanda	*La estrategia de ciberdefensa* (2012, p. 4).	El ciberespacio es entendido como útil para cubrir todos los entes que están o podrían estar conectados digitalmente. El dominio incluye conexiones permanentes, así como temporales y locales, y en todos los casos está relacionado, de alguna manera, con los datos presentes en este (códigos fuente, información etc.).
19	Rumania	Decisión N.º 271 para la aprobación de la estrategia de seguridad cibernética rumana y plan de acción nacional sobre la aplicación de la ciberseguridad nacional (2013, p. 7).	El ciberespacio es el ambiente virtual generado por la infraestructura cibernética, incluyendo la información procesada, almacenada o transmitida, y las acciones desarrolladas por los usuarios en su interior.
20	Turquía	*Estrategia nacional de ciberseguridad y plan de acción 2013-2014* (2013, p. 8).	El ciberespacio es el ambiente consistente en sistemas de información que se expanden en el mundo entero, incluyendo las redes que los interconectan.

	País	Fuente	Definición
21	India	Política Nacional de ciberseguridad (NCSP-2013) (2013, p. 1).	El ciberespacio es un ambiente complejo que consiste de interacciones entre personas, *software* y servicios, soportados por sistemas tecnológicos mundiales de distribución de información y comunicaciones, así como de redes.
22	Nueva Zelanda	Estrategia de ciberseguridad de Nueva Zelanda (2011, p. 12).	El ciberespacio es la red global de infraestructuras interdependientes de las tecnologías de la información, las redes de telecomunicaciones y los sistemas de procesamiento informático, y en la que tiene lugar la comunicación en línea.
23	Sudáfrica	"Aviso de intención" para realizar la estrategia nacional sudafricana de ciberseguridad (2010, p. 12).	El ciberespacio es el terreno físico y no físico creado y compuesto por algunos o de los siguientes elementos, o todos ellos: computadores, sistemas de cómputo, redes, programas, datos y su tráfico, y los usuarios.
24	Colombia	CONPES 3701/11: "(Resolución CRC 2258 de 2009)".	El ciberespacio es el ambiente, tanto físico como virtual, compuesto por computadores y por sistemas computacionales, programas computacionales (*software*), redes de telecomunicaciones, datos e información, y que es utilizado para la interacción entre usuarios.

Fuente: traducción no oficial del autor, a partir de Maurer y Morgus (2014).

Las interacciones del ciberespacio se dan cuando uno o varios usuarios o sistemas responden recíprocamente a estímulos provenientes de otros usuarios o sistemas, y generan así una dinámica continua de acción-reacción, que no necesariamente es instantánea. La razón por la cual se incluyen los sistemas responde a la calidad intangible del ciberespacio; es decir, a la habilidad de este para existir por fuera del mundo material gracias a una serie de elementos tecnológicos interconectados.

Los elementos tecnológicos que albergan al ciberespacio tienen la facultad de ser programados para que, según las indicaciones y las motivaciones de sus dueños, realicen ciertos estímulos y reacciones. Así, mientras no exista una efectiva inteligencia artificial que nos reemplace, los sistemas están concebidos para ser fieles representantes de los usuarios, y ello hace posible una interacción que, podría decirse, es *despersonificada*. Por esta razón, cuando se habla

de *usuario*, y a menos que se exprese lo contrario, el presente libro siempre se estará refiriendo a un ser humano.

Frente a la pregunta de por qué se generan las interacciones, la definición dada indica que es para la satisfacción de *intereses*. Estos son cualquier cosa que represente valor para un individuo o una colectividad, independientemente de que respondan o no a una lógica racional.[1] En ese sentido, no existe interacción sin interés de por medio. Es sumamente difícil imaginar el empleo del ciberespacio por el mero acto de hacerlo: incluso el ocio tiene una razón de ser. De esa forma, los estímulos y las respuestas, incluyendo las programadas en los sistemas, se vuelven una manifestación del deseo del usuario de hacer o tener lo que considera importante. Esto es igualmente válido tanto para interacciones cotidianas (por ejemplo, realizar una compra electrónica) como para aquellas sumamente complejas (por ejemplo, vulnerar la seguridad o sistema de centrifugado de una planta nuclear).

Cuando abrimos el explorador para ingresar el dominio de nuestra página de *e-commerce* favorita,[2] con el interés de adquirir un producto particular, estamos desencadenando una serie de estímulos (acciones) y respuestas (reacciones) que muchas veces desconocemos. La primera reacción es el enrutamiento de los servidores, que nos permite acceder al contenido deseado. Una vez allí, se nos exige autenticar la identidad (estímulo) para abrir el carrito de compras donde se generará el pago (respuesta). Dicho encadenamiento continuará dentro del sistema de la empresa vendedora y el operador bancario, hasta que el cliente reciba, en algún momento, su producto o el dinero pagado.

Similar al ejemplo de la compra electrónica, la vulneración de la planta nuclear iraní, en 2009, responde a la misma dinámica de las interacciones. Quien haya ordenado introducir la USB en los computadores iraníes para propagar a *Stuxnet* tenía un interés claro: entorpecer el programa nuclear de ese país. El *gusano*[3] aprovechó vulnerabilidades desconocidas por los administradores del sistema (*zero-day exploit*)[4] para introducir una carga dañina (*payload*)[5] que alterara los ciclos en las centrífugas de enriquecimiento de material radioactivo. En ese

1 La lógica racional establece que los individuos toman decisiones ponderando diferentes tipos de información, buscando maximizar los beneficios frente a los costos.

2 Transacciones comerciales realizadas a través de internet.

3 Tipo de *malware* que se propaga o se replica por sí mismo en y entre computadores.

4 Un *zero-day exploit* son defectos o vulnerabilidades que existen en un *software* y son desconocidas para los fabricantes.

5 El *payload* son las líneas de código de un *malware* destinado a comportamiento dañino.

sentido, la carga se transforma en el estímulo, y el comportamiento del sistema de control (SCADA), en la respuesta recíproca esperada. Se especula que *Stuxnet* fue exitoso, pero había la posibilidad de que hubiese fracasado, como muchos otros *malwares* lo hacen a diario (Falliere et al., 2011; Lendvay, 2016; Mueller & Yadegari, 2012).[6]

Entablar interacciones en el ciberespacio —y por ende, recibir respuestas a los estímulos— no implica que el otro reaccione siempre como requerimos o deseamos. Las razones pueden ser múltiples: desde errores involuntarios que entorpecen la interacción (por ejemplo, un servidor caído) hasta un deseo consciente de bloqueo. Adicionalmente, y suponiendo que se logren, las respuestas recíprocas esperadas, bien fuere persona o un sistema, no necesariamente conllevan la generación de beneficio mutuo. Si eso es cierto, las interacciones tienen una naturaleza dual: son distributivas e integrativas.

Las interacciones en el ciberespacio donde las partes involucradas no vean sus intereses satisfechos, y ello sea consecuencia de un comportamiento premeditado para generar resistencia, se consideran distributivas. La distribución ocurre cuando las ganancias de una parte implican, necesariamente, pérdidas proporcionales o mayores para otras. En el momento en que una interacción distributiva no permita llegar a una conciliación, entendida tal situación como el punto donde ninguna de las partes quiera ceder en sus intereses, los estímulos y las reacciones se reducen a una mecánica de imposición, protección y defensa. Esto se puede apreciar fácilmente cuando se entra en materia de ciberseguridad y ciberdefensa.

Imagine nuevamente a la persona que realiza la compra en la plataforma de *e-commerce*: esta se encuentra convencida de que si hace las interacciones necesarias podrá recibir al final el producto deseado. Ahora bien, ¿qué sucedería si el dominio ha sido víctima de *pharming*,[7] y el comprador, quien cree que está realizando un procedimiento habitual, ingresa su información bancaria, y se vuelve, en cambio, objeto de un fraude? En este caso, no solo la interacción fracasó para el comprador, pues no satisfizo su interés, sino que resultó perjudicial; sin embargo, para quien orquestó la estafa, la historia es de completo éxito. Si se le pudiese preguntar a la víctima sobre la proporción en que estaría dispuesta a

6 El término *malware* es un acrónimo de *malicious software*. Es un término genérico para referirse a todo *software* que pretenda generar algún tipo de daño o perturbación a los sistemas de cómputo (por ejemplo, virus, gusanos, troyanos, *backdoors*, *spyware* y *adware*, entre otros).

7 El *pharming* es un tipo de ataque cibernético que busca redirigir el tráfico de una página legítima a una falsa que ostenta la misma apariencia.

ser robada, muy seguramente diría que ninguna; es más: si fuera consciente del riesgo, tomaría medidas para evitarlo. Lo mismo ocurrió en el caso de *Stuxnet*.

Stuxnet se diseñó para afectar el tipo de órdenes que el SCADA iraní daba,[8] y no para minar la capacidad de este para controlar la infraestructura nuclear; es más, el *malware* dependía para su funcionamiento de que el sistema de control hiciera correctamente el trabajo para el cual fue diseñado. Eso, en los términos aquí descritos, es causar que las estimulaciones del SCADA recibieran las respuestas recíprocas esperadas por parte de las centrífugas. El logro de dicha interacción significó, debido al cambio en la configuración por parte del gusano, un golpe a los intereses iraníes, así como una victoria para su contraparte.

Los creadores de *Stuxnet*, al igual que sucede con los de otros arsenales cibernéticos (por ejemplo, Duqu, Flame, Gauss, y los incluidos Vault 7), pronosticaron un nivel de resistencia por parte de su objetivo, lo cual los obligó a asumir un diseño particular para evitar una eventual detección: por ejemplo, usar *rootkits* y manipular la librería s7otbxdx.dll del SCADA.[9] El hecho de que se hayan tomado el tiempo para adquirir acceso, sin autorización y evitando detección, demuestra un claro deseo de imposición. Ahora bien, frente a si los iraníes esperaban defender sus intereses, las dinámicas de política internacional para ese momento por parte del gobierno de Ahmadinejad sugieren un rotundo sí.

En contraposición a las interacciones distributivas, en las de carácter integrativo se generan ganancias mutuas para las partes involucradas. En tales casos, al verse satisfechos los intereses de todos, ni los estímulos ni las respuestas asumen una postura de competencia, sino una de cooperación; la decisión dependerá de la percepción que cada usuario posea de los demás y su de entorno. Las dinámicas integrativas en el ciberespacio son comunes en materia de ciberseguridad y ciberdefensa. Quienes tratan de imponerse o de defenderse terminan uniéndose para facilitar la coordinación y el logro de objetivos comunes de múltiples clases; incluso, aquellos ilegales para los ordenamientos jurídicos.

Cuando se habla de pérdidas y ganancias, inevitablemente se termina ingresando en el campo subjetivo, donde el usuario hace una ponderación del efecto que una interacción generó en sus intereses. En el ciberespacio, los efectos

[8] El término SCADA es el acrónimo de *Supervisory Control and Data Acquisition*; los cuales son sistemas de control y supervisión de diferentes procesos y maquinaría de tipo industrial.

[9] *Software* diseñado para generar acceso como administrador, sin autorización ni detección, a un computador. Puede ser utilizado para controlar remotamente un dispositivo. Este oculta su presencia en el PC; usualmente, dentro de alguna de las capas inferiores del sistema operativo. "Avast, what is a rootkit". https://www.avast.com/c-rootkit

pueden ser clasificados como *directos* e *indirectos*. Son directos los que resultan como consecuencia inmediata de una interacción, lo cual refleja claramente un objetivo y una intención. Los indirectos, por otro lado, son todas las afectaciones colaterales de un efecto directo (Balcells, 2011; Mann & Endersby, 2002).

En septiembre de 2007, las FF. MM. israelíes llevaron a cabo la Operación Orchard, la cual tenía como objetivo la destrucción de un supuesto reactor nuclear en territorio sirio. Los israelíes —y aquí todavía se debate si dicha acción realmente pertenece al campo cibernético o solo al electrónico— alteraron la imagen percibida por los radares de su contraparte árabe, y así neutralizaron por completo la capacidad de estos para detectar objetos extraños en el cielo. Acto seguido, un escuadrón de aviones de combate con la estrella de David como insignia bombardeó, sin ninguna oposición, el complejo, para luego volver rápidamente, sanos y salvos, a su lugar de origen. La falta de reacción del gobierno de Assad no se debió a la ausencia de poder militar, sino, simplemente, a la amenaza: nunca se la vio llegar ni partir (Follath & Stark, 2009; Singer, 2013, pp. 126-133).

El efecto directo de la interacción entre los israelíes y los sistemas sirios fue la afectación de la autenticidad de la información recibida y presentada por los radares, lo cual formó una ventana de oportunidad que fue aprovechada para el bombardeo. Los efectos indirectos, seguramente, fueron múltiples (por ejemplo, pérdidas económicas y políticas, retrasos logísticos, etc.), pero la mayoría son desconocidas para la opinión pública, salvo el maremágnum diplomático que terminó con una serie de visitas del Organismo Internacional de Energía Atómica (OIEA). Aunque en 2009 el OIEA confirmó que la infraestructura sí era un reactor nuclear, lo cual contradecía abiertamente las declaraciones del gobierno sirio, las sanciones nunca llegaron; muy seguramente, porque un debate sobre la violación a la soberanía en una región tan volátil generaría problemas mayores (Heinrich, 2009).

No hay nada más erróneo que otorgarles mayor preponderancia a los efectos indirectos, al punto de establecerlos como los verdaderos logros. La manera como estos se desarrollan es completamente inesperada, por más que puedan llegar a visualizarse. Por ejemplo, es posible afirmar que una sociedad altamente dependiente de la tecnología sufrirá disrupciones si se vulnera el sistema bancario, pero contar con que ello cause una destitución inmediata del gobierno es un acto netamente especulativo.

Controlar el comportamiento de los efectos es igualmente difícil para los de carácter directo; en particular, por las interconexiones existentes entre las

distintas redes que hacen parte del ciberespacio. Cuando *Stuxnet* se utilizó, su propósito no era, hasta donde se sabe, propagarse salvajemente a escala mundial; sin embargo, este terminó infectando controladores industriales y computadores en diferentes partes del mundo, y eso llevó a empresas como Norton a crear indicaciones especiales frente al *malware* (Falliere et al., 2011). El hecho de que no se causaran mayores estragos se debió, muy posiblemente, al diseño de la carga maliciosa, pero no siempre se tendrá el mismo final.

Para la fecha de redacción de este libro, uno de los debates más difíciles que se dan en la comunidad internacional es la aplicación del Derecho Internacional Humanitario (DIH), tanto convenciones de Ginebra como protocolos complementarios, dentro del marco de los conflictos cibernéticos. El objetivo es procurar que se mantengan los distintos principios del DIH; particularmente, la proporcionalidad y la distinción, tanto si se trata se trata de un nuevo entorno como si no. La dificultad se exacerba debido a la falta de leyes y jurisprudencia específicas; lo más cercano es el *Manual de Tallin*, y este no tiene naturaleza vinculante. Las preocupaciones en la materia son bien fundamentadas; una interacción puede causar una cascada de efectos indirectos que, fácilmente, al salirse de control, generarían estragos indeseados e ilegítimos en múltiples niveles.

La Operación Orchard tiene una lección adicional para entender las interacciones en el ciberespacio: no todos los intereses se logran empleando únicamente dicho entorno. Tal como sucedió, el ejército israelí utilizó al entorno cibernético para facilitar un bombardeo, y este último fue considerado el modo idóneo para destruir la infraestructura nuclear de Siria. A esta forma de proceder el presente libro la ha denominado una *interacción extraciberespacial*.

Las interacciones extraciberespaciales son las que, a partir de estímulos y respuestas en el ciberespacio, buscan complementar a otros medios y modos del "mundo físico" considerados por los usuarios como más propensos a satisfacer sus intereses finales. Estas interacciones se oponen a las *intraciberespaciales*, que, a su vez, constituyen todos los esfuerzos que se manifiestan solamente en el interior del entorno intangible, y que, sin ningún acompañamiento externo, pueden cumplir las aspiraciones de los usuarios. El caso de estudio de *Stuxnet* y los eventos ocurridos en Estonia y Georgia entre 2007 y 2008, así como la mayoría de los incidentes de espionaje documentados (por ejemplo, Sony, Play Station, Boeing), pueden ser fácilmente categorizados como interacciones de este último tipo.

En el argot militar existen diferentes conceptos que son utilizados para referirse a las interacciones intraciberespaciales, según el tipo de efecto directo que se pretenda causar con ellas y, por ende, según el interés por cumplir. Los más comunes son: explotar, interrumpir, destruir, manipular, degradar, engañar, responder, influenciar, proteger, detectar y restaurar, como se muestra en la tabla 2; no obstante, estos también son válidos para actores que no encajen en la naturaleza militar.

Tabla 2. *Definiciones de argot militar en el ciberespacio*

Concepto	Definición
Destruir	Dañar un sistema o una entidad hasta el punto de que ya no puede funcionar ni ser restaurado a una condición útil sin que se lo reconstruya por completo.
Interrumpir	Romper temporalmente el flujo de la información.
Degradar	Reducir la efectividad o la eficiencia de los sistemas del adversario y sus capacidades de recolección de información; también se puede degradar la moral de una unidad o reducir el valor del blanco o la calidad de las decisiones y las acciones del adversario.
Negar	Impedir al adversario acceder y utilizar información, sistemas y servicios críticos.
Engañar	Lograr que una persona crea algo falso; buscar engañar a los adversarios manipulando su percepción de la realidad.
Explotar	Lograr acceso a los sistemas del adversario para recolectar información, o sembrar información falsa o decepcionante.
Influenciar	Hacer que otros se comporten de una manera favorable a intereses ajenos a los suyos propios.
Proteger	Tomar acciones para prevenir el espionaje o la captura de equipos e información sensibles.

Concepto	Definición
Detectar	Descubrir una invasión en los sistemas de información.
Restaurar	Reponer a su estado original la información y los sistemas de información.
Responder	Reaccionar rápidamente a los ataques o las invasiones del adversario.

Fuente: Golinger (2011, pp. 89-94).

Al principio de este capítulo se dijo que los *usuarios* en el ciberespacio son *seres humanos*, y esa afirmación se mantiene. Ahora bien, se ha mencionado, así mismo, que los individuos hacen parte de colectividades, lo cual lleva, indiscutiblemente, a preguntarse por la posibilidad de que estas asuman el rol de usuarios en el ciberespacio. De manera anticipada, ya que esto será profundizado posteriormente, se debe afirmar que las colectividades sí son usuarios de dicho entorno, pero sus interacciones no son consideradas únicas y coordinadas.

Clásicamente, los Estados son asumidos, dentro del marco de las políticas públicas y la seguridad, y tanto en el sector académico como fuera de este, como el principal actor. En el ciberespacio es por completo diferente: allí se vive una desestatalización de las colectividades. No debería ser para menos. Operar en ese entorno es relativamente costo-eficiente; solo es necesario contar con conocimiento y acceso para ser considerado, por así decirlo, digno de importancia. Por tal razón, el espectro de actores es bastante amplio: los Estados con sus instituciones, incluyendo la Fuerza Pública; grupos terroristas e insurgentes; crimen organizado transnacional; organizaciones internacionales; empresas privadas; *hacktivistas*; *script noobs* o *kiddies*, y las personas en general, claro está.

Las colectividades no estatales han demostrado ser capaces de realizar interacciones intraciberespaciales similares a las ya enunciadas (i.e. explotar, interrumpir, destruir, etc.) para satisfacer intereses muy diferentes de los de carácter nacional. Una clara muestra es *Anonymous*. Este grupo **hacktivista**, considerado uno de los más prolíferos hasta el momento, ostenta una considerable reputación que pocos gobiernos se atreven a menospreciar. Sus incidentes cibernéticos exitosos, autodenominados operaciones u ocupaciones (por ejemplo, *chanology, payback, avenge Assange, bradical, anti-security, WTO hack, darknet*

relauch), han sido muestra de su capacidad para imponerse sobre otros que ostentan mayores recursos.[10]

Una vez cubierta toda la temática de las interacciones en el ciberespacio y puestos sobre la mesa los diferentes tipos de colectividades, queda una pregunta por responder: ¿cómo logran estas, en su diversidad, imponer sus intereses a partir de interacciones intra y extraciberespaciales, así como distributivas e integrativas? La respuesta es: *a través de la proyección de poder*.

Lecciones

- El ciberespacio es un entorno intangible compuesto por distintos elementos (i.e. *software*, *hardware*, datos, infraestructura física e individuos), de los cuales el factor humano es el más complejo y el menos estudiado.
- Los individuos, así como las colectividades a las cuales estos pertenecen, interactúan en el ciberespacio para satisfacer distintos intereses. Estos son cualquier cosa que tenga valor para el usuario, independientemente de que obedezcan o no a una lógica racional.
- Las interacciones del ciberespacio se dan cuando uno o varios usuarios o sistemas responden recíprocamente a estímulos provenientes de otros usuarios o sistemas, y generan así una dinámica continúa de acción-reacción.
- Los sistemas de información son, mientras no exista una efectiva inteligencia artificial, fieles representantes de la voluntad y los intereses de sus dueños, que los hacen válidos como "parte" para interactuar.
- Los estímulos de las interacciones no siempre tendrán la respuesta recíproca esperada o deseada por el usuario que los causa. Esto puede deberse a múltiples razones; entre ellas, un deseo premeditado de bloqueo. Así, las interacciones en el ciberespacio pueden ser *distributivas* o *integrativas*.
- Las interacciones distributivas implican que las ganancias de una parte, entendidas como la satisfacción de los intereses de esta, causan

[10] Ver https://iamanonymous.com/, para acceder al histograma completo de las operaciones de Anonymous.

pérdidas proporcionales o mayores para las demás. En caso de no conciliación, y de mantenerse el ímpetu, las interacciones terminan desencadenando una dinámica de competencia que se caracteriza por esfuerzos de imposición, protección y defensa. Esto es común en el contexto de la ciberseguridad y la ciberdefensa.

- Las interacciones integrativas, por su parte, ocurren cuando ambas partes ven satisfechos sus intereses, lo cual motiva esfuerzos de cooperación; la decisión dependerá de la ponderación que las partes hagan de los demás y de su entorno. La cooperación puede darse, paradójicamente, entre los esfuerzos de imposición, protección y defensa.
- Hablar de beneficios y pérdidas exige entender los efectos que una interacción tiene sobre los intereses de los usuarios. Los efectos en el ciberespacio pueden ser *directos* o *indirectos*. Los primeros son todos los que se produzcan como consecuencia inmediata del emparejamiento entre estímulo y respuesta que refleje claramente un objetivo y una intención. Los segundos, por otro lado, son todas las afectaciones colaterales que puedan desencadenarse tras un efecto directo.
- No todos los intereses de los usuarios se satisfacen empleando únicamente el ciberespacio. Por ello también se habla de *interacciones extra* e *interciberespaciales*. Las extraciberespaciales son las que, a partir de estímulos y respuestas en el ciberespacio, buscan complementar a otros medios y modos del "mundo físico" considerados por los usuarios como más propensos a satisfacer sus intereses finales. Estas interacciones se oponen a las intraciberespaciales, que constituyen todos los esfuerzos que se manifiestan solo en el interior del entorno intangible, y que, sin ningún acompañamiento externo, pueden cumplir las aspiraciones de los usuarios.
- Las interacciones inter y extraciberespaciales no son excluyentes de las distributivas o integrativas, sino complementarias de ellas.
- Si bien los Estados se mantienen como actores importantes en el ciberespacio, también existe una pluralidad de colectividades con múltiples naturalezas, intereses y motivaciones. Estos deben ser, por la evidencia disponible de sus interacciones y sus capacidades, tomados muy en serio.

Referencias

Ackerman, S. (2015). US Central Command Twitter account hacked to read 'I love you Isis'. *The Guardian*.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. I*nternational Journal of Drug Policy, 35*, 7-15. https://doi.org/10.1016/j.drugpo.2016.04.020

Assaf, A., & Moshnikov, D. (2020). Contesting sovereignty in cyberspace. *Int. Cybersecur. Law Review. 1*, 115-124.

Associated Press, & AFP. (2015). *Bar manager gets more than TWO YEARS hard labour in Myanmar for putting headphones on Buddha in online drinks ad*. https://tinyurl.com/bde9ew88

Ayers, C. E. (2016). *Rethinking sovereignty in the context of cyberspace*. Center for Strategic Leadership, United States Army War College. https://www.hsdl.org/?view&did=802916

Bachrach, P., & Baratz, M. S. (1962). Two faces of power. *The American Political Science Review, 56*(4), 947-952.

Bakken, D. E., Rarameswaran, R., Blough, D. M., Franz, A. A., & Palmer, T. J. (2004). Data obfuscation: anonymity and desensitization of usable data sets. *IEEE Security and Privacy, 2*(6), 34-41.

Balcells, L. (2011). Continuation of politics by two means: Direct and indirect violence in civil war. *The Journal of Conflict Resolution, 55*(3), 397-422. http://www.jstor.org/stable/23049892

Barlow, J. P. (2009). Declaración de independencia del ciberespacio (1996). *Periférica Internacional. Revista Para el Análisis de la Cultura y el Territorio, 1*(10), 241-242.

Beevor, A. (2009). *D-Day: The battle for Normandy*. Viking.

BBC News. (2017). Two Britons arrested in Thailand over football streaming. https://www.bbc.com/news/technology-39947622.

Bergman, M. (2001). *The Deep Web: Surfacing hidden value*. Bright Planet: Deep Content.

Blocked on Weibo. (s.f.). https://blockedonweibo.tumblr.com/tagged/list.

Bonaparte, N. (2018). *Napoleon the art of war & power: Slip-cased edition*. Arcturus Publishing Ltd. (Obra original sin fecha conocida).

Brainard, L. A. (2010) Cyber-communities. En H. K. Anheier, S. Toepler (Eds.), *International Encyclopedia of Civil Society*. Springer. https://doi.org/10.1007/978-0-387-93996-4_43

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology (1973), 97*(2), 379-475.

Brock, J. L. (2000). *Critical infrastructure protection "ILOVEYOU": Computer Virus Highlights Need for Improved Alert and Coordination Capabilities (GAO/T-AIMD-00-181*. United States General Accounting Office.

Bronk, C., Monk, C., & Villaseñor, J. (2012). The dark side of cyber finance survival. *Journal Survival Global Politics and Strategy 54*(2), 129-142. doi:10.1080/00396338.2012.672794

Burgess, M. (2016). *Chinese hacker jailed after stealing 'cutting-edge' military secrets*. https://www.wired.co.uk/article/chinese-hack-us-military-su-bin

Buzan, B. (1983). *People, states, and fear: The national security problem in international relations*. Wheatsheaf Books Ltd.

Clemente, D. (2011). International security: Cyber security as a wicked problem. *The World Today, 67*(10), 15-17.

Command, U. A. T. a. D. (2005). *Cyber operations and cyber terrorism*. Handbook No. 1.02. Leavenworth, KS.

Corbin, C. (2017). Pro-ISIS hackers release 'kill list' with 8,786 targets in US and UK. *Fox News*.

Dahl, R. A. (1957). The concept of power. *Behavioral Science, 2*(3), 201-215. doi:10.1002/bs.3830020303

Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2017). Battlefield cyberspace: Exploitation of hyperconnectivity and internet of things. En M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.), *Developing next-generation countermeasures for homeland security threat prevention* (pp. 204-235). IGI Global. http://doi:10.4018/978-1-5225-0703-1.ch010

Dittus, M., Wright, J., & Graham, M. (2018). Platform criminalism: The 'Last-Mile' geography of the darknet market supply chain. Paper presented at the *Proceedings of the 2018 World Wide Web Conference*. Lyon, France.

Douhet, G. (2013). *Command of the air*. Books Express Publishing. (Obra original publicada en fecha desconocida).

Dowding, K. (2006). Three-dimensional power: A discussion of Steven Lukes' power: A Radical View. *Political Studies Review, 4*.

Economy, E. (2018). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*.

El Tiempo. (2008). Informe de Interpol sobre computador de 'Raúl Reyes' calentó la cumbre de Lima. https://tinyurl.com/ynsnkhk2

Facebook. (2015). *Declaración de derechos y responsabilidades* [video]. https://tinyurl.com/2p95jzc2

Facebook. (s.f.). *Principios de Facebook*. https://www.facebook.com/principles.php.

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32. Stuxnet Dossier*. Symantec Security Response.

Fuerzas Militares de Colombia. (1997). *Manual de estrategia*. Bogotá.

Foch, M. (2007). *The principles of war*. Kessinger Publishing, LLC. (Obra original publicada en 1903).

Follath, E., & Stark, H. (2009). *The story of 'Operation Orchard': How Israel destroyed Syria's Al Kibar nuclear reactor*. https://tinyurl.com/35axjzkh

Foucault, M. (1982). The subject and power. *Critical Inquiry, 8*(4), 777-795.

Fox, N., & Roberts, C. (1999). Gps in Cyberspace: The Sociology of a 'Virtual Community.' *The Sociological Review, 47*(4), 643–671. https://doi.org/10.1111/1467-954X.00190

Fuller, J. (1926). *The foundations of the science of war*. Hutchinson & CO.

Gady, F.-S. (2015). *New Snowden documents reveal Chinese behind F-35 Hack*. https://tinyurl.com/mpp2k4sk

Galaxy 3. (s.f.). *Terms*. http://galaxy3m2mn5iqtn.onion/terms

Gaventa, J. (1980). *Power and powerlessness*. University of Illinois Press.

Gilman, N., Goldhammer, J., & Weber, S. (2013). Deviant globalization. En M. Miklaucic & J. Brewer (Eds.), *Convergence: Illicit networks and national security in the age of globalization* (pp. 3-15). National Defense University Press.

Golinger, E. (2011). La guerra cibernética. En N. D. Ferreyra, *Periodistas sin miedo 1* (pp. 89-94). https://tinyurl.com/yw23mstn

Google. (2017). *Condiciones de servicio de Google*. https://policies.google.com/terms?hl=es.

Handel, M. (1991). *Sun Tzu and Clausewitz: The art of war and on war compared*. Strategic Studies Institute U.S. Army War College.

Hanzhang, T. (2000). *Sun Tzu art of war: The modern Chinese interpretation*. Sterling Publishing Co., Inc.

Heinrich, M. (2009). *IAEA finds graphite, further uranium at Syria site*. https://tinyurl.com/47hx8br4

Hua, J., & Bapna, S. (2015). Industrial cyber espionage. *Journal of Management Systems, 25*(3), 67-18.

Huffingtonpost. (2011). Operation Delego: Dreamboard child sex ring bust nets 72 arrests in U.S., Canada, France, Germany. *The Huffingtonpost Canada*.

Jomini, A.-H. (2008). *The art of war*. Wilder Publications. (Obra original publicada en fecha desconocida).

Lee, J. (2013). Cyber kleptomaniacs: Why China steals our secrets. *World Affairs, 176*(3), 73-79.

Lendvay, R. L. (2016). *Shadows of stuxnet: Recommendations for U.S. Policy on critical infrastructure cyber defense derived from the stuxnet attack*. Naval Postgraduate School.

Lewis, J. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic and International Studies.

Liaropoulos, A. (2013). Exercising state sovereignty in cyberspace: An international cyber-order under construction? *Journal of Information Warfare, 12*(2), 19-26.

Lolifox. (s.f.). *Rules*. http://lisach7joohmqk3a.onion/.

Lukes, S. (2005). *Power: A radical view* (2nd Edition). Palgrave MacMillan.

Mager-Hois, E. A. (2010). Ideología y poder. *Revista Multidisciplina, 5*(1), 46-60.

Mahan, A. (2018). *The influence of sea power upon history, 1660-1783* (Classic Reprint). Forgotten Books. (Obra original publicada en fecha desconocida).

Mann, E., & Endersby, G. (2002). *Thinking effects effects-based methodology for joint operations. Cadre paper n.°15: College of Aerospace Doctrine, Research and Education*. Air University

Maurer, T., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*. https://tinyurl.com/3seuwwyf

Mcdonald, T., & Mills, R. (2010). *An application of deception in cyberspace: Operating system obfuscation*. Paper presented at the International Conference on Information Warfare and Security At: Dayton OH

Miyamoto, M. ([2014], s.f.). *El libro de los cinco anillos*. Santiago de Chile: EDAF. (Obra original publicada en fecha desconocida)

Moscaritolo, A. (2010). *Analysts pick apart "huge" Mariposa botnet*. Itnews.com.au.

Mueller, P., & Yadegari, B. (2012). *The stuxnet worm*. University of Arizona.

National Cybersecurity and Communications Integration Center (NCCIC). (2014). *Combating the insider threat*. Department of Homeland Security.

NortonLifeLock. (2017). *What is the difference between black, white and grey hat hackers?* Norton. https://tinyurl.com/bdd59mkv

NSPCC. (s.f.). *Grooming: What it is, signs and how to protect children*. https://tinyurl.com/32x7npma

Ogun, M. N. (2015). *Terrorist use of cyberspace and cyber terrorism: New challenges and responses* (Vol.42). Delft University Press.

Panda Security. (2013). *Los virus más famosos de la historia: ILoveYou*. https://tinyurl.com/yc58mpph

Paquet-Clouston, M., Décary-Hétu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy, 54*, 87-98. https://doi.org/10.1016/j.drugpo.2018.01.003

Parks, R., & Duggan, D. (2011). Principles of cyberwarfare. *IEEE Security and Privacy Magazine, 9*(5), 30-35.

Pricewaterhouse Coopers. (2018). *The scale and impact of industrial espionage and theft of trade secrets through cyber*. European Comission. https://tinyurl.com/yc4c3kwv

Pérez, B., Musolesi, M., & Stringhini, G. (2018), *You are your metadata: Identification and obfuscation of social media users using metadata information*. Paper presented at the Twelfth International AAAI Conference on Web and Social Media.

Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power*. The MIT Press.

Rabinovich, A. (2005). *The Yom Kippur war: The epic encounter that transformed the Middle East United States*. Schocken.

Revista Semana. (2008). "Los archivos de los computadores de 'Raúl Reyes' no han sido manipulados": Interpol. https://tinyurl.com/2uuxxsj2

Richard, L. C. (1984). *Conflict and violence in Singapore and Malaysia 1945-1983*. G. Brash.

Sadan, E. (1997). *Empowerment and community planning: Theory and practice of people-focused social solution*. Hakibbutz Hameuchad Publishers.

Schneider, F., & Williams, C. C. (2013). *The shadow economy*. Institute of Economic Affairs (IEA).

Sevnet. (s.f.). *Terms of service*. http://servnetshsztndci.onion/terms-of-service.

Shamsi, A., Zeadally, S., Sheikh1.F, & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications. *Security Comm. Networks*, 9:2886-2900. doi: 10.1002/sec.1485

Shimomura, T. (1996). *Takedown: The pursuit and capture of Kevin Mitnick, America's Most wanted computer outlaw - By the man who did it*. Voice. First edition.

Singer, P. A. (2013). *Cybersecurity and cyberwar: what everyone need to know*. Oxford University Press.

Siyuan, C., & Chen-Wei, C. (2019). *Singapore's latest efforts at regulating online hate Speech: a perspective from international law and international practices*. Research Collection School of Law, Singapore Management University. https://ink.library.smu.edu.sg/sol_research/2921

Soghoian, C. (2012). Surveillance and security lessons from the petraeus scandal. *ACLU. ORG*. https://tinyurl.com/257tm5tr

Springer, P. (2015). *Cyber warfare: A reference handbook*. ABC-CLIO, LLC.

Strenski, I. (1998). Religion, power, and final Foucault. J*ournal of the American Academy of Religion, 66*(2), 345-367.

Sun Tzu. (1963). *The art of war*, S. B. Griffith (Ed.). Oxford University Press. (Obra original publicada en fecha desconocida).

The Independent (2014). Why Filipinos have become the punching bag. https://tinyurl.com/2p84uwc2

The Statutes of the Republic of Singapore. (2013). *Sedition Act* (Chapter 275). https://sso.agc.gov.sg/Act/SA1948?ProvIds=pr1-#pr1-

UK Ministry of Defense. (2014). *Joint doctrine publication 0-01 (JDP 0-01)*. (5 ed.). Forms and Publications Section.

US Army. (1984). *The soviet army: Operations and tactics (FM 100-2-1)*. Headquarters. Department of the Army.

US Army. (1993). *U.S. army field manual: Operations (FM 100-5)*. Headquarters Department of the Army.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183-189. https://doi.org/10.1016/j.drugpo.2013.10.009

Von Clausewitz, C. (2007). *On war*. M. Howard, P. Paret, & B. Heuser (Eds.). Oxford University Press. (Obra original publicada en fecha desconocida).

Wallimann, I., Tatsis, N. C., & Zito, G. V. (1977). On Max Weber's definition of power. *The Australian and New Zealand Journal of Sociology, 13*(3), 231-235. doi:10.1177/144078337701300308

Walzer, M. (1983). *Spheres of justice: A defense of pluralism & equity*. Basil Blackwell.

Winter, P. (2012). *The great firewall of China: How it blocks tor and why it is hard to pinpoint*. USENIX - The Advanced Computing Systems Association.

Wolfsfeld, G., Segev, E., & Sheafer, T. (2012). Social media and the Arab Spring: Politics Comes First. *The International Journal of Press/Politics, 18*(2), 115-137.

Wray-Lake, L., Christens, B. D., & Flanagan, C. A. (2014). Community values. En A. C. Michalos (Ed.), Encyclopedia of Quality of Life and Well-Being Research. Springer. https://doi.org/10.1007/978-94-007-0753-5_482

Yagoda, B. (2014). A short history of "Hack". *The Newyorker*. https://tinyurl.com/4ktnhcb5

YouTube. (s. f.). *Términos del servicio*. https://tinyurl.com/28rt8ykv

Yuan, G. (2013). *Las 36 estratagemas chinas. La sabiduría de Oriente para Occidente*. EDAF.

Zedong, M. (2007 [1937]). *On guerrilla warfare*. S. B. Griffith (Ed.). BN Publishing.