

# CONCEPTUALIZACIÓN del ciberespacio humano

Steven Jones-Chaljub



Escuela Superior de Guerra  
"General Rafael Reyes Prieto"  
Colombia

COLECCIÓN CIBERSEGURIDAD Y CIBERDEFENSA



# Conceptualización

del ciberespacio humano





# Conceptualización

## del ciberespacio humano

STEVEN JONES-CHALJUB

Escuela Superior de Guerra "General Rafael Reyes Prieto"  
Escuela Militar de Cadetes "General José María Córdova"  
Bogotá D.C., 2022

**Catalogación en la publicación – Escuela Superior de Guerra “General Rafael Reyes Prieto” /  
Escuela Militar de Cadetes “General José María Córdova”**

Jones-Chaljub, Steven (autor)

Conceptualización del ciberespacio humano / Steven Jones-Chaljub - Bogotá : Editorial ESDEG, ESMIC Sello Editorial, 2022.

100 páginas : ilustraciones y gráficas ; 24 cm.

Incluye bibliografía p.95

ISBN impreso: 978-628-7602-14-4

E- ISBN: 978-628-7602-13-7

(Colección Ciberseguridad y Ciberdefensa)

1.Ciberespacio 2.Telemática i.Salamanca Rodríguez, Edgar Alexander, Brigadier General (prefacio) ii.Realpe Díaz, Milena Elizabeth, Teniente Coronel (presentación) iii.Colombia. Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG) iv.Colombia. Escuela Militar de Cadetes “General José María Córdova” (ESMIC)

HM851 J66 2022

303.4833 23

Registro Catálogo SIBFuP 991251008807231



Archivo descargable en formato MARC en: <https://tinyurl.com/esdeg991251008807231>

### **Conceptualización del ciberespacio humano**

Primera edición, 2022

**Autor:**

Steven Jones-Chaljub

2022 Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Vicedirección de Investigación

Sello Editorial ESDEG

Carrera 11 No. 102-50 Bogotá D.C., Colombia

[www.esdeglibros.edu.co](http://www.esdeglibros.edu.co)

**Cubierta:**

José Vicente Gómez con base en imágenes de freepik.es

2022 Escuela Militar de Cadetes

“General José María Córdova”

Departamento de I+D+i

Sello Editorial ESMIC

Calle 80 No. 38-00 Bogotá D.C., Colombia

[www.librosesmic.com](http://www.librosesmic.com)

### **Colección Ciberseguridad y Ciberdefensa**

ISBN impreso: 978-628-7602-14-4

ISBN digital: 978-628-7602-13-7

DOI: <https://doi.org/10.25062/9786287602137>

Libro electrónico publicado a través de la plataforma Open Monograph Press.

Tiraje de 200 ejemplares

Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra “General Rafael Reyes Prieto”, publicado en coedición con la Escuela Militar de Cadetes “General José María Córdova”.

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra “General Rafael Reyes Prieto”, la Escuela Militar de Cadetes “General José María Córdova”, las Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.



Los libros publicados por el Sello Editorial ESDEG y el Sello Editorial ESMIC son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas. <https://creativecommons.org/licenses/by-nc-nd/4.0/>



Brigadier General  
**Edgar Alexander Salamanca Rodríguez**  
SUBDIRECTOR

Capitán de Navío  
**Jorge Luis García Durán**  
VICEDIRECTOR DE PROYECCIÓN INSTITUCIONAL

Teniente Coronel  
**Andres Eduardo Fernández Osorio**  
VICEDIRECTOR DE INVESTIGACIÓN

Coronel  
**Oscar Otoniel Torres Conde**  
VICEDIRECTOR ACADÉMICO

Teniente Coronel  
**Diego Alejandro Parra Villamarín**  
VICEDIRECTOR ADMINISTRATIVO



Teniente Coronel  
**Andres Eduardo Fernández Osorio**  
JEFE SELLO EDITORIAL ESDEG

Teniente Coronel (R)  
**Carlos Alberto Ardila Castro**  
COORDINADOR SELLO EDITORIAL ESDEG

**Gustavo Adolfo Patiño Díaz**  
CORRECTOR DE ESTILO

**Eva María Rey Pinto**  
ASISTENTE EDITORIAL

**José Vicente Gómez Alvarez**  
DIAGRAMADOR



# Contenido

---

<b>Prefacio</b> BG Edgar Alexander Salamanca Rodríguez	9-10
<b>Presentación</b> TC Milena Elizabeth Realpe Díaz	11-14
<b>Capítulo 1</b> <b>El ciberespacio como un entorno de interacciones</b> Steven Jones-Chaljub	15-29
<b>Capítulo 2</b> <b>El ciberespacio y sus particularidades</b> Steven Jones-Chaljub	31-51
<b>Capítulo 3</b> <b>El poder en el ciberespacio</b> Steven Jones-Chaljub	53-78
<b>Capítulo 4</b> <b>La sorpresa y el poder en las relaciones interciberespaciales</b> Steven Jones-Chaljub	79-93



# Prefacio

---

**Brigadier General Edgar Alexander Salamanca Rodríguez**

Subdirector de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

Actualmente los contextos estratégicos de los Estados, incluyendo el colombiano, se encuentran en un proceso acelerado de transformación caracterizado por los cambios en la naturaleza de los retos y oportunidades. Uno de los cambios a resaltar es la creciente dependencia que las sociedades modernas han demostrado hacia las tecnologías de la información y comunicaciones (TIC). Esta dependencia ha catalizado la aparición de nuevas amenazas, híbridas y tradicionales, desde y en el ciberespacio, las cuales tienen la posibilidad de afectar toda clase de usuarios (por ejemplo, individuos, empresas y gobiernos).

Colombia es un país considerado como digitalizado. En reconocimiento a esto, el Gobierno nacional, a través de los CONPES 3701/11 y 3854/16, ha creado y potenciado organismos que ostentan funciones particulares en el ciberespacio: CCOC, CSIRT-PONAL, CCP, COLCERT y Comandos Cibernéticos FF. MM. Estos organismos procuran la defensa y explotación del ciberespacio con el propósito de satisfacer y proteger los intereses nacionales, el cual es considerado como la quinta dimensión o quinto dominio de la guerra. Sin embargo, al igual que ocurre con los demás Estados, los organismos encargados de la ciberseguridad y ciberdefensa ven como los retos rebasan a sus capacidades. Las soluciones que se plantean se concentran principalmente en desarrollar e innovar en material, equipo, infraestructura y educación para personal especializado.

El autor afirma que este enfoque ha resultado insuficiente porque no se entiende la verdadera naturaleza de los usuarios de las tecnologías de la información y comunicaciones. Por el contrario, se han fijándose en el imaginario cultural conceptos errados que acentúan en los tomadores de decisiones la percepción que el ciberespacio no es algo que les concierna. Detrás de las máquinas no solo existen quienes interactúan con sus dispositivos en complejos lenguajes de programación, también están quienes buscan un espacio para extender sus

relaciones y actividades sociales con motivaciones legales e ilegales. Recocer y fortalecer esta visión es la razón que impulsó al autor a escribir el presente libro: *Conceptualización del ciberespacio humano*.

Contar con una postura innovadora hacia el ciberespacio invita, sin duda alguna, a reflexionar y analizar la manera como todos nos relacionamos con las tecnologías, incluyendo los beneficios y retos que de éstas se desprenden. Un conocimiento que nos resultará útil a todos en las circunstancias actuales.

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.

Para el desarrollo de la obra se contó con la contribución multidisciplinaria de diversos académicos militares y civiles de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Así mismo, su contenido fue validado a través de un procedimiento de evaluación de pares externos tipo doble ciego. Los puntos de vista pertenecen al autor y no reflejan necesariamente los de las instituciones participantes. Invitamos a los lectores a analizar estos enfoques y así ampliar el conocimiento sobre el tema.

# Presentación

---

## Teniente Coronel Milena Elizabeth Realpe Díaz

Jefe de la Maestría en Ciberseguridad y Ciberdefensa  
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Los seres humanos constantemente soñamos con conquistar lo desconocido. Vimos hacia el firmamento y descubrimos tierras extrañas; subimos nuestra mirada y fuimos al espacio; miramos al mar y nos sumergimos más allá de sus profundidades. Pero ahora, por primera vez en la historia de nuestra especie, no estamos explorando "algo" que estaba allí afuera, sino que lo estamos creando. Esta creación es, sin duda alguna, singular, pues podemos interactuar con y dentro de ella, pero es, al mismo tiempo, tan subjetiva como el tiempo, del cual podemos ver sus manifestaciones en ciertos dispositivos sin que este realmente exista en un plano físico. Tal creación es un logro de la modernidad, y lleva como nombre *ciberespacio*.

Nuestra relación con el ciberespacio, al igual que con las tecnologías que paulatinamente se han ido desprendiendo de este a medida que avanzamos, por así decirlo, no ha sido del todo sencilla. Paradójicamente, comprendemos muy poco nuestra propia creación; principalmente, porque se mantiene una concepción errónea de que "todo lo que tenga que ver con computadores" es una nebulosa que solo compete a personajes caricaturescos que ostentan un conocimiento técnico altamente especializado. Es verdad que el ciberespacio, como veremos, depende de una infraestructura sumamente compleja para existir, pero también es cierto que tiene un lado sociológico y antropológico que no puede ser ignorado, por una simple razón: mientras no existan una inteligencia artificial que nos reemplace o sistemas altamente autónomos, el usuario final en el ciberespacio será una persona de carne y hueso. Dicha posición es resumida en el interior de este libro por la expresión *ciberespacio humano*.

Emplear el ciberespacio humano como punto de referencia tiene grandes ventajas. Al simplificarse el lenguaje técnico, sin perder rigurosidad, se lleva la toma de decisiones a un contexto más cómodo para la mayoría de las personas,

y permite mayores niveles de conciencia y de cálculo individual y organizacional. Adicionalmente, integra otras áreas del conocimiento que brindan herramientas adicionales para seguir construyendo, explotando y, como es el deseo de algunos, controlando "nuestra creación". Estas implicaciones son importantes porque, gústenos o no, el ciberespacio se halla completamente arraigado en todos los niveles de la sociedad moderna, por lo cual se requiere una aproximación más holística para su estudio.

El presente libro es la primera parte de una serie que tiene como objetivo adentrarse en ese lado humano del ciberespacio, a fin de abrir el debate y proponer conceptos que permitan aproximarse a los complejos fenómenos que se presentan en su interior e irradian al "mundo material" en el que vivimos. Debido a la magnitud de la temática, los fenómenos que serán analizados y ejemplificados, así como la gran mayoría de bibliografía empleada, corresponden al campo de la seguridad y defensa en el sentido más estricto posible, incluyendo su vertiente tradicional (por ejemplo, guerra) y no tradicional (por ejemplo, terrorismo, insurgencia y crimen organizado, entre otros).

Esta primera entrega desarrolla varios conceptos interesantes relacionados con el ciberespacio humano. Para iniciar, y de acuerdo con la postura socio-antropológica asumida, se define al ciberespacio como un entorno intangible donde los individuos, así como las colectividades a las cuales estos pertenecen, interactúan para satisfacer diferentes intereses; sin embargo, gracias a los adelantos en la tecnología, la dinámica de estímulo y respuesta que constituye una interacción no se realiza indispensablemente en tiempo real ni con personas presenciales. Las máquinas son susceptibles de ser empleadas como representantes de nuestra voluntad, por lo cual nos permiten manipular el ritmo de las interacciones como, por ejemplo, cuando enviamos un *e-mail* y le damos respuesta un mes más tarde.

Todos tenemos intereses cuando empleamos el ciberespacio, por muy insignificantes que estos sean. Pueden ser desde cosas cotidianas, como leer una noticia, enviar un mensaje, ver un video o hacer una transacción, hasta algunas bien complejas e ilegales. En el reconocimiento de que los intereses no se satisfacen únicamente en el ciberespacio, y de que estos pueden significar la existencia de un conflicto entre partes, particularmente en el área de la seguridad y defensa, este libro ha señalado la existencia de dos grupos de interacciones que no son mutuamente excluyentes. Por un lado, están las *integrativas* y las *distributivas*, las cuales retoman el principio de que es posible cooperar y

competir cuando de intereses se trata. Y por otro, están las *intraciberespaciales* y las *extraciberespaciales*, que, usando como criterio los impactos de las acciones, distinguen el ciberespacio como un entorno o como un medio más del mundo material.

En el ciberespacio existen múltiples actores y colectividades de diferentes naturalezas, y tienen intereses que, usando como criterio la posición del Estado, pueden ser legales/legítimos o ilegales/ilegítimos. En el presente libro, por su enfoque en las disciplinas de la seguridad y los estudios estratégicos, se identifican los siguientes: los *insiders*, los *script-noobs* o *scrip-kiddies*, los *hackers* profesionales, las empresas, el crimen organizado, los grupos terroristas e insurgentes y los *hacktivistas*. La proliferación de actores relevantes se debe a una de las características propias del ciberespacio, denominada *desestatalización*, la cual reconoce que la accesibilidad a las tecnologías de la información y las comunicaciones (TIC) ha permitido generar capacidades por fuera del ámbito de control tradicional, y catalizado así la aparición de actores no estatales con la habilidad para competir con los gobiernos del mundo al mismo nivel, o incluso, para ponerlos en peligro.

La desestatalización no es la única característica singular que tiene el ciberespacio, y que afecta la forma como nos aproximamos a él conceptualmente; este libro ha identificado tres adicionales: 1) la *desterritorialización*, 2) la *dilución de la identidad* y 3) la *hiperconectividad*. La primera de estas características se refiere al hecho de que el ciberespacio, entendido como un todo, no se encuentra bajo el control o el dominio absoluto de un solo ente, a pesar de que la infraestructura tecnológica que lo hace posible está repartida en territorios particulares y, por ende, sujeta a los efectos de las diferentes soberanías estatales. La dilución de la identidad afirma, en general, que un usuario puede tener múltiples versiones de sí mismo en el ciberespacio, que estas pueden ser reales o falsas y que no necesariamente es posible saber con certeza quién está detrás manipulando los dispositivos (Bakken et al., 2004; McDonald & Mills, 2010; Pérez et al., 2018; Shamsi et al., 2016). Finalmente, la hiperconectividad presenta las consecuencias que se generan socialmente del tiempo que las personas permanecen haciendo uso del ciberespacio, de la forma como estas constituyen una audiencia que intercambia a gran velocidad información y de la intrincada red de infraestructura conectada a lo largo y ancho del globo (Dawson et al., 2017).

Las últimas temáticas que este libro desarrolla son el poder en el ciberespacio y la sorpresa como un medio para potenciarlo o socavarlo. El poder es

asumido por este libro en los términos de Lukes (2005) y de Gaventa et al. (como se cita en Dowding, 2006): la habilidad que tiene un actor A para lograr que otro, un actor B, haga, no haga o deje de hacer algo; incluso, en contra de sus propios intereses. A partir de dicha postura, y considerando la existencia de colectividades, se dividió el poder dentro del ciberespacio en dos manifestaciones: *comportamental* y *funcional*. La comportamental desarrolla la manera como las colectividades, en su proceso de autorregulación, por medio del cumplimiento de un sistema de valores y la existencia de unos actores que ejercen autoridad, terminan influenciando qué pueden hacer los usuarios en el ciberespacio. El poder funcional, por el contrario, hace referencia a todas las afectaciones dirigidas a los componentes tecnológicos que permiten el acceso y las interacciones, y que determinan cómo y cuándo los usuarios usan el ciberespacio.

El poder no existe por sí mismo: este tiene fuentes de las cuales emana (por ejemplo, el dinero, las Fuerzas Militares [FF. MM.], las armas nucleares, la información, etc.) y, por lo tanto, no es inalterable ni perene. Existen muchas maneras como dichas fuentes pueden ser potenciadas para lograr más rápido y mejor los resultados esperados y, de igual forma, hacerlas insignificantes o menguar sus impactos. Una de estas es la sorpresa, la cual ha sido uno de los principios generales de la estrategia para las civilizaciones antiguas y modernas. La siguiente entrega de esta serie analizará y comparará los demás principios, desde Sun Tzu (como se cita en Hanzhang, 2000; Sun Tzu, [1963] N.d.) y Von Clausewitz (como se cita en Handel, 1991; Von Clausewitz, [2007]) Fuller (1926), para ver su pertinencia en el ciberespacio humano.

Solo queda por señalar que el ciberespacio humano es un enfoque considerablemente nuevo y, por lo tanto, se sugiere discreción al lector en el empleo de los conceptos desarrollados al respecto, indistintamente del campo donde el ciberespacio tiene injerencia (por ejemplo, el comercio, el mercadeo, la educación o los procesos productivos, entre otros). De igual forma, y con el propósito de contribuir en el debate y acrecentar nuestro entendimiento de este complejo entorno, es indispensable tener una mente abierta y curiosa a lo largo de toda la lectura, porque, como dijo una vez Einstein, "lo importante es no dejar de hacerse preguntas".

## 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	<i>Seguridad y Defensa de los Sistemas de Información: Estrategia de Francia</i> (2011, p. 21).	Espacio de las comunicaciones creado por la interconexión mundial de equipos de procesamiento de datos digitales.
2	Rusia	<i>Concepto de Estrategia para la Ciberseguridad de la Federación Rusa</i> , 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	<i>La Estrategia de Ciberseguridad del Reino Unido: Protegiendo y promoviendo el Reino Unido en un mundo digital</i> (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	<i>La Estrategia de Ciberseguridad del Reino Unido: Protección, seguridad y resiliencia en el ciberespacio</i> (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	<i>La estrategia nacional para asegurar el ciberespacio</i> (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	<ul style="list-style-type: none"> <li>• <i>Diccionario de términos militares y asociados del Departamento de Defensa</i> (2011, p. 92).</li> <li>• Glosario de términos clave de la seguridad de la información del NIST (2013, p. 58).</li> <li>• Concepto operacional del ciberespacio y plan de capacidades del Ejército de Estados Unidos 2016-2028 (2010, p. 6).</li> </ul>	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	<ul style="list-style-type: none"> <li>• <i>Estrategia de Ciberseguridad de Alemania</i> (2011, p. 9).</li> <li>• Oficina Federal para la Seguridad de la Información (BSI): Glosario.</li> </ul>	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	<i>Estrategia de Ciberseguridad: Hacia un ciberespacio de liderazgo mundial, resistente y vigoroso</i> (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	<i>Estrategia de Ciberseguridad para una más fuerte y próspera Canadá</i> (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.º 1 de la decisión gubernamental N.º 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	<i>Marco estratégico nacional para la seguridad del ciberespacio</i> (2013, p. 9).	El ciberespacio es un dominio construido por el hombre, y compuesto, esencialmente, de nodos de TIC, redes, <i>hosting</i> 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	<i>Estrategia nacional de ciberseguridad para Montenegro 2013-2017</i> (2013, p. 5).	El ciberespacio es más que internet: incluye no solo el <i>hardware</i> , el <i>software</i> y los sistemas de información, sino también, las personas y las interacciones sociales dentro de estas redes.
18	Holanda	<i>La estrategia de ciberdefensa</i> (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	Rumanía	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	<i>Estrategia nacional de ciberseguridad y plan de acción 2013-2014</i> (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, <i>software</i> 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 ( <i>software</i> ), 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.<sup>1</sup> 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,<sup>2</sup> 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*<sup>3</sup> aprovechó vulnerabilidades desconocidas por los administradores del sistema (*zero-day exploit*)<sup>4</sup> para introducir una carga dañina (*payload*)<sup>5</sup> que alterara los ciclos en las centrífugas de enriquecimiento de material radioactivo. En ese

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

<sup>2</sup> Transacciones comerciales realizadas a través de internet.

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

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

<sup>5</sup> 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).<sup>6</sup>

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*,<sup>7</sup> 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

---

<sup>6</sup> 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).

<sup>7</sup> 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,<sup>8</sup> 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.<sup>9</sup> 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

---

<sup>8</sup> El término SCADA es el acrónimo de *Supervisory Control and Data Acquisition*; los cuales son sistemas de control y supervisión de diferentes procesos y maquinaria de tipo industrial.

<sup>9</sup> *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 interrupciones 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 de un nuevo entorno como si no. La dificultad se exagera 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.<sup>10</sup>

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 continua 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

---

<sup>10</sup> 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.



## Capítulo 2

# El ciberespacio y sus particularidades\*

DOI: <https://doi.org/10.25062/9786287602137.02>

**Steven Jones-Chaljub**

Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Citación APA:** Jones-Chaljub, S. (2022). El ciberespacio y sus particularidades. En Jones-Chaljub, S., *Conceptualización del ciberespacio humano* (pp. 31-51). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602137.02>

### 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.

Los estudios en ciencias sociales, en general, se han centrado tradicionalmente en fenómenos, variables y estructuras que pertenecen al “mundo material”, o “real”, o que se manifiestan en él; sin embargo, a medida que la humanidad avanza, estos han tenido que migrar hacia nuevas áreas, que constituyen todo un reto y exigen mantener cierta flexibilidad. Es apenas lógico. El conocimiento no está constituido por axiomas, sino por un entrelazado de interpretaciones y posturas que, a la larga, terminan por brindar *algo* de sentido a nuestro entorno.

La aparición del ciberespacio, en virtud de su naturaleza como un entorno intangible donde se puede interactuar para satisfacer intereses, es, sin duda, un nuevo campo de estudio. Y como tal, no podemos pretender que las aproximaciones teóricas del pasado tengan completa habilidad explicativa. La razón radica en las características del ciberespacio que deconstruyen varios elementos básicos de las ciencias sociales: el espacio y el tiempo, los vínculos entre individuo y sociedad y la presencialidad en la formación de relaciones.

Habiendo dicho lo anterior, conviene ahora profundizar lo que hace del ciberespacio algo tan especial, y que determina la forma como debemos aproximárnosle. Estas características son, entonces, las siguientes: desestatalización, desterritorialización, dilución de la identidad e hiperconectividad.

## Desestatalización

El primer capítulo de este libro dio una breve introducción a por qué el concepto de *usuario* del ciberespacio exige una separación del Estado como actor principal o, en otras palabras, una desestatalización. Vale la pena retomar la razón de fondo. Los individuos, así como las colectividades a las cuales estos pertenecen, han demostrado ser en extremo hábiles para desenvolverse en el ciberespacio,

en procura de unos intereses por completo distintos de los de carácter nacional. De igual forma, su capacidad para poner constantemente en jaque al aparato estatal les otorga una muy merecida posición en ese entorno intangible.

Existen múltiples fuentes bibliográficas que explican al detalle las categorías en las cuales se clasifican los actores no estatales del ciberespacio (Brenner, 2007; Bronk et al., 2012; Clemente, 2011; Command, 2005; Gilman et al., 2013; Lewis, 2002; Springer, 2015), por lo cual no viene al caso entrar a desglosarlas en su totalidad. Lo importante para nosotros es entender que estas se hallan compuestas por seres humanos que buscan tener o lograr algo en dicho entorno intangible, y que eso puede llevar a interacciones distributivas donde se manifiesten comportamientos de imposición y de resistencia, según se muestra en la tabla 3.

**Tabla 3.** Actores del ciberespacio

ESTÍMULO	INSIDERS	SCRIPT-NOOBS /SCRIPT-KID- DIES	HACKERS PRO- FESIONALES	EMPRESAS	TERRORISTAS/ INSURGENTES	CRIMEN ORGA- NIZADO	HACKTIVISTAS	ESTADOS
Recursos económicos	X		X	X	X	X		X
Ideología (política, cultura, religión)	X		X		X	X	X	X
Membresía (pertenencia, autoestima, identidad)		X			X	X	X	
Reputación		X	X	X	X	X	X	X
Valores (justicia, solidaridad, libertad)	X		X	X	X		X	X
Curiosidad		X						

ESTÍMULO	INSIDERS	SCRIPT-NOOBES / SCRIPT-KID-DIES	HACKERS PROFESIONALES	EMPRESAS	TERRORISTAS/ INSURGENTES	CRIMEN ORGANIZADO	HACKTIVISTAS	ESTADOS
Caos/supervivencia					X			
Modos	1) Inteligencia y espionaje (explotar, filtrar); 2) reclutamiento; 3) coordinación y logística; 4) influenciar y engañar (integridad información, ingeniería social, propaganda); 5) atacar sistemas, redes e información (dañar, interrumpir, degradar, negar, responder); 6) defender sistemas, redes e información propios o terceros (proteger, detectar, restaurar).							
Técnicas y medios	<i>Rootkits, defacement, spoofing, ransomware, phishing (whaling, spear, smishing, vishing), malware (troyanos, gusanos, virus), distributed denial of service (DDoS), keyloggers, sniffers, ataques cinéticos, bombas lógicas, ataques SQL, buffer overflow, botnets, cross-site scripting, advanced persistent threat (APT), account hijacking.</i>							

**Fuente:** elaboración propia.

La tabla 3 resume los estímulos que podrían incitar a los distintos actores del ciberespacio a actuar en contra de otros; dentro de ellos están enmarcados los intereses. De igual forma, presenta los modos (el cómo), así como las técnicas y los medios más comunes para imponer o resistirse (el con qué).

Los considerados como *insiders* son los usuarios que hacen parte de una colectividad y están dispuestos a interactuar en contra de ella por dinero, por una ideología o por un conjunto de valores. Su comportamiento puede ser inducido —penetración en el argot del espionaje— o consecuencia de la motivación personal. La diferencia entre un *insider* y un “individuo común” que utiliza el ciberespacio es la calidad de “miembro” del primero. Finalmente, estos pueden o no tener competencias técnicas en materia tecnológica (NCCIC, 2014).

Edward Snowden y Chelsea (Bradley) Manning pueden ser considerados casos icónicos de *insiders* en el ciberespacio. Ellos, por sus respectivas posiciones éticas e ideológicas, decidieron hacer enormes filtraciones de material sensible de la Agencia Nacional de Seguridad (en inglés, NSA, por las iniciales de National Security Agency) y del Ejército de Estados Unidos, para así vulnerar los intereses de dichas colectividades. No todos los *insiders* tienen las motivaciones de Snowden y Manning; otros terminan vendiendo la información en el mercado negro, al mejor postor.

Los *script-noobs*, o *scrip-kiddies*, hacen referencia, peyorativamente, a los usuarios que están incursionando en el *hacking*, pero no tienen el conocimiento o la habilidad suficientes para desarrollar sus propias técnicas o modos y, por tanto, se limitan a utilizar código y *software* publicado por otros (por ejemplo, Angry IP Scanner, Kali Linux, Cain & Abel, y Ettercap, Metasploit, entre otros). Estos usuarios no se preocupan, en general, por entender el funcionamiento de las herramientas, sino por generar impactos rápidos que los lleven a adquirir mayor reputación, saciar su curiosidad o cumplir con los criterios de membresía de alguna colectividad.

Es necesario desmitificar la figura del *hacker* para tener más claridad sobre este como usuario del ciberespacio. La primera vez que el término se empleó para establecer una relación entre las personas y la tecnología modernas se remonta, según indica la cultura popular, a los años cincuenta del siglo XX, en los salones del Massachusetts Institute of Technology (MIT). De acuerdo con Jesse Sheidlower, presidente de la Sociedad Americana de Dialéctica, *hackear* se refería a "trabajar en" o "solucionar" un problema asociado a una máquina o una tecnología de una forma más creativa o diferente de aquella establecida por el manual de usuario (Yagoda, 2014). A partir de ese momento, el término evolucionó rápidamente de uno benigno, usado para designar a entusiastas interesados en adquirir mayores conocimientos que la media sobre los sistemas y las tecnologías, hacia uno negativo que implicaba la vulneración de sistemas, programas e información (Yagoda, 2014). La estigmatización del *hacker* llevó rápidamente a la creación de categorías para establecer las intenciones del usuario, y así dio origen a los adjetivos de *blanco* (buenos o éticos) y *negro* (malos o mal intencionados) (NortonLifeLock, 2017).

Los que son verdaderos *hackers* profesionales no son tan comunes como uno podría creer, y tampoco son fieles copias del estereotipo de hombre obeso y con acné que vive en el sótano de la casa de su madre. Han existido algunos bastante famosos entre las categorías de "sombrero blanco" y "sombrero negro" que, incluso, se vestían con ropa de diseñador y poseían varios millones de dólares en sus cuentas personales (por ejemplo, Gary McKinnon, Kevin Mitnick, Adrian Lamo, Kevin Poulson y Albert González).

Los considerados de "sombrero blanco", también llamados *hackers* éticos, utilizan sus habilidades para propósitos legales; por ejemplo, irrumpir en sistemas para evitar que una vulnerabilidad desconocida sea explotada para causar daño. Los de "sombrero negro" son todo lo contrario: estos buscan beneficios personales

en prácticas que son ilegales o antiéticas. Realmente, la distinción entre ambas categorías es subjetiva, pues se mueve entre la dicotomía de bueno-malo, la cual está cargada de juicios de valor; por tal razón, el título dependerá de la posición que cada actor tenga frente a las actividades desarrolladas por el *hacker*.

Los *hackers* profesionales pueden trabajar solos o ser parte de un grupo (por ejemplo, LulzSec, ShadowCrew, Lizard Squad), donde, seguramente, ostentan una posición de liderazgo. De igual manera, están dispuestos a perseguir sus propios intereses o ser contratados, a manera de mercenarios, por terceros. Los estímulos que los afectan pueden ser diferentes y variar según la circunstancia, pero lo que sí es seguro es que rara vez se dejan llevar por la curiosidad infantil o el caos sin sentido. Contrario a la creencia, este libro considera que los *hackers* de este nivel han aprendido por experiencia, en la mayoría de los casos, a comportarse más bajo una lógica racional que por el narcicismo o el ego; sus carreras dependen de su reputación, y han visto cómo un simple error puede echarlo todo a perder.

Kevin Mitnick, conocido por el alias de *Cóndor*, fue un respetado *hacker* de "sombrero negro" que, simplemente, se dejó llevar demasiado por el ego, lo cual le significó cinco años de cárcel. En vez de dedicarse a realizar sus actividades ilegales, robar cualquier tipo de información que pudiese vender y mantenerse fuera de los radares del FBI gracias a sus habilidades superiores, se enfrascó en un pulso con la persona equivocada: el experto en seguridad informática Tsutomu Shimomura. El reto de superar a Shimomura, quien por motivos personales se alió con el FBI, lo llevó a ser capturado en 1995 (Shimomura, 1996).

Todos los actores analizados hasta el momento tienen la posibilidad de existir fácilmente por fuera de una colectividad o desvinculados de esta. Para ser parte de las categorías de *insiders*, *script-noobs*, o *kiddies*, y *hackers* profesionales, tan solo se requiere a uno mismo. Los actores restantes, como se muestra en la figura 1 (i.e. empresas, terroristas/insurgentes, crimen organizado y Estados) son todo lo opuesto. Ellos, a excepción de los Estados, por razones obvias, rara vez se manifiestan de forma distinta de la de un conglomerado de personas.

Las empresas, multinacionales o no, utilizan al ciberespacio para el desarrollo de sus actividades cotidianas. El empleo va desde cosas sencillas, como el manejo de las redes sociales a efectos de mercadeo, hasta la administración de los procesos productivos a través de los sistemas de control industrial (en inglés, ICS, por las iniciales de *Industrial Control Systems*); sin embargo, en los términos aquí descritos, la mayor parte de las interrelaciones terminan siendo estimuladas

por recursos económicos y materializándose en el fenómeno del espionaje económico, político y social (Hua & Bapna, 2015; PricewaterhouseCoopers, 2018).

El espionaje industrial o corporativo puede ocurrir con o sin el apoyo de los recursos del Estado; algunos países —en particular, China— han sido reiteradamente denunciados por dicha práctica. Existen dos casos que son emblemáticos para el estudio del espionaje corporativo desde el ciberespacio: *Black Dragon* y el caso del F-35 de Lockheed Martin.

En febrero de 2011 la compañía McAfee publicó el informe *Global Energy Cyberattacks: Night Dragon*. En este se revelaba que diferentes empresas del sector energético, dentro de las cuales se encontraban Exxon Mobil y Royal Dutch Shell, habían sido víctimas de una serie de ataques encubiertos, sostenidos y coordinados desde 2009. McAfee reveló que el APT *Night Dragon* empleó herramientas, técnicas y redes de origen chino, y que su origen era la ciudad de Heze, en la provincia de Shandong. Este ciberataque causó multimillonarias pérdidas, representadas en información financiera y operacional (Lee, 2013).

Distintas fuentes, dentro de las cuales se incluye Edward Snowden, argumentan que entre 2007 y 2009 el gobierno chino estuvo involucrado en el robo de información ultrasecreta relacionada con el avión de combate F-35 *Lightning*, de la empresa Lockheed Martin. Los *terabytes* de información técnica de la aeronave (por ejemplo, radar y motores, entre otros) significaron pérdidas económicas por más de 100 millones de dólares, y un riesgo para la seguridad de Estados Unidos y sus aliados. Se cree que los aviones chinos J-31 y *Chengdu* J-20 tienen componentes copiados directamente del avanzado F-35 (Gady, 2015).

En marzo de 2016, el empresario chino Su Bin, también conocido como Stephen Su y Stephen Subin, se declaró culpable por el delito de conspiración ante la Corte del Distrito de los Ángeles, Estados Unidos. Por su rol central en el robo de información del F-35, así como otros objetivos (por ejemplo, C-17), Su Bin fue condenado en julio de 2016 a cuatro años de prisión y una multa de 10.000 dólares, de una sentencia que abarcaba un máximo de cinco años de cárcel, y a pagar el mayor valor entre 250.000 dólares o el doble de las ganancias o las pérdidas que resultasen del crimen (Burgess, 2016).

El espionaje corporativo puede tener o no relación con el crimen organizado, pero lo cierto es que ambos terminan apuntando, salvo para casos en los cuales se involucra la seguridad nacional, a la búsqueda constante de beneficios económicos. Para estos últimos, el ciberespacio es usado principalmente para la coordinación, la logística y las comunicaciones, al igual que como lugar de compra y venta de bienes,

productos y servicios. En la *Dark Web* —contenido no indexado que solo es accesible a través de ciertos navegadores no tradicionales (por ejemplo, TOR)— existe una gran variedad de plataformas dedicadas a la compra y la venta de armas, drogas, dinero falso y tarjetas de crédito plagiadas, así como a la contratación de asesinos a sueldo, pornografía infantil, tráfico de órganos y personas, y servicios en el ciberespacio (por ejemplo, alquiler de *botnets* y de *hacking*), entre otros.

Una de las plataformas más famosas de la *Dark Web* fue *Silk Road* —en español, camino de la seda—. Dicho portal fue puesto en funcionamiento en 2011, y hasta su desmantelamiento por el FBI, en 2013, contaba con alrededor de 25.000 productos. Se calcula que el volumen de ventas al mes era de 1,2 millones de dólares, que dejaban una comisión de 92.000 dólares al operador del *Silk Road*: el ciudadano estadounidense Ross William Ulbricht, también conocido por el alias de Dread Pirate Roberts (Aldridge & Décary-Héту, 2016; Bergman, 2001; Dittus et al., 2018; Schneider & Williams, 2013; Van Hout & Bingham, 2014). El caso de *Silk Road* fue el más famoso mediáticamente, pero luego de su desaparición han surgido nuevos y más complejos mercados negros: *Farmer's Market Place*, *Black Market Reloaded*, *Drug Market*, *Drugs4You*, *Onion Pharma*, *Pablo Escobar Drugstore*, *Alphabay* y *Hansa*. Los últimos dos listados fueron “capturados” en julio de 2017, y Alphabay, particularmente, tuvo un tamaño diez veces mayor que el de *Silk Road*; este contaba con 40.000 vendedores y 250.000 productos y producía más de 5 millones mensuales de dólares en volumen de ventas (Paquet-Clouston et al., 2018).

El crimen organizado no es la única colectividad considerada fuente de inseguridad que se mantiene activa en el ciberespacio: también lo hacen las organizaciones terroristas e insurgentes. Muchos consideran que las interacciones realizadas por dichas organizaciones en este entorno intangible se hallan direccionadas a ocasionar un apocalipsis tecnológico, así como a vulnerar SCI de infraestructura crítica, a fin de ocasionar miles de muertes. Si bien es posible que estos lo consideren una opción, las probabilidades son escasas. Y es que los recursos que esa opción implica —personal, equipo e infraestructura, al igual que los niveles de coordinación y persistencia del ataque— superan con creces las capacidades conocidas de las organizaciones actuales.

La opción de estos actores de *tercerizar* conocimiento especializado, digamos *hackers* profesionales, se ve menguada por la presión proveniente de la agenda internacional contra el terrorismo y la insurgencia. El alto grado de prioridad que los Estados dan a dicho fenómeno conlleva una destinación importante de recursos para la prevención, la detección, la reacción y la mitigación. Ello, en

consecuencia, aumenta ostensiblemente los riesgos para el prestador del servicio, el cual, salvo que tuviese alguna filiación ideológica, podría obtener iguales o mayores beneficios desarrollando otras actividades delictivas.

Las organizaciones terroristas e insurgentes tienen un comportamiento semejante en el ciberespacio. Cabe recordar que estos, al menos en teoría, tienen una motivación ideológica que los impulsa a "ganar los corazones y las mentes" de una audiencia particular. Y para ello requieren hacer uso de todos los medios masivos de comunicación que estén a su alcance. Así, el ciberespacio no solo es empleado para captación de recursos, coordinación logística y reclutamiento, sino también, como un valioso aliado para la propaganda —incluyendo ataques cibernéticos de impacto bajo (por ejemplo, *defacement*)—. <sup>1</sup> Cabe mencionar, además, que estos también emplean los mercados negros listados, lo cual, a su vez, causa un fenómeno de convergencia donde es difícil distinguir entre el crimen y la violencia políticamente motivada (Ogun, 2015).

El Estado Islámico de Irak y el Levante (ISIL), también conocido como ISIS o *Daesh*, ha sido particularmente prolífero en el empleo del ciberespacio. Lo primero que viene a la mente son los macabros videos de calidad cinematográfica que ISIL ha puesto en circulación, y donde se evidencian múltiples ejecuciones con diversos métodos; sin embargo, hay muchos otros elementos que el individuo promedio desconoce. Existen diferentes foros, perfiles en redes sociales y publicaciones (por ejemplo, la revista *Dabiq*) cuyo objetivo es radicalizar a la audiencia y mantener un contacto continuo con ella.

ISIL también tiene partidarios o miembros cuyo rol es generar disturbios en el ciberespacio y filtrar información. Tal es el caso del Cyber Caliphate Army (CCA), un grupo pro-ISIL cuyos *hackers* estuvieron al frente del *defacement* de la cuenta de Twitter del Comando Central de los Estados Unidos (CENTMON) en 2015 (Ackerman, 2015). La misma organización publicó una lista de 8.786 personas, con sus respectivos datos personales en Estados Unidos e Inglaterra, que eran susceptibles de ser objetivos para los "lobos solitarios" (Corbin, 2017). <sup>2</sup> Se cree que el líder del CCA, Osed Agha, fue abatido durante un bombardeo de las FF. MM. de Estados Unidos, en marzo de 2017 (Corbin, 2017).

---

<sup>1</sup> El *defacement* es un tipo de ataque cibernético dirigido a una página *web* o una cuenta de red social, y que tiene el propósito de cambiar el contenido visible original por algo completamente distinto. En la mayoría de los casos, el contenido falso es alusivo a la ideología del atacante o constituye una crítica a la víctima.

<sup>2</sup> Los "lobos solitarios" (en inglés, *homegrown terrorism*) son personas que, sin tener algún vínculo directo como miembros, lanzan golpes a favor de una organización terrorista, insurgente o criminal.

Las Fuerzas Armadas Revolucionarias de Colombia (FARC), organización que fluctúa entre las etiquetas de insurgencia y terrorismo, también ha sabido aprovechar el ciberespacio. Las FARC cuentan, incluso antes de concluir el proceso de paz de La Habana, con diferentes páginas *web* activas, las cuales tienen un diseño elaborado, interfaces a redes sociales, *blogs*, publicaciones en múltiples idiomas, emisora y sección de noticias independientes. A la fecha, estas son: [mujerfariana.org](http://mujerfariana.org); [farc-ep.co](http://farc-ep.co); [farc-epeace.org](http://farc-epeace.org); [resistencia-colombia.org](http://resistencia-colombia.org); [frenteant.org](http://frenteant.org); y [farc-ep-occidente.org](http://farc-ep-occidente.org).

La última de las colectividades que queda por ser analizada de acuerdo con la tabla 3 son los grupos *hacktivistas*. Este libro ya trató gran parte de la temática en su primer capítulo, cuando habló de *Anonymous*; solo queda por reafirmar que las interacciones de dichas colectividades en el ciberespacio son estimuladas directamente por una agenda ideológica. Esta puede tener variaciones circunstanciales relacionadas con los lugares geográficos, pero mantiene un conjunto de valores que se desprenden de la asociación entre información y libertad. Lo anterior no significa que no estén dispuestos a defender su reputación cuando ella sea puesta en entredicho.

La desestatalización del ciberespacio es, sin duda alguna, una de sus características fundamentales. El hecho de que existan varios actores no estatales con la habilidad para interactuar al mismo nivel no puede ser menospreciado; no, particularmente, para entender cómo estos actúan cooperativa o distributivamente dentro del marco de distintos intereses o estímulos. Y es que, como se vio en la presente sección, existen momentos donde, a pesar de las distintas naturalezas, el ciberespacio es empleado de manera semejante. Este nivel de complejidad podría ser manejado por los académicos y los tomadores de decisiones del mundo, salvo porque es acentuado por la siguiente característica: la desterritorialización.

## La desterritorialización

El ciberespacio sufre una relativa desterritorialización o, en otras palabras, la no completa subordinación de su existencia a un territorio particular. Esto último, en el sentido estrictamente legal, se refiere a cualquier lugar bajo la soberanía de un Estado.<sup>3</sup> Se le otorga preponderancia a la concepción del territorio bajo la lógica del sistema

<sup>3</sup> El concepto de *territorio* varía según el Estado. En el caso de Colombia, el artículo 101 de la Constitución Política establece que el territorio está compuesto por lo siguiente: “[...] el subsuelo, el mar territorial, la zona contigua, la plataforma continental, la zona económica exclusiva, el espacio aéreo, el segmento de la órbita geostacionaria, el espectro electromagnético y el espacio [...]”.

Estado nación por encima de otras alternativas, por simple practicidad. Todos vivimos, gústenos o no, en dicho sistema, y mientras perdure, lo que suceda en el mundo tendrá que ver de alguna u otra forma con sus dinámicas; por lo tanto, abstraerse del Estado nación para analizar el ciberespacio es un gesto irresponsable.

Se ha dicho que la desterritorialización es relativa porque al respecto coexisten dos verdades. En principio, si se lo entiende como un todo, el ciberespacio no se encuentra bajo la soberanía absoluta de ningún Estado u organismo; ni siquiera, de la *Internet Corporation for Assigned Names and Number* (ICANN). De esa forma, no existe tal cosa como un ente que resida en el entorno y tenga la facultad para controlar las interacciones de todos los individuos, así como el flujo completo de información; sin embargo, también es cierto que, dentro del marco de sus propios territorios, los Estados sí tienen múltiples facultades que les permiten ejercer influencia en el ciberespacio (Assaf & Moshnikov, 2020; Ayers, 2016; Liapopoulos, 2013).

La ausencia de un totalitarismo en el ciberespacio, desde el todo, radica en la manera como se distribuyen geográficamente los elementos de la arquitectura tecnológica. Dicho entorno existe a través de las interconexiones transnacionales de diversos componentes tecnológicos que se encuentran en los territorios de múltiples países, lo cual, a su vez, causa que bajo el sistema del Estado nación ninguno tenga hegemonía sobre el entramado completo. Tal argumento se halla presente, hasta cierto punto, en el documento titulado *Declaración de Independencia del Ciberespacio*.

La *Declaración de Independencia del Ciberespacio*, originalmente en inglés, es un documento publicado por John Perry Barlow, fundador de Electronic Frontier Foundation, en 1996, durante su estadía en Davos, Suiza. Barlow es un notable activista que ha adquirido su reputación como defensor de los derechos y las libertades civiles en un mundo digital. Vale la pena presentar textualmente un apartado de la declaración:

Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente [...] No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo [...] No tenéis ningún derecho moral a goberarnos ni poseéis métodos para hacernos cumplir vuestra ley que debemos temer verdaderamente.

No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras [...] Estamos creando nuestro propio Contrato Social. Esta autoridad se creará según las condiciones de nuestro mundo, no

del vuestro. Nuestro mundo es diferente [...] está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos [...] Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia. Aquí no hay materia. Nuestras identidades no tienen cuerpo, así que, a diferencia de vosotros, no podemos obtener orden por coacción física [...]. (Barlow, 2009, p. 241-242)

La declaración de Barlow no es del todo acertada. Como ya se mencionó, los Estados sí ejercen control sobre la porción de infraestructura tecnológica que se encuentra en sus territorios (por ejemplo, servidores y cables de fibra óptica, entre otros), lo cual les brinda la habilidad para limitar el acceso a internet y censurar el contenido a los usuarios domésticos, así como a los extranjeros a quienes se les provea el servicio. En tal sentido, sí hay una relativa soberanía en el ciberespacio o, como Barlow lo describe, el entorno de la "mente".

Existen múltiples formas como los Estados limitan el acceso al ciberespacio y censuran el contenido disponible a los usuarios. Una de ellas, aunque poco efectiva, es programar a través del *Domain Name Service* (DNS) de los proveedores de internet que las peticiones a un dominio reflejen como nulo. De una forma más simple, la ventana del navegador de un usuario que quiera ingresar a una página *banned* no mostrará información, sino un aviso de "censura" o los famosos errores http 403 'forbidden', http 404 'not found' y http 451 'unavailable for legal reason'. Otra manera —quizás, la más apropiada— consiste en establecer diversos sistemas de monitoreo y bloqueo en la salida de los cables submarinos que conectan a los operadores locales con el *backbone* de internet —esto se ampliará en la sección de hiperconectividad—. China es uno de los países reconocidos por el empleo de dichas prácticas.

Los esfuerzos legales y técnicos del Partido Comunista de China (PCC) para controlar el ciberespacio, y que algunos han denominado jocosamente como 'El Gran *Firewall* de China', han terminado bloqueado el funcionamiento de las plataformas de Facebook, Twitter, Snapchat, YouTube y Google, así como de diferentes periódicos y revistas, entre otros (*Economy*, 2018; Winter, 2012). De igual manera, las búsquedas de eventos o temáticas sensibles son infructuosas o presentan información manipulada por el gobierno (por ejemplo, la masacre en la plaza de Tiananmen, la independencia del Tíbet o la de Xinjiang y el Estado de Taiwán) (Blocked on Weibo, s.f.).

La soberanía de los Estados también se extiende, por medio de la ley y el castigo, a todos los individuos y las colectividades que permanecen en sus territorios.

Incluso, cuando se trata de interacciones en el ciberespacio, estos últimos se enfrentan a la decisión de desafiar o no el ordenamiento jurídico que rige su existencia material. Relacionarse o no dentro de ese entorno con temáticas "prohibidas" es de libre potestad del individuo, pero el riesgo de que su identidad sea descubierta, con todas las consecuencias que ello implica, se encuentra latente.

Aquello que se prohíbe realizar o poseer en el ciberespacio tiene, por lo general, una connotación de inmoral o inconveniente para una sociedad o un gobierno determinados; no obstante, como las interrelaciones pueden desarrollarse entre individuos o sistemas separados por miles de kilómetros de distancia —y por ende, bajo distintas soberanías—, lo castigable en un lugar no necesariamente lo será en otro. Ello dificulta enormemente la cooperación internacional, y hace que la política sea el principal mecanismo para generar presión.

La pornografía infantil es uno de esos temas respecto a los cuales los gobiernos del mundo se encuentran altamente motivados —al menos, públicamente— para cooperar a fin de castigar el uso indebido del ciberespacio por parte de otros usuarios. Las diversas operaciones de naturaleza transnacional dan muestra de ello. Una de las más icónicas, debido a su nivel de impacto y de coordinación, fue realizada en 2009, bajo el nombre de *Operation Delego*. Esta fue liderada por Estados Unidos y dio como resultado el desmantelamiento de una red de 72 personas en diferentes países, y la confiscación de, aproximadamente, 16.000 DVDs (*Huffingtonpost*, 2011).

Contrario a la pornografía infantil, el asunto de perseguir a infractores que vulneren intereses económicos privados es mucho más complejo (por ejemplo, derechos de autor, filtraciones...). En primer lugar, al desligarse los efectos de los valores comunes a la humanidad, como la protección de la infancia frente al acoso sexual, se genera menor simpatía y responsabilidad colectiva. En segundo lugar, no todos los Estados tienen claridad o capacidades para atender situaciones donde los usuarios del ciberespacio en su territorio vulneran, en los términos descritos, los intereses de terceros que se encuentren por fuera de este.

El mandato de la ley sobre los usuarios en el ciberespacio se halla supeditado a la habilidad del Estado para encontrar un sujeto imputable a quien adjudicar responsabilidad de un comportamiento "prohibido"; en otras palabras, se necesita saber quién debe ser castigado. En el "mundo material", la responsabilidad puede dividirse entre actores (por ejemplo, facilitadores, actor intelectual, etc.),

pero al final esta termina siendo asociada a una identidad vinculada a un único cuerpo físico. Si usted comete un delito, y determinan su identidad, no hubo "múltiples usted" para ser juzgados, sino solo uno. En el ciberespacio, esto es posible gracias a la "dilución de la identidad".

## Dilución de la identidad

La identidad, entendida como el conjunto de rasgos propios, se puede manifestar en este entorno intangible de dos formas principales: *perfiles* y *componentes* técnicos. La primera hace referencia directa al usuario como individuo o colectividad, mientras que la segunda está enfocada en la infraestructura tecnológica que permite hacer uso del ciberespacio.

Las herramientas, las plataformas, las comunidades, los foros y los videojuegos, entre otros, que están conectados a internet solicitan al usuario su identidad para tener mayor acceso a contenido. Esta, por lo general, se encuentra constituida por un perfil, un "nombre de usuario", un "avatar" y una contraseña. El perfil es toda esa información personal que nos distingue de otros (por ejemplo, nombres, edad, género, *e-mail*, etc.). El nombre de usuario y el avatar son, respectivamente, la representación textual (i.e. alfanumérica, cirílica, pictogramas, etc.) y gráfica de nuestro perfil.

Un actor puede tener múltiples versiones cibernéticas de sí mismo, así como la capacidad para interactuar de manera simultánea con todas ellas. La proliferación es consecuencia de las políticas de homónimos de los sistemas, al igual que de la falta de verdaderos mecanismos de verificación.

Seguramente ustedes ya se habrán enfrentado a la dispendiosa labor de crear una cuenta para, por ejemplo, ingresar a las redes sociales, cuando vamos a la opción "Registrarse", el sistema nos presenta un formulario con diferentes campos para llenar, dentro de los cuales están el correo electrónico, el nombre de usuario y la contraseña. En la selección del nombre de usuario, salvo que tengan suerte o sea algo genuino, tendrán que elegir entre ciertas recomendaciones automáticas, porque su elección "ya existe" o "no está disponible". Si replican el mismo procedimiento para otros fines, al final del ejercicio tendrán, al menos, entre dos y tres nombres de usuario que los representarán en el ciberespacio.

Luego de haber completado el registro, el sistema envía a sus correos electrónicos, previamente suministrados, un hipervínculo que deben abrir para verificar la creación de la cuenta. Eso está diseñado más para evitar los abusos de máquinas

virtuales que para determinar si ustedes realmente son lo que en sus perfiles dicen ser. Y aquí es donde aparece la verdadera dilución de la identidad. No existe una manera efectiva de determinar si la información suministrada en un perfil corresponde a la realidad de un usuario; al menos, no para los servicios y las redes abiertas al público. Como resultado, tener completa y constante certeza de quién está realizando las interacciones en el ciberespacio es algo imposible.

Los depredadores sexuales —en especial, los de infantes y adolescentes— utilizan constantemente la dilución de la identidad para sus cometidos. La primera forma como la emplean es conocida como *grooming* (NSPCC, s. f.). Esta se caracteriza por la creación de perfiles falsos en redes sociales, donde los agresores se muestran como contemporáneos de las posibles víctimas (NSPCC, s. f.). El objetivo es lograr una relación de confianza, para que los potenciales agredidos accedan a un encuentro en la vida real, un intercambio de imágenes propias de naturaleza sexual o un *videochat* con el mismo propósito. La segunda forma tiene como fin, también a través de perfiles falsos, cambiar o trazar el material adquirido de las víctimas en los mercados negros del ciberespacio.

La dilución de la identidad en el ciberespacio se manifiesta no solo con la creación de perfiles falsos, sino también, a través de la suplantación de los reales. Con suficiente conocimiento técnico es posible apoderarse del perfil de un usuario descuidado, llevar a cabo algún acto ilegal o inaceptable socialmente y evitar ser vinculado como responsable. Esto puede lograrse fácilmente con ingeniería social, *software* y *malware* (por ejemplo, *keyloggers*).

Un apunte final frente a la dilución de la identidad desde los perfiles. Las distintas interrelaciones que se generan en el ciberespacio no solo requieren una identidad, sino también, que esta sea demostrada, autenticada o certificada. Por tal razón, existen cosas como las claves, las palabras secretas, los códigos y los *tokens*, entre otros. A pesar de ello, la identidad no siempre está atada a una única persona en el mundo material. En muchas colectividades —particularmente, las consideradas ilegales— se comparten los elementos de autenticación para evitar una monopolización del acceso o de la información. Así, puede existir un perfil cibernético que es utilizado por múltiples personas, lo cual, a su vez, crea una paradoja: todos son uno, pero el uno no es alguien en particular.

La muestra perfecta de este tipo de dilución es el empleo de los correos electrónicos como medio de coordinación entre grupos criminales, terroristas e insurgentes. Para evitar ser rastreados, sus miembros comparten entre ellos las claves de un correo electrónico, de forma que cualquiera tenga acceso para

compartir información a través de la bandeja "Borrador". Más precisamente, alguien escribe un mensaje, pero no lo envía, lo cual hace que el contenido se almacene en una especie de "nube", y permite que este sea consultado y modificado, con relativa seguridad, por quien posea la contraseña. En tales casos, las autoridades vinculan fácilmente el perfil a una organización, pero no a individuos en concreto, salvo, claro, que estos sean descuidados (Soghoian, 2012).

En 2008, las FF. MM. de Colombia neutralizaron a alias Raúl Reyes, miembro del máximo nivel jerárquico de las FARC: el Secretariado. Durante la operación, con código "Fénix", se recuperaron, en estado lamentable, varios computadores portátiles y memorias USB. Gracias a la ayuda de la Interpol, el Gobierno colombiano pudo acceder a la información almacenada en estos elementos, la cual, para sorpresa de todos, incluía cientos de correos electrónicos y comunicados de la cuenta personal de alias Reyes (*Revista Semana*, 2008).

La Operación Fénix, junto con los correos de alias Reyes, desató una tormenta diplomática entre Colombia y sus países vecinos. De forma casi inmediata, se generó una disputa en materia de soberanía; sin embargo, en los meses posteriores, los correos dieron lugar a múltiples señalamientos. De acuerdo con la información disponible, el computador de alias Reyes sugirió la existencia de una estrecha cooperación entre las FARC y ciertos gobiernos de la región. Los perfiles de los alias Teodora de Bolívar, Ángel y El Cojo eran los que levantaban más sospechas, pero, a la fecha, no se han demostrado públicamente sus identidades reales (*El Tiempo*, 2008).

La identidad en el ciberespacio, ya desde una posición más técnica, se manifiesta a través de una serie de protocolos, procesos y datos (por ejemplo, IP, *tracking cookies*, *caches*, *referrers*, metadata en imágenes y texto, etc.). De estos, el más común —al menos, para el público general— es el *Internet Protocol* (IP) y sus direcciones (por ejemplo, IPv4 69.45.21.345/ IPv6 2002:65D4:64D4:FE01). Las direcciones IP son números únicos que representan a un dispositivo conectado a alguna red que sustenta la transferencia de información en el protocolo TCP/IP. El protocolo TCP/IP, junto con otros existentes (i.e. FTP, HTML, POP3, SMTP, DHCP), constituye el lenguaje común que permite a la infraestructura tecnológica constituir el ciberespacio.

Análogamente, las IP son muy parecidas a las direcciones postales de nuestras viviendas, salvo por la forma como son adjudicadas por el proveedor de servicio de internet. Por petición del usuario, una IP puede ser *estática* o *dinámica*. Las primeras son, como su nombre indica, estables; son asociadas de

forma permanente al usuario. Las segundas, por el contrario, pueden cambiar automática y periódicamente a través del *Dynamic Host Configuration Protocol* (DHCP), así como manualmente desde el *CMD*, o desconectando el *router*.

Los proveedores de servicio de internet (ISP), dependiendo de la región o el país, retienen el registro de la adjudicación de IP estáticas y dinámicas y generan un enlace directo con la identidad de quien contrata el servicio. De igual manera, mantienen, por un tiempo determinado, datos de la navegación de sus clientes en internet (i.e. *IP Logs*); sin embargo, respecto a la dilución, las direcciones IP no permiten saber quién está realmente tras el dispositivo haciendo uso del servicio contratado, y tampoco son infalibles.

La identidad adjunta a la dirección IP puede ser manipulada con facilidad. Por un lado, y en las versiones más sencillas, es posible hacer uso de *Virtual Private Networks* (VPN) y otros tipos de *software*/navegadores (por ejemplo, TOR) para mantener la anonimidad en la red, evitar la geolocalización y evadir mecanismos de seguridad. Mayores niveles de complejidad implican el secuestro de un dispositivo y su acceso a la red, como sucede, por ejemplo, con las *botnets*.

Las *botnets* son un conjunto de computadores infectados por malware —en el argot son conocidos como *zombies*—, los cuales responden al unísono a las órdenes de uno o varios computadores maestros. En este caso particular, los dueños de los *zombies* no son conscientes de que sus máquinas —y por ende, sus identidades cibernéticas— están siendo utilizadas por otro; quizás solo noten un cambio moderado en la velocidad de funcionamiento. Las *botnets* son comúnmente empleadas para el envío de SPAM y *Distributed Denial of Service* (DDoS). Algunas de las más elaboradas que han existido son: *Zero Access*, *Windigo*, *Storm*, *Conficker*, *Srizbi*, *Mariposa*, y *Bredolab*. Por ejemplo, **Mariposa**, una de las *botnets* más extensas, tuvo una cuenta de afectación de 13 millones de computadores en 2009, de los cuales cerca del 5% se encontraban en Colombia. La existencia de las *botnets* y sus altos números, entre otros fenómenos que ocurren paralelamente, son posibles gracias a otra característica del ciberespacio: la hiperconectividad (Moscaritolo, 2010).

## La hiperconectividad

Cuando se habla de hiperconectividad en el ciberespacio se está haciendo referencia a dos cosas diferentes. Por un lado, el término atañe al incremento en el tiempo que las personas pasan conectadas a internet; particularmente, a través

de la diversificación y la disminución del costo/precio de los dispositivos con conexión (i.e. internet de las cosas). Por otro, se refiere al complejo entramado que conforman las redes globales de comunicaciones donde, para sorpresa de muchos, no solo se encuentra el internet que usamos a diario en nuestros hogares y nuestros trabajos (por ejemplo, Planet Lab, Internet 2 and 3, GSM, ESnet, GLIF, entre otros). A efectos de diferenciación, estas hiperconectividades se llamarán, respectivamente, *humana* y *estructural*.

La hiperconectividad, vista desde lo humano, no es una característica del ciberespacio, sino una consecuencia directa de la proliferación, la penetración y la interrelación de las redes que conforman dicho entorno. Esta se entiende como la conformación de una audiencia de varios millones de usuarios que, a través de interrelaciones cibernéticas, intercambian a gran velocidad datos, experiencias y posiciones de diversos eventos y fenómenos. Así, la hiperconectividad humana se halla estrechamente relacionada con la facilidad del usuario para acceder a información de múltiples fuentes y orígenes geográficos.

El fácil acceso a la información que caracteriza la hiperconectividad humana cataliza y exagera tensiones, sentimientos y juicios en los usuarios (algunas veces, de manera apresurada), los cuales tienen efectos políticos, económicos y sociales. Las razones son varias. Por un lado, la información empodera a la persona, la hace actor y juez del entorno; una situación fomentada por la facultad para realizar comparaciones y rectificaciones en los sistemas de valores sociales (i.e. bueno/malo, moral/inmoral). Y por otro, se genera un efecto de masificación, donde la individualidad —a menos que se tenga el criterio suficiente para superar el temor al aislamiento— se somete a la colectividad.

La Primavera Árabe, las marchas en Colombia (por ejemplo, la Marcha NO + FARC) y la movilización ciudadana en Venezuela en contra del chavismo son muestras de cómo una minoría, con ciertas opiniones o sistemas de valores, usó la hiperconectividad humana en el ciberespacio —por ejemplo, las redes sociales— para influenciar una masa poblacional. La consecuencia —al menos, para el caso de los países árabes y de Magreb— fue la caída de varios regímenes dictatoriales, como ocurrió en Libia y Egipto, y el inicio de la crisis en Siria (Wolfsfeld et al., 2012).

La hiperconectividad humana también juega un rol importante en la economía: genera mayores niveles de productividad, gracias al acceso a información, la coordinación y las capacidades que superan los límites de la naturaleza humana (por ejemplo, mayor procesamiento de datos). Algunas manifestaciones

son las comunidades de interés, las agencias de inteligencia, las bases de datos y estadísticas mundiales, la conectividad entre procesos productivos y cadenas de suministros, y las campañas masivas de mercadeo, entre otros.

La hiperconectividad, ya desde una posición más técnica o estructural, como aquí se la denomina, es mucho más sencilla de explicar desde una analogía. El entramado de redes y dispositivos a escala global es al ciberespacio como los adelantos en los medios de transporte a la salud humana; ambos facilitan la veloz propagación de nuevas y más resistentes epidemias, y hacen del tiempo y de la cooperación los recursos más preciados.

La hiperconectividad estructural es el reflejo de la infraestructura de una red. Veamos, por ejemplo, a internet, que es, sin duda alguna, la de mayor importancia para las sociedades modernas. En el centro de todo se encuentra lo que se denomina el *backbone* —en español, columna vertebral—. Esta es la principal línea de transferencia de información de internet, y se encuentra constituida por la interconexión de grandes redes estratégicas, llamadas **Network Service Providers** (NSP), y una serie de *core routers*. Las NSP están, por así decirlo, unidas a través de *Network Access Points* (NAP) o *Metropolitan Area Exchanges* (MAE), lo cual permite un funcionamiento homogéneo y rápido de internet.

Las NSP venden ancho de banda a los proveedores de servicio de internet (PSI) nacionales, y estos, a su vez, a los regionales. Ambos tipos de PSI brindan acceso a internet al usuario final; todo dependerá de la cobertura del servicio. En el caso de Colombia, los principales PSI nacionales son ETB, UNE, Telefónica y Claro. El tráfico de estos es llevado a través de cables submarinos al NAP de Miami, y de allí es redirigido a los NSP a los cuales se les haya comprado el tránsito (por ejemplo, TeliaSonera, Sprint, Tata y NTT). En contraste, los PSI regionales, al no tener acceso a los NSP, prestan sus servicios a través de la compra de tránsito a los PSI nacionales.

La estructura de internet descrita, salvo por los componentes del *backbone*, se replica múltiples veces a lo largo y ancho del planeta Tierra. Así, un usuario en Asia estará interconectado, de alguna u otra forma, con otro en América, gracias a las interacciones entre sus PSI, NAP o MAE, y NSP. Sin ello, entendido por este libro como *hiperconectividad estructural*, las bondades de internet no serían posibles tal como las conocemos, y el ciberespacio sería tan solo un entorno constituido por islotes que jamás se tocarían.

## Lecciones

- El ciberespacio tiene una serie de características que deben ser tomadas en cuenta por los académicos y los tomadores de decisiones para hacer análisis y asumir posturas con verdadero valor. Estas tienen la habilidad de deconstruir elementos básicos de las ciencias sociales sobre los que se soportan la mayoría de las políticas y las estrategias: el espacio y el tiempo, los vínculos entre individuo y sociedad y la presencialidad en la formación de relaciones.
- Las características del ciberespacio para tomar en cuenta, en entre otras, son: la desestatalización, la desterritorialización, la dilución de la identidad y la hiperconectividad.
- La desestatalización demuestra que en el ciberespacio coexisten diferentes actores no estatales que tienen la habilidad para interactuar al mismo nivel, por intereses o motivaciones disímiles, de las diferentes formas descritas en el capítulo primero de este libro: 1) cooperativa o distributivamente, o 2) intra o extraciberespacialmente. La desestatalización libera al estudio del ciberespacio del monopolio del Estado, desde el sentido más realista posible, lo cual obliga a los académicos y a los tomadores de decisiones a asumir una postura más incluyente.
- La desterritorialización acentúa el impacto de la desestatalización, toda vez que genera una relativa desvinculación del ciberespacio del control soberano que ejercen los Estados sobre el territorio. Cuando se lo entiende como "un todo", el ciberespacio no está en ningún territorio en particular, lo cual hace que ningún gobierno tenga el dominio absoluto del entorno; sin embargo, la arquitectura tecnológica que hace posible la existencia de dicho espacio, así como los usuarios, sí se encuentran en lugares geográficos delimitados, y ello permite que los Estados puedan ejercer cierta influencia en el interior de sus fronteras.
- La desterritorialización presenta grandes retos a los Estados; particularmente, cuando se trata de encontrar un responsable susceptible de ser castigado por el uso "ilegal" o "inmoral" del ciberespacio. Y es que las leyes domésticas, gracias al sistema de Estado nación, no se extienden por fuera de las fronteras, lo cual hace que los esfuerzos de cooperación queden reducidos a voluntad política.

- La identidad es entendida como el conjunto de rasgos de un usuario que lo identifican como único en el ciberespacio. Esta puede manifestarse de dos maneras principales: perfiles y componentes técnicos; sin embargo, a través de distintas herramientas y prácticas, la identidad puede ser diluida, y así exacerbar aún más los retos para los Estados. En otras palabras, no es fácil tener certeza de quién está empleando un dispositivo para interactuar en el ciberespacio; por ello, las operaciones en el entorno intangible —particularmente, la *Dark Web*— requieren varios meses para generar resultados concluyentes.
- La hiperconectividad es la última de las características del ciberespacio listadas por el presente libro. Esta hace referencia a la posibilidad para las personas de tener acceso constante a información proveniente de diversas fuentes (i.e. hiperconectividad humana), así como al entramado existente entre las distintas redes y la infraestructura que dan vida al ciberespacio (i.e. hiperconectividad estructural). En cualquiera de los casos, el mensaje final de la hiperconectividad es que cualquier cosa que suceda en el entorno intangible se magnifica a una velocidad alarmante, y genera impactos políticos, económicos y sociales.
- Las características del ciberespacio que fueron desarrolladas en este capítulo, junto con la aproximación desde las interrelaciones, constituyen el marco referencial sobre el que se sustentará el estudio del poder en dicho entorno.



## Capítulo 3

# El poder en el ciberespacio\*

DOI: <https://doi.org/10.25062/9786287602137.03>

**Steven Jones-Chaljub**

Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Citación APA:** Jones-Chaljub, S. (2022). El poder en el ciberespacio. En Jones-Chaljub, S., *Conceptualización del ciberespacio humano* (pp. 53-78). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602137.03>

### 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.

A lo largo de la historia, las mentes de muchos han sido cautivadas, al punto de la obsesión, por el irresistible deseo de entender, poseer o mantener el "poder". Les ha ocurrido a los puramente teóricos y académicos, así como a diversos personajes, icónicos y comunes, ilustres y nefastos, que se desarrollaron en las múltiples esferas de la sociedad. Lo interesante es que dicha tendencia se mantiene hoy por hoy.

Todos, y con ello me refiero a la humanidad en general, tenemos cierto conocimiento tácito del poder. Podemos sentirlo, verlo y vivirlo con facilidad, pero cuando llevamos la experiencia al lenguaje y tratamos de profundizar en sus laberintos, nos perdemos en un mar de interrogantes.

En ese esfuerzo por acercarse al "poder" se han manifestado diversos planteamientos, desde numerosas áreas del conocimiento, que han permitido conformar un nutrido marco conceptual. En sociología y en ciencias políticas, Maquiavelo y Hobbes sentaron los cimientos del debate, el cual fue continuado, solo por mencionar a los más representativos, por Webber (como se cita en Wallimann et al., 1977), Dahl (1957), Bachrach y Baratz (1962), Lukes (2005), Gaventa (1980), Clegg y Giddens (como se cita en Sadan, 1997) y Foucault (1982). En el ámbito de seguridad y defensa, se destacan Sun Tzu ([1963], s. f.), Napoleón ([2018], s. f.), Von Clausewitz ([2007], s. f.), Mahan ([2018], s. f.), Douhet ([2013], s. f.), Jomini ([2008], s. f.), y Fuller (como se cita en Strenski, 1998).

A pesar de sus múltiples contribuciones, los trabajos de estos autores tienen un punto de convergencia que, inevitablemente, lleva a cuestionar la pertinencia de emplearlos textualmente para analizar al poder en el contexto del ciberespacio: todos ellos terminaron por reducir el poder a variables y estructuras que pertenecen o manifiestan en el "mundo material" o "real", lo cual choca directamente con el argumento de la flexibilidad teórica, soportado por las características desarrolladas en el segundo capítulo de este libro. Eso no significa que los

trabajos de los estudiosos clásicos quedan descartados, sino que deben emplearse a la luz de las circunstancias; es decir, tomar lo que sea útil y descartar lo que resulte inverosímil para ese entorno intangible.

Este tercer capítulo busca desarrollar la manera como el poder se manifiesta en el ciberespacio. El énfasis que se hace en la preposición no es al azar: indica que solo se tendrán en cuenta las interacciones interciberespaciales. La razón es sencilla. En dichas interacciones el ciberespacio funge como un entorno, con las particularidades que lo caracterizan, donde los actores y los sistemas se encuentran, se relacionan y se influyen mutuamente. En las interacciones extraciberespaciales, por el contrario, el entorno intangible se transforma en una simple herramienta más para la proyección de poder en el mundo material, lo que no contribuye al debate.

En el orden de ideas planteado, el capítulo se encuentra dividido en tres secciones. La primera de ellas comprende las premisas básicas teóricas que serán utilizadas para analizar el poder en el ciberespacio. La segunda desarrollará la forma como los actores influyen el comportamiento de otros a partir de un sistema de valores, si se toma en cuenta que el ciberespacio es, en esencia, y a pesar de su inmaterialidad, un entorno social. La última sección analiza la forma como los actores pueden configurar a otros el acceso al ciberespacio, al igual que la información que se encuentra disponible. De esta manera se responden ciertas preguntas fundamentales: quién, cómo, cuándo y dónde se puede o no hacer qué en el ciberespacio.

## Las premisas del poder en el ciberespacio

Los estudios tradicionales del "poder" comienzan, por lo general, estableciendo como punto de partida la existencia de uno o varios sujetos, representados por las letras "A" y "B", que tienen la habilidad para interrelacionarse en un contexto particular, por múltiples razones. Dentro de este marco, se afirma que el "poder" se manifiesta cuando "A" consigue que "B" realice o no algo que este último no habría hecho de manera autónoma o voluntaria; es decir, sin la intervención de "A". La misma dinámica se manifiesta con diferentes nombres y condicionamientos: por ejemplo, en Lukes (2005), Gaventa (1980), Clegg y Giddens (como se cita en Sadan, 1997); pero la esencia es igual. Las diferencias entre los autores se desprenden de la naturaleza de los sujetos "A" y "B", la calidad y las consecuencias de su relación, el nivel de conciencia que ambas

partes tengan, las fuentes de donde emana el poder y las maneras como este último es empleado.

A la pregunta sobre cuál debería ser la aproximación teórica correcta para el ciberespacio, en la opinión propia del autor, la respuesta la brindan sus propias particularidades. El ciberespacio es un *entorno intangible creado desde componentes materiales y digitales que se constituyen en requisitos inamovibles para tener acceso; los usuarios pueden interactuar en y desde el ciberespacio solo si pueden ingresar a este*. Ello hace que el contexto donde se desarrollan las relaciones de poder se inclinen más hacia las *interciberespaciales* (usuario-usuario, usuario-sistema y sistema-sistema) que hacia las **extraciberespaciales**. En cualquier caso, debido a la desestatalización, los sujetos "A" y "B" se mueven en las categorías previamente mencionadas: individuos comunes, *insiders*, *script-noobs* o *script-kiddies*, *hackers* profesionales, *hacktivistas*, terroristas, insurgentes, crimen organizado, empresas y Estados.

La razón por la cual este libro acepta la proliferación de actores como premisa para analizar el poder es simple. Se ha demostrado que todos esos actores tienen la habilidad para relacionarse en el ciberespacio, y que al tener algún tipo de interés que los lleva a cooperar o competir entre ellos mismos, incluso por encima de sus diferentes naturalezas, tienen un incentivo para tratar de influenciar al otro. Ahora bien, esto es cierto cuando se tienen o no niveles elevados de conciencia sobre la relación de poder.

Si el poder es la habilidad para lograr que el otro haga o no algo, existe la posibilidad de que ese otro se resista. El éxito del empleo del poder implica que el otro, bajo esta lógica, debe percibir que resistirse es imposible, o que al intentarlo fracase. Cuanto esto último ocurre se habla de conflicto *directo* o *latente*. En ambos casos, los actores, quienes influyen y resisten, tienen un alto nivel de conciencia de la relación de poder; a esto se le denomina *poder directo* (Mager-Hois, 2010).

El poder directo está presente en la mayoría de los autores clásicos especializados en seguridad y defensa. Para dichos autores, a los Estados se les reconoce abiertamente como la principal fuente de inseguridad, lo cual los hace conscientes de su necesidad de proteger sus intereses a través del monopolio y el ejercicio del poder. Esa es una postura normal cuando se plantea el realismo puro como enfoque teórico.

Los actores pueden no ser conscientes de hallarse inmersos en una relación de poder, así como de la posición favorable o desfavorable que ocupan, por lo cual consideran su comportamiento algo natural y propio de la vida. Cuando algo

así ocurre se está ante un caso de *poder tácito*. En materia de seguridad y defensa, el poder tácito es transversal a la aparición de amenazas no estatales (por ejemplo, insurgencia y terrorismo), donde el objetivo es influenciar indirectamente a la población. De igual forma, el poder tácito hace parte activa de los estudios donde se analizan las estructuras sociales del poder, y la relación de estas con el individuo; a ese respecto, los de Michel Foucault son los más reconocidos.

Los niveles de conciencia en las relaciones de poder generan, entonces, una dualidad que debe ser tomada en cuenta en el contexto del ciberespacio: poder directo y poder tácito; sin embargo, dicha dualidad no se manifiesta de manera independiente, sino a través de las interrelaciones *interciberespaciales*. Al final de cuentas, el poder es una dinámica entre actores que es incapaz de existir abstraída de la relación que se gesta entre ellos.

Queda una cuestión final que debe ser respondida para completar las premisas de este capítulo, y la cual *cuestiona* el origen del poder. Respecto a si este realmente se adquiere y se pierde de formas particulares o si, por el contrario, es una variable perenne e innata de la condición humana, este libro acepta ambas posturas. En el ciberespacio, tal como se mostrará, existen medios de los cuales emana el poder, y dichos medios se pierden o se agotan en el tiempo. De igual forma, al ser el ciberespacio un entorno donde los seres humanos transfieren sus interacciones, muchas de las estructuras sociales del "mundo real" son, voluntaria o involuntariamente, replicadas (por ejemplo, valores, códigos de conducta, vigilantismo, etc.).

## El poder comportamental en las interrelaciones interciberespaciales

La desestatalización, acompañada por la relativa desterritorialización, aparta al ciberespacio de la concepción hobbesiana del poder. Al difuminarse el rol del Estado y generarse los vacíos de soberanía propios de la relación con el territorio, se vuelve inviable el impulso unánime de toda la colectividad ciberespacial de transferir o ceder, en términos de Hobbes (como se cita en Buzan, 1983), los medios de poder a un leviatán para garantizar la seguridad en un entorno anárquico. En consecuencia, se genera una proliferación de actores que pueden fungir como intermediarios de la voluntad del Estado, así como competir o no con este en el desarrollo de gobernanza; estos serán denominados a partir de ahora como *actores reguladores*.

Los principales *actores reguladores* identificados son los Estados, las plataformas/sistemas, los escenarios cibernéticos, y las comunidades virtuales. Estos ejercen influencia sobre las interrelaciones de los usuarios del ciberespacio o, en otras palabras, delimitan lo que estos últimos pueden y no hacer, al igual que la forma como lo hacen. Esa habilidad es denominada por este libro como *poder comportamental*, y será el objeto de análisis de la presente sección. Este tipo de poder puede ser tácito o directo, dependiendo del nivel de conciencia que los actores mencionados, junto con el usuario final, tengan de la relación.

Entender a los *actores reguladores* y la manera como estos se comportan y ejercen poder comportamental requiere el desarrollo de cuatro conceptos sociológicos básicos: comunidad, membresía, sistemas de valores y autoridad. Estos son requeridos porque el ciberespacio, no obstante ser intangible, es un lugar donde ocurren interrelaciones que, al final, siguen siendo entre personas. Y las personas, en su comportamiento como criaturas sociales, extrapolan al ciberespacio, consciente o inconscientemente, *mecanismos de autorregulación existentes* en el "mundo real" (por ejemplo, administradores, aceptación de términos, resolución de controversias, vigilantismo, etc.) (Brainard, 2010; Fox & Roberts, 1999).

Las comunidades, desde la posición del comunitarismo de Walzer (1983), son un conjunto de individuos que conviven e interactúan para el cumplimiento de un objetivo común. En estas, la membresía, entendida como la posibilidad de ser parte del grupo, se distribuye con el fin de asegurar que únicamente los iguales estén juntos. Los criterios de distribución de la membresía y la calidad de "igual" se desprenden de la alineación y la aceptación de un sistema de valores que constituyen la identidad de la comunidad. A eso se le conoce como la *autodeterminación de la comunidad* y, en teoría, sus miembros deberían estar prestos a defenderla.

El sistema de valores se compone de múltiples elementos: creencias, ritos, historias, memoria colectiva, normas y leyes, símbolos y comportamientos aceptados y condenados, entre otros. Dicho sistema se manifiesta a través de las instituciones de gobierno, religión y educación, al igual que en los medios de expresión escrita, oral y visual (por ejemplo, arte, leyes, literatura, canciones, etc.). Para que un sistema de valores sea útil para la comunidad, este debe ser claro y enseñado a sus miembros (Wray-Lake et al., 2014).

La desviación del sistema de valores —y por ende, el incumplimiento del contrato social— puede desencadenar distintas formas de castigo. Estos pueden

ser *privativos* (por ejemplo, el aislamiento), *físicos y psicológicos* (por ejemplo, la tortura y la muerte), *económicos* (por ejemplo, las multas y las compensaciones), *simbólicos* (por ejemplo, el señalamiento y la exigencia de disculpas públicas), e ir directamente contra la membresía (por ejemplo, la expulsión y el exilio). El propósito del castigo es forzar el cumplimiento —incumplir en sí mismo ya constituye algo— y suplir el daño que la acción genera en la comunidad o en algún otro miembro.

Aquel considerado la “autoridad” es quien se encarga de velar por el sistema de valores, así como de determinar y ejecutar el castigo correspondiente. La autoridad puede ser adquirida por mérito propio, como ocurre en las dictaduras, o ser designada a través de la elección popular. En cualquier caso, y no sin un límite en la mayoría de los casos, la autoridad controla los medios coerción, disuasión y persuasión. Por ejemplo, en las democracias sus miembros, entendidos como los nacionales, o población, ceden al gobierno el monopolio de la fuerza (por ejemplo, la policía), pero este tiene ciertas reglas que, por principio, debe respetar, y que se pierden completamente en los regímenes dictatoriales (por ejemplo, el uso de la policía para reprimir la oposición política).

Al trasponer estos cuatro conceptos sociológicos al contexto de *ciberespacio*, y suponiendo que se mantengan el comportamiento social que nos define como especie y el acceso tecnológico, todos los usuarios, desde los comunes hasta los considerados ilegales ante los ojos de la ley (por ejemplo, criminales, terroristas, etc.), hacen parte de o han tenido acceso a algún tipo de comunidad virtual. La comunidad virtual se erige como una asociación de usuarios, con o sin identidad diluida, que conviven e interactúan por o para un fin común en particular (Brainard, 2010; Fox & Roberts, 1999).

Las comunidades virtuales tienen, por lo general, una persona denominada “administrador”, que tiene las funciones de: proteger el sistema de valores de la comunidad; otorgar y modificar accesos y privilegios, y aceptar, negar y despojar membresías. Dicho administrador puede o no ser el creador de la comunidad, y termina estableciendo qué interactúan los miembros dentro del marco del objetivo común que los define, y cómo lo hacen. Por ejemplo, el administrador de una comunidad existente en un foro o en un grupo de red social que tiene como fin compartir fotos de aves establece normas frente a la autoría de tales imágenes, y puede *bannear* (prohibir) —equivalente ello a despojar de la membresía— a los usuarios que se adjudiquen impropriamente créditos o que solo comparten fotografías de automóviles.

Las comunidades virtuales no existen en la nada: requieren un escenario cibernético delimitado que las soporte (por ejemplo, redes sociales, aplicación, intranet, videojuegos en línea, canales, foros, *boards*, *chans*, *chats*, etc.). El escenario cibernético es un conjunto de datos, parámetros, configuraciones, protocolos y demás que son designados para cumplir un fin determinado que implica el acceso de varios usuarios conectados en red (i.e. comunicarse, compartir imágenes, realizar transacciones, etc.). La accesibilidad se hace posible y fácil a través de la creación de interfaces gráficas y auditivas intuitivas para los usuarios; adicionalmente, los componentes que dan vida a los escenarios cibernéticos se encuentran alojados en otras plataformas o sistemas de mayor envergadura, o dependen de ellos para su funcionamiento. Algunos escenarios famosos son Instagram, YouTube, WhatsApp, Facebook, Twitter y 4Chan. La *Dark Web* también tiene los suyos, pero son más difíciles de ubicar de forma permanente (por ejemplo, 8Chan). Una característica de los escenarios que debe tomarse en cuenta es su capacidad para dar forma a más de una comunidad virtual no excluyente; es decir, comunidades que brindan a los usuarios membresía de manera simultánea. Así, en el ejemplo del grupo de aves, los usuarios pueden ser miembros, de forma paralela, de otras comunidades dentro de Facebook.

Al igual que ocurre en las comunidades virtuales, los escenarios cibernéticos tienen sus propios sistemas de valores, los cuales dan a conocer, en la mayoría de los casos, en forma de "condiciones" de prestación del servicio. Estas condiciones aplican sobre todas las comunidades virtuales que utilizan el escenario cibernético para existir, al igual que los usuarios que se encuentran en cada una de ellas. En el caso YouTube, producto de Alphabet Inc., cuando alguien se dispone a crear una identidad o una cuenta, el escenario requiere al usuario remitirse a los siguientes términos:

Al usar o ingresar al sitio de Internet de YouTube o cualquier producto, software, feed de datos y servicio de YouTube [...] usted acuerda expresamente (1) estos términos y condiciones (en lo sucesivo los "Términos del Servicio"), (2) la política de privacidad de YouTube [...] que declara expresamente conocer y aceptar en todos sus términos, y que se considera aquí íntegramente reproducida [...] y (3) los Lineamientos de la Comunidad YouTube, [...] que declara expresamente conocer y acepta en todos sus términos [...] Si no estuviera de acuerdo con los Términos del Servicio, la política de privacidad de YouTube o los Lineamientos de la Comunidad YouTube, por favor no utilice el Servicio. (YouTube, s.f.)

En el ciberespacio muy pocos escenarios existen sin un “dueño”; la mayoría de estos son productos o servicios prestados, con o sin ánimo de lucro, por usuarios o empresas. Dichos “dueños” son, igualmente, *actores reguladores*, identificados con el nombre de plataforma/sistema en esta sección, que tienen sus propios sistemas de valores, los cuales proyectan hasta el usuario final. Facebook, por ejemplo, es una plataforma/sistema que tiene bajo su tutela diferentes escenarios cibernéticos, considerados por ellos productos o servicios, y sobre los cuales establecen los términos que se detallan a continuación.

## Declaración de derechos y responsabilidades

Esta Declaración de derechos y responsabilidades [...] tiene su origen en los Principios de Facebook y contiene las condiciones de servicio que rigen nuestra relación con los usuarios y con todos aquellos que interactúan con Facebook, así como con las marcas, los productos y los servicios de Facebook, que se denominan “servicios de Facebook” o “servicios”. Al utilizar o acceder a los servicios de Facebook, muestras tu conformidad con esta Declaración, que se actualiza periódicamente [...] Puesto que Facebook ofrece una amplia gama de servicios, es posible que te pidamos que leas y aceptes condiciones complementarias aplicables a tu interacción con una aplicación, un producto o un servicio determinados. (Facebook, 2015)

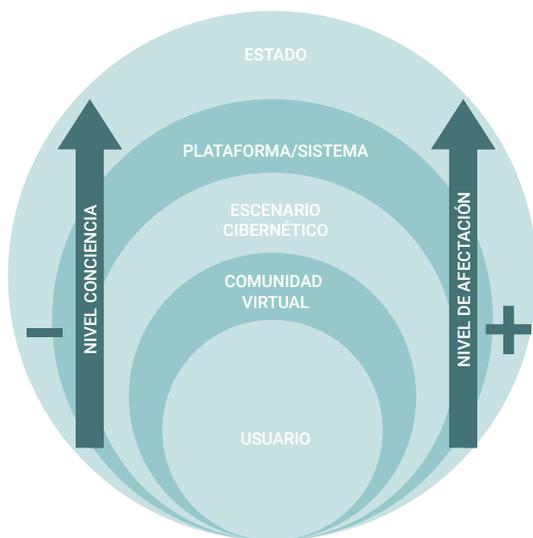
Facebook, como se evidencia en el fragmento anterior, contiene sus propios “principios” —elementos de un sistema de valores— que, espera, sean aceptados por todos, y que eventualmente acaban influenciando las interacciones de los usuarios. Los principios del sistema/plataforma son: 1) libertad para compartir y conectarse; 2) propiedad y control de la información; 3) flujo libre de información; 4) igualdad fundamental; 5) valor social; 6) plataformas y estándares abiertos; 7) servicio fundamental; 8) bienestar común, y 9) un mundo. Los sistemas/plataformas no son autónomos, pues sus actividades se hallan regidas por las reglamentaciones del territorio donde su infraestructura tecnológica se encuentra, así como por las del sitio donde prestan el servicio. Así lo establece Facebook cuando afirma en la introducción de sus principios que “la consecución de estos [...] debería estar limitada únicamente por la ley, la tecnología y las normas sociales en continuo desarrollo” (Facebook, s. f.).

La manera como los *actores reguladores*, desde el Estado hasta la comunidad virtual, influyen las interrelaciones de los usuarios, o, en otras palabras, proyectan poder comportamental, se puede describir a la manera de un flujo en

cascada, como el que se muestra en la figura 1. Un evento ocurrido en Singapur en 2014 permite describir de mejor manera dicho flujo, al igual que la manera como este tipo de poder funciona.

Singapur es uno de los países con tejido social más complicados del mundo. En esta pequeña isla del Pacífico conviven miles de personas provenientes de múltiples países, al punto de que existen en su territorio cuatro idiomas oficiales (i.e. inglés, mandarín estándar, tamil y malayo) y diez religiones (i.e. hinduismo, zoroastrismo, judaísmo, budismo, taoísmo, jainismo, cristianismo, islam, sijismo y baha'i). En el pasado, el país sufrió revueltas religiosas y raciales; una de las más complejas fue la de 1964, denominada *Communal Riots*, que dejó varias docenas de muertos y heridos (Richard, 1984).

**Figura 1.** Establecimiento de los flujos del poder comportamental, según los autores reguladores



**Fuente:** elaboración propia.

Con el fin de evitar nuevas rupturas en la nación, el gobierno de Singapur estableció fuertes leyes contra cualquier manifestación de "discursos de odio", o *hate speech*, por medio de la *Sedition Act* (The Statutes of the Republic of Singapore, 2013). Las empresas de servicios cibernéticos que operan en la isla deben tener especial cuidado y ver por el cumplimiento de sus políticas frente a la temática. De igual forma, transfieren esas políticas a los productos que

ofrecen, y esperan que los usuarios acepten y cumplan, como clientes, ciertos compromisos. Un usuario que no admita dichos términos, simplemente, no podrá hacer uso del servicio (Price, 2002).

En junio de 2014, Google (plataforma o sistema) se vio obligado a remover el blog llamado *Blood Stained Singapore* (comunidad virtual), ofrecido por su producto Blogger (escenario cibernético), luego de que el gobierno singapurense emitió su "recomendación" al respecto. El blog tenía como propósito describir y demostrar disgusto, de manera no violenta, hacia la población filipina que habita la isla. Las autoridades locales consideraron que esa era la visión de un extremista que podría ser enjuiciado, junto con sus simpatizantes (usuarios), mientras algunos analistas vieron en ello un disgusto de la población frente a las políticas laborales (*The Independent*, 2014).

Los usuarios del ciberespacio en Singapur, y muy seguramente en otros países, vieron cómo los valores considerados correctos por un Estado fueron impuestos a un sistema o una plataforma de servicios cibernéticos. Así mismo, evidenciaron cómo estos se transformaron en políticas que los clientes tuvieron que aceptar para emplear sus productos y, eventualmente, poder interactuar. En tal sentido, los usuarios en Singapur que empleen los servicios de Google enfrentan la siguiente situación: aceptar los términos (i.e. no hacer expresiones de odio) para emplear el escenario que les permite constituir una comunidad virtual donde interactuar o, por el contrario, no hacerlo y verse obligados a buscar otro medio. (Siyuan & Chen-Wei, 2019).

El flujo de los *actores reguladores* tiene sus propias particularidades que deben distinguirse, y que el ejemplo de Singapur no desarrolla. En primera instancia, si bien la figura 1 muestra una relación jerárquica, el flujo no necesariamente es continuo; en otras palabras, la influencia puede provenir desde cualquiera de los niveles superiores al usuario, y no necesariamente tiene que pasar por todos los niveles para ser efectiva. Veamos a continuación algunos casos en los cuales esto se genera.

## 1. Flujo Directo Estado-Usuario

- En 2015, el ciudadano neozelandés Philip Blackwood fue sentenciado a dos años de cárcel y trabajos forzados en Myanmar por valerse de una imagen de Buda usando audífonos para promocionar un bar en su cuenta de Facebook. Aunque Facebook no consideraba esto una violación de sus "normas comunitarias o principios", para el país donde se

encontraba el usuario el acto fue tipificado como el delito de "irrespeto a la religión" (Associated Press & AFP, 2015).

- En 2017, dos ingleses fueron capturados en Tailandia por realizar *streaming* ilegales, con ánimo de lucro, de los partidos de la Champions League, a través de Cajas Kobi y de IPTV. Aunque el país asiático no es famoso por sus reglas hacia la propiedad intelectual —y eso no es diferente en sus prestadores de servicios cibernéticos—, la operación se hizo por la presión ejercida desde el gobierno británico. Prueba de dicha presión es que los individuos fueron eventualmente entregados a la embajada inglesa (BBC News, 2017).

## 2. Flujo directo plataforma/sistema-usuario

- Aunque los países tienen diferentes regulaciones frente a la protección de datos y de información personal, Alphabet Inc. —nuevo *holding* que contiene a Google— establece su propio criterio a los usuarios de cualquiera de sus servicios creando su propio conjunto de normas —componente de un sistema de valores—. En su sección de "Condiciones y privacidad" se lee textualmente:

Al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google [...] una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas [...] comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros Servicios. (Google, 2017)

- SERVNET es un sistema/plataforma de la *Dark Web* que tiene como función brindar *hosting* y encriptación, y diseñada principalmente para la Tor Network. Debido a su naturaleza, no es posible determinar a qué sistema legislativo se supedita SERVNET, pero establece una serie de normas para la prestación de su servicio a todos los escenarios cibernéticos y usuarios:

Network Security - You are not allowed to use this service for:

- » Spam, all forms of Email Abuse and Bulk Email related products
- » Background running programs (bots/daemons/monitors)

- » Unauthorized monitoring of data or traffic on any network or system without express authorization.
- » IP range scanning/port scanning/vulnerability scanning
- » Unauthorized access to or use of data, systems or networks, including any attempt to scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization.
- » The placement of material not deemed in good taste is not permitted such as CP - customer is held fully responsible for any misuse of account regardless of whoever published the content.
- » Distributed Denial of Service (DDoS) - No resources and servers may be used to perform any form of DDoS/DoS attacks. (Sevnet, s. f.)

### 3. Flujo directo escenario cibernético-usuario:

- Wordpress.org es una de las plataformas disponibles para el almacenamiento y el desarrollo de blogs. Aunque cada blog es una comunidad virtual independiente, Wordpress.org establece una serie de reglas que deben ser tomadas en cuenta, y las cuales no hacen referencia a ningún Estado en particular. Algunas hacen referencia a conceptos técnicos para el uso del correcto del servicio, mientras otras establecen una lista de contenido que no es permitido: *spam*, pornografía, publicar información personal, publicidad, violaciones a la propiedad intelectual...
- GALAXY 3 es una red social de la *Dark Web* que tiene como propósito conectar usuarios que quieran interactuar de manera anónima. Es soportada por el sistema/plataforma Elgg (elgg.org), pero no es posible determinar algún lugar geográfico que la vincule a leyes específicas —no tendría sentido si el propósito es tener anonimato en la *web*—. Aun así, GALAXY 3 establece las siguientes reglas para, como afirma, evitar que esta se convierta en un mercado situado en el foco de atención de las diversas agencias gubernamentales y de las fuerzas policiales, así como para evitar que se convierta en el blanco de tales agencias:
  1. No images of children. Including 3D or cartoon. Use your common sense, if in doubt ask before you post. DO NOT ask for these things either, you will be banned [...]
  2. No public commercial trade. We don't want Galaxy3 turning into a market place targeted by Government agencies [...]
  3. No pornographic

content and / or gore in public areas. Legal (18+) pornography / erotica and gore are allowed in closed groups [...] 4. Images and avatars are considered public content, so rule 1. and rule 3. apply [...] 5. No doxing or posting anything that may endanger someone [...] 6. Do not solicit members into committing a crime. This includes, but not limited to, hacking and carding requests [...] 7. Do not advertise criminal internet resources (clearnet or hidden) [...] 8. Be respectful. Galaxy is a respectful community, allowing Freedom of Speech. Harassment will get you banned [...] 9. Do not spam [...] 10. Do not scam [...] 11. Do not advertise extremist / terrorist material [...] 12. No public sex ads. This is not a dating site. (Galaxy 3, s. f.)

#### 4. Flujo directo comunidad virtual-usuario

- Actualmente existe una proliferación de grupos cerrados en Facebook que se diseñan con diversos propósitos: por ejemplo, compartir una pasión, tranzar bienes o servicios y establecer redes de apoyo. Dichos grupos, generalmente, tienen un administrador que establece las reglas de interacción y determina qué es o no realizable en la comunidad. Dichas reglas no necesariamente son un reflejo de Facebook o de las leyes de los Estados. Así, es común ver cosas como: "prohibido ofrecimientos por inbox", "publicaciones con fotos reales", etc.
- LOLIFOX es una comunidad de la *Dark Web* que permite crear *imageboards* —una especie de foro que opera, principalmente, haciendo uso de imágenes—. LOLIFOX establece una serie de reglas aplicables para todos los usuarios que hacen uso de sus *boards*. No es posible establecer una línea directa de influencia de otros *actores regulares*, por lo cual es posible suponer que las siguientes reglas son propias del administrador de LOLIFOX:
  - (1) Do not post child pornography or questionable 3DCG/3DPG/human dolls sexual depictions of children or child abuse[...] (2) Do not post wipe, spam, bypassing spam sheet, damage to the site and calls for it [...] (3) Bypassing the ban can lead to an increase in the ban period and removal of all posts [...]
  - (4) The user is personally responsible for the materials posted on the site and for compliance with the laws of the country in which it is located. (Lolifox, s. f.)
- DEVIL'S SKY-MARKT es un mercado en la *Dark Web* que funciona con *bitcoins*, y en el cual es posible hallar diferentes drogas (por ejemplo, cocaína, LSD, marihuana, heroína) y servicios de *malware* y *hacking*, así como elementos falsificados (por ejemplo, dinero, tarjetas de crédito, pasaportes, etc.).

A pesar de tener una naturaleza ilegal, el administrador demarca los bienes prohibidos que se vayan a tranzar: servicios de asesinato, venenos, armas de destrucción masiva, pornografía infantil o armas de fuego, y acciones que atenten contra la integridad de personas (i.e. *red romos*). De igual manera, establece unos comportamientos prohibidos para los usuarios, como, por ejemplo, subirse personalmente la calificación, o *rating*.

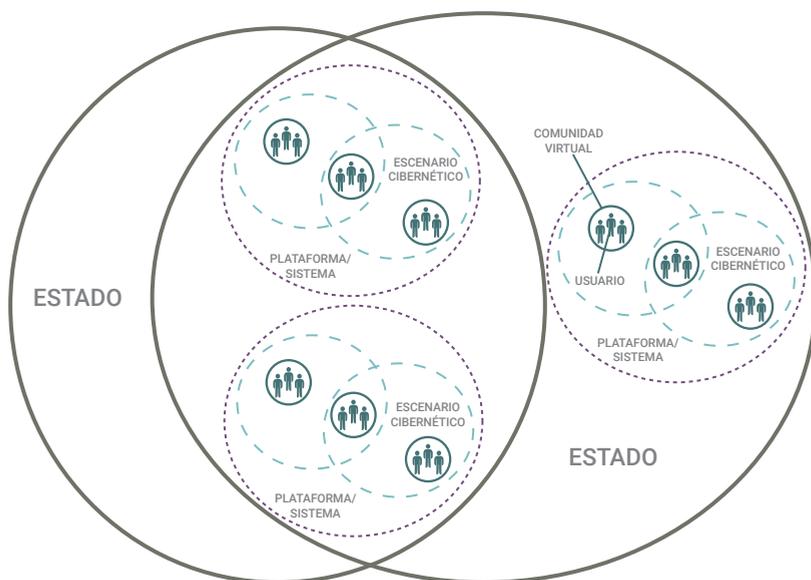
Las demás características del flujo de los *actores reguladores* que es necesario describir responden a los niveles de conciencia y de influencia, como se muestra en la figura 1. Centrado en la posición de los usuarios finales, la conciencia que estos tienen del poder comportamental que ejercen los *actores reguladores* sobre sus habilidades para realizar interacciones interciberespaciales tiene una tendencia a decrecer a medida que dichos usuarios se acercan más al Estado; no obstante, no puede afirmarse lo mismo de la relación entre *actores reguladores*. Los casos estudiados evidencian que estos, por lo general, conocen los sistemas de valores de quienes que se encuentran en un lugar superior en la jerarquía, lo cual explica por qué crean descargos de responsabilidad —en inglés, *disclaimer*—.

Es necesario profundizar en la explicación de la tendencia frente a la conciencia en el flujo de los actores reguladores. Aun así, la sociología nos brinda una pista: Foucault (1982) incita a pensar que identificamos con mayor facilidad los sistemas de valores de las estructuras con las cuales tenemos una interacción directa (por ejemplo, familia, colegio, amigos, clubes etc.), y tendemos a desconocer las que son más subjetivas; de ahí que sean pocas las personas que conocen las leyes que gobiernan al ciberespacio en cada país donde se encuentran, y menos aún, las que leen y cumplen los términos de un sistema/plataforma.

La característica final del flujo de los *actores reguladores* tiene que ver con el nivel de influencia o, en otras palabras, la magnitud de poder comportamental que son capaces de transmitir a otros actores y usuarios finales. El Estado es el actor que ejerce mayor influencia, y esta se va diluyendo para los otros actores en la medida en que se acercan al usuario final en la jerarquía descrita en la figura 1. De esa manera, y debido a la *desterritorialización*, los Estados solo podrán influenciar a quienes se encuentren en su territorio, salvo que haya alguna herramienta que brinde capacidades transnacionales. Así mismo, una plataforma/sistema solo podrá influenciar los escenarios cibernéticos bajo su control directo; los escenarios cibernéticos y a sus comunidades, y estas últimas, a sus miembros.

Existe, entonces, un límite a la influencia del poder comportamental que se manifiesta a modo de una frontera imaginaria, como se muestra en la figura 2. A pesar de ello, se debe tener presente que la manifestación simultánea de múltiples *actores reguladores* no implica que sus sistemas de valores sean excluyentes: por el contrario, pueden fácilmente darse los casos en los que estos se complementen, o en los que un *actor regulador* define cuál es el sistema que tiene mayor preponderancia. De igual forma, los actores pueden optar por esquemas de coinfluencia, a través de mecanismos de cooperación o entendimiento (i.e. *joint-ventures*, tratados, etc.).

**Figura 2.** Distribución de la influencia de los actores reguladores en el marco del poder comportamental.



**Fuente:** elaboración propia.

Facebook, en sus condiciones de servicio, hace la salvedad de que, debido a la existencia de múltiples productos, los cuales se comportan como escenarios cibernéticos delimitados, hay términos complementarios que pueden llegar a entrar en conflicto con su "Declaración de Condiciones (DDR)". Por tal razón, el sistema/plataforma afirma lo siguiente:

Puesto que Facebook ofrece una amplia gama de servicios, es posible que te pidamos que leas y aceptes condiciones complementarias aplicables a tu interacción con una aplicación, un producto o un servicio determinados. En caso de que esas condiciones complementarias entren en conflicto con esta DDR, las condiciones complementarias asociadas con la aplicación, el producto o el servicio prevalecerán en lo referente al uso de tales aplicaciones, productos o servicios en caso de conflicto. (Facebook, 2015)

Los Estados utilizan comúnmente los medios ofrecidos por las organizaciones internacionales para entablar mecanismos de cooperación. Los compromisos adquiridos o demostrados en los documentos de dichas organizaciones no contravienen, por ser un principio fundacional de estas, la soberanía de ninguno de sus miembros. En tal sentido, los sistemas de valores de los Estados coexisten paralelamente para lograr cierto grado de coinfluencia en el ciberespacio o, en otras palabras, proyectar de manera conjunta poder comportamental.

En el contexto del ciberespacio, la Organización de los Estados Americanos (OEA) tiene varios documentos que sirven para demostrar la afirmación anterior. Estos son: 1) *Declaración sobre Seguridad en las Américas de 2003*; 2) *Seguridad Multidimensional* (OEA/Ser.K/XXXVIII/ CES/dec.1/03 rev. 1); 3) *Adopción de una Estrategia Inter-americana para combatir las Amenazas a la Ciberseguridad* (AG/RES. 2004/XXXIV-O/04), y 4) *Declaración para el Fortalecimiento de la Ciberseguridad en las Américas* (OEA/Ser.L/X.2.12/ 7 March, 2012 CICTE/ DEC.1/12 rev. 1).

La *Declaración de Seguridad de las Américas*, de 2003, reconoce los incidentes en la seguridad cibernética como una amenaza no tradicional a los Estados. En la mencionada declaración los miembros se comprometen a enfrentar las manifestaciones de terrorismo y delincuencia en el ciberespacio, así como a desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética. La estrategia diseñada (AG/RES. 2004/XXXIV-O/04) urge, entre otros elementos, a que los Estados participantes establezcan e identifiquen los *Computer Security Incident Response Teams* (CSIRT). Tales compromisos se reafirman en la *Declaración para el Fortalecimiento de la Ciberseguridad*, de 2012.

Se debe tener presente que el poder comportamental no se circunscribe únicamente a las interacciones interciberespaciales persona-persona, sino que también cobija aquellas entre persona-sistema y sistema-sistema, lo cual significa que los estímulos, automatizados o no, tienen unos limitantes. Por ejemplo,

por más que un usuario quiera vulnerar un escenario delimitado, estos tendrán políticas que expresan directamente el comportamiento como indeseado. De forma similar, los sistemas de valores restringen las respuestas recíprocas a los estímulos de un actor. En otras palabras, un miembro de una comunidad virtual no debería esperar que otro responda inmediatamente de forma contraria a las reglas internas, incluso si es incitado.

Debe hacerse una última observación frente al poder comportamental, y es sobre la capacidad de los actores para resistir la influencia. Existen múltiples técnicas para hacerlo —esto será la temática del próximo capítulo, pero, dicho de forma superficial, es posible tomando la decisión de migrar, crear o destruir los escenarios donde se realizan las interrelaciones interciberespaciales—; sin embargo, al igual que como ocurre con el resto del modelo, cuanto más cerca se esté del Estado, tanto más difícil será. Por ejemplo, un usuario cansado de la forma como un administrador lleva la dinámica en un grupo de Facebook puede optar por salirse para buscar o crear uno nuevo y, de esa forma, hacer que la influencia del administrador desaparezca; no obstante, cambiarse de red social es más difícil, y aún más lo será encontrar un escenario cibernético que no se halle controlado por alguna de las grandes compañías de tecnología (por ejemplo, Facebook, Apple, Microsoft, Amazon, eBay o Alphabet).

En la *Dark Web*, la dinámica descrita se manifiesta de una forma muy similar, salvo por el comportamiento del Estado. Debido a los productos y los servicios ilegales que allí se transan —se debe mencionar que no todo lo que allí se transa o se hace es necesariamente ilegal—, los Estados son bastante agresivos en buscar el cumplimiento de sus sistemas de valores por parte de los demás *actores reguladores* y usuarios. Ello termina reflejándose en una mayor destinación de recursos para el ejercicio de la autoridad y en castigos más fuertes.

En términos de la concepción básica del “poder”-relación de “A” y “B”, el poder comportamental se traduce de la siguiente manera: un *actor regulador* (“A”) puede lograr que otro *actor regulador* de menor jerarquía, o usuario final (“B”), realice o no algo en el ciberespacio que guarda estrecha relación con un sistema de valores predefinido. Para ello, el sistema es acompañado de mecanismos de castigo y autoridad que pueden afectar, entre otros, la membresía. En cualquier caso, el poder comportamental de “A” sobre “B” termina influyendo las interacciones de “B”, así como las respuestas recíprocas de terceros a sus estímulos.

## El poder funcional en las interacciones interciberespaciales

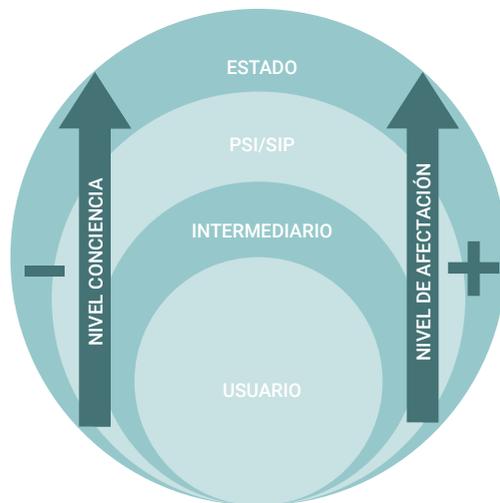
El ciberespacio depende de unos componentes materiales y tecnológicos para existir como un entorno intangible donde los usuarios pueden interrelacionarse (por ejemplo, redes, computadores, servidores, cableado, etc.). Quienes controlan y vulneran estos elementos tienen la facultad para determinar quiénes pueden interactuar y por cuánto tiempo, así como los resultados de algunas interacciones. La facultad descrita es denominada por este libro *poder funcional* y, al igual como ocurre con el comportamental, tiene una serie de *actores reguladores* con su respectivo flujo de influencia y su respectivo nivel conciencia. Dichos actores son: Estados, proveedores de servicio de internet (PSI) e intermediarios.

En el capítulo segundo se desarrolló la manera como los Estados ejercen soberanía sobre el componente físico del ciberespacio que se encuentra en sus territorios, según se ve en la figura 3. En dicho capítulo se sugirió que los Estados, como lo evidenciaba el caso del “Gran Firewall de China”, tienen la facultad de limitar acceso al ciberespacio y controlar su contenido para todos los usuarios que se hallen sujetos al sistema jurídico nacional. La misma idea fue ampliada en el poder comportamental, y ahora es necesario retomarla para entender el poder funcional.

En la mayoría de los países existen normatividades que reafirman el absoluto dominio del Estado sobre todo lo que tiene que ver con las telecomunicaciones en el interior de sus fronteras. Y como la mayoría de estos no tienen la capacidad o los recursos para satisfacer autárquicamente la necesidad, también establecen los procedimientos y las contraprestaciones para ceder a empresas privadas la prestación del servicio. De esa forma, la primera manifestación del poder funcional es la potestad del Estado para determinar quiénes pueden brindar acceso al ciberespacio, así como las reglas generales para hacerlo; en otras palabras, para seleccionar los actores reguladores en el nivel PSI, tal cual se muestra en la figura 3.

En Colombia se estableció la Ley 1341 de 2009, por la cual se definen los principios y los conceptos sobre la sociedad de la información y organizaciones de las TIC. En su artículo 10, se habilita de forma general la provisión de redes y servicios de telecomunicaciones, el cual se reconoce como un servicio público, bajo la titularidad del Estado, a terceros que quieran hacerlo a cambio de una contraprestación periódica. Ello se ve complementado por el Decreto 1078 de 2015, que obliga a todos los posibles interesados a tener un *Registro TIC* para facilitar el control estatal.

**Figura 3.** Establecimiento de los flujos del poder funcional, según los autores reguladores



**Fuente:** elaboración propia.

La segunda manifestación del poder funcional desde el Estado es la prohibición expresa de acceso a internet en ciertos lugares y nichos poblacionales. Canadá, por ejemplo, prohíbe el uso de internet en sus cárceles provinciales y federales para los prisioneros. Estados Unidos, por el contrario, tiene un sistema altamente monitoreado que permite un acceso restringido a sus presidiarios a correos electrónicos (i.e. *Trust Fund Limited Inmate Computer System*), así como internet para fines de educación y reintegración.

La tercera manifestación del poder funcional del Estado es, como en el caso de China, su habilidad para manipular y denegar cierta información a los usuarios del ciberespacio a partir de consideraciones en sus sistemas de valores. Esto último, en los términos del primer capítulo, significa que los estímulos de los usuarios solo tendrán las respuestas recíprocas esperadas, no por ellos, sino por un tercero aparentemente exógeno a la interacción (por ejemplo, búsquedas de Taiwán en China). Esta última manifestación pone sobre la mesa, y de manera evidente, la relación que hay entre ambos tipos de poder.

El poder funcional y el poder comportamental son independientes, pero se hallan estrechamente relacionados. El primer tipo de poder afecta directamente al ciberespacio como entorno, y tácitamente, a los actores reguladores y usuarios finales. El segundo tipo, por el contrario, afecta particularmente a los actores

y usuarios, sin que ello implique algún tipo de influencia sobre el ciberespacio. Aun así, el poder funcional se alimenta del sistema de valores central del comportamental para justificar su aplicación; es decir, para encontrar un argumento que permita dictar los términos de conectividad al ciberespacio y el acceso a información. Miremos una analogía que nos permita entender esto mejor:

Imaginemos un bar exclusivo que brinda el lugar perfecto para interactuar. En la entrada de este se encuentra un individuo del personal encargado de brindar seguridad, así como de permitir y cobrar el ingreso a otras personas. Supongamos que al personal de seguridad se le han dado unos criterios para controlar la admisión: solo mayores de edad, uso de traje formal, 50 dólares por persona y hasta las 2:00 a. m. Adicionalmente, y una vez dentro, se espera que los clientes tengan un comportamiento enmarcado dentro de las reglas fijadas por la administración.

El personal de seguridad está empleando poder funcional cuando configura la naturaleza del bar, y cuando determina quiénes pueden entrar o no, así como el tiempo de permanencia. Quienes se encuentran afuera solo podrán interactuar con los demás clientes si superan, a través del cumplimiento de los requisitos de ingreso, la infraestructura física que conforma al bar, y que funge como barrera (i.e. paredes, ventanas y puertas). Una vez adentro, el sistema de valores del establecimiento entra en acción ejerciendo poder comportamental sobre todos los presentes, y configurando lo que se puede o no se puede hacer, al igual que las formas para ello. Las personas que no acepten o violen el sistema de valores podrán ser expulsadas del lugar.

En la analogía, el entorno donde las personas se encuentran interactuando, lo que entendemos abstractamente como "bar", es el ciberespacio. La mesa, las paredes, los asientos, la barra, la música, los aromas y los demás componentes que hacen posible la concepción de un "bar" equivalen a la infraestructura física y digital del ciberespacio. Las reglas impuestas por la administración a sus clientes son similares a los sistemas de valores que proyectan los *actores regulares*; en este caso, una comunidad virtual. Y la función que cumple el personal de determinar el ingreso y la permanencia de los clientes es, como veremos a continuación, análoga a la de un proveedor del servicio de internet.

Ahora bien, supongamos que a la puerta del bar llega alguien que cumple con los criterios de ingreso, pero viene en estado de embriaguez. El personal de seguridad puede optar por restringirle a dicha persona el acceso al establecimiento argumentando que tiene la capacidad potencial para violentar las reglas

de comportamiento fijadas por la administración. En tal sentido, el poder funcional se alimenta del sistema de valores del poder comportamental. Un equivalente en el ciberespacio es cuando China bloquea las búsquedas en internet relacionadas con Tiananmen porque contradicen la lectura oficial de los hechos y, por ende, pueden poner en peligro la unidad de la nación.

No solo los Estados ejercen poder funcional en el ciberespacio: todos los que tengan privilegios y control sobre la infraestructura física y su configuración podrán hacerlo. Los PSI, de hecho, ejercen tal tipo de poder sobre sus usuarios. Al controlar los servidores de conexión, ellos determinan quiénes pueden acceder al ciberespacio, su velocidad de conectividad y el tiempo disponible.

Supongamos que un usuario quiere ver todas las temporadas disponibles de la serie de moda en su computador, vía *streaming*. Para ello, el usuario contrató por un mes con un PSI una suscripción prepagada a internet que le brinda 1MB de velocidad real; sin embargo, debido a la longitud y el número de capítulos, requeriría al menos dos meses para satisfacer completamente su interés. Al comenzar el proceso de *streaming*, el usuario se da cuenta de que la velocidad de su servicio detiene constantemente la reproducción, y hace casi imposible disfrutar la serie.

En términos del poder funcional e interacciones en el ciberespacio, la situación hipotética del *streaming*, bastante común de por sí, se traduce de la siguiente forma: el individuo hace un estímulo al sistema que almacena la serie, del cual obtiene la respuesta recíproca esperada, pues evidencia cómo el video carga en su computador; no obstante, el ancho de banda que el PSI le permite tener (i.e. 1 MB) constriñe el nivel de respuesta del sistema, y eso lleva a que el interés del individuo se vea afectado. Así, las condiciones del PSI, las cuales representan sus posturas económicas como prestador del servicio, establecen unas condiciones —en tiempo y modo— que enmarcan el ciberespacio donde nuestro individuo pretende interactuar.

Otra manifestación del poder funcional que permite ilustrar cómo un actor diferente del Estado delimita al ciberespacio para otros, desde el contenido y la información, ocurre cuando tenemos conexión de cortesía en algún establecimiento. Cuando llegamos a un lugar comercial o público, y hacemos uso de su Wifi, es común someterse a un cronómetro que indica el uso gratuito de conexión, diferentes procesos de registro y autenticación, *banners* de propaganda y un sistema de control parental. Dichos elementos influyen enormemente las formas como interactuamos, al igual que las razones para hacerlo.

Seguramente, muchos de nosotros hemos utilizado el Wifi de un aeropuerto donde se nos indica que tenemos "30 minutos gratis de internet", pero pocos hemos analizado lo que sucede bajo el lente del poder. Lo primero que ocurre es que aceptamos develar nuestra identidad, y, por la premura del tiempo, asumir un ritmo acelerado. Subsecuentemente, nos vemos forzados a ver contenidos que no esperamos o no deseamos (por ejemplo, propagandas), porque es una exigencia para completar el proceso de conexión. Y, finalmente, una vez logrado el acceso, debemos ajustar lo que podemos hacer al sistema de filtro de la red. Así, sucede que muchas veces terminamos llenos de *e-mail* promocionales, pese a no haber podido lograr nuestro cometido durante esos valiosos 30 minutos.

En el poder funcional, el flujo de influencia y el nivel de conciencia se comportan de manera similar a como sucede en el poder comportamental. Así, el nivel de afectación o de influencia puede ir desde un individuo en particular hasta toda una comunidad; el tamaño dependerá del nivel de control que un actor tenga sobre la infraestructura y la configuración del ciberespacio. De igual forma, es muy raro que un usuario final tenga completo conocimiento de las medidas tomadas por un Estado o PSI, y de la manera como estas influyen en sus interacciones interciberespaciales.

Ahora bien, el poder funcional, a diferencia del comportamental, es más susceptible a la intervención de actores exógenos que no hacen parte del flujo como *actor regulador* que se ilustró en la figura 3. Por ejemplo, un *hacker* o un Estado pueden fácilmente vulnerar la accesibilidad, los componentes físicos y digitales y el contenido del ciberespacio en otro territorio, y así afectar directamente las interacciones interciberespaciales; sin embargo, raro sería que estos pudiesen influenciar el sistema de valores, y en consecuencia, tácitamente, el comportamiento de los usuarios finales.

La resistencia del poder funcional dependerá de si el *actor regulador* hace parte del flujo descrito, como se ve en la figura 3, o de si, por el contrario, es un tercero exógeno a la relación de influencia. En el primer caso, en la relación usuario-intermediario, el poder se agota cuando el usuario decide encontrar otra fuente de conexión, y el intermediario, no prestar el servicio; sin embargo, hacer lo mismo respecto a un PSI es más difícil y tomará más tiempo, pues en ello intervienen variables como la oferta existente, las políticas de la compañía y los recursos financieros del usuario para cambiar el servicio. Finalmente, si el Estado es el que está condicionando al ciberespacio, superar su influencia es, para alguien sin conocimiento técnico avanzado, algo imposible.

Cuando la fuente del poder funcional es un actor exógeno, la resistencia a la influencia se transfiere al dominio de la ciberseguridad o ciberdefensa. En tales casos, el objetivo es evitar, por los medios y las técnicas necesarios, que ese actor controle los términos de conexión y de contenido disponible. En este campo es posible hablar de la triada de la seguridad de la información (i.e. disponibilidad, confidencialidad e integridad), al igual que de conceptos relacionados con el servicio (i.e. accesibilidad, redundancia, resiliencia, entre otros).

En términos de la concepción básica del "poder"-relación de "A" y "B", el poder funcional se traduce de la siguiente manera: un actor regulador ("A") puede lograr que otro actor regulador de menor jerarquía, o usuario final ("B"), tenga o no acceso al ciberespacio, o visualice cierta información. En tal sentido, el actor "A" configura el tipo del ciberespacio al que "B" puede acceder, así como las formas y los modos para hacerlo. Para ello, "A" depende del control que pueda ejercer sobre la infraestructura tecnológica y física del entorno intangible, así como de los argumentos que le permitan crear los sistemas de valores. El poder funcional de "A" sobre "B" termina influyendo en las interacciones de "B", en el sentido de que determina cuándo pueden realizarse, así como las respuestas recíprocas de terceros a sus estímulos.

## Lecciones

- La aparición de *actores reguladores* desvirtúa la concepción del ciberespacio como un lugar donde reina la anarquía. A decir verdad, existen múltiples sistemas de valores jerarquizados que coexisten, y constituyen así un intrincado conjunto de criterios que influyen directamente la manera como los usuarios realizan interacciones interciberespaciales, al igual que las respuestas recíprocas y los estímulos llevados a cabo.
- El poder comportamental constituye la manera como los actores reguladores proyectan sus sistemas de valores en el ciberespacio, en un fenómeno que se comporta como un flujo descendente. El sistema de valores delimita qué, cómo y dónde los actores reguladores, según la jerarquía y los usuarios, pueden "*HACER*" en el ciberespacio.
- Los actores reguladores identificados para el poder comportamental son, en orden descendente: 1) el Estado, centro del sistema social moderno; 2) las plataformas/sistemas, proveedores de los escenarios cibernéticos delimitados donde ocurren las interacciones; 3) los escenarios

cibernéticos delimitados, o servicios cibernéticos que permiten la interacción, y que contienen más de una comunidad virtual; 4) la comunidad virtual, o asociación de usuarios, con o sin identidad diluida, que conviven e interactúan por o para un fin común en particular.

- El poder funcional es la habilidad de un actor para dictar los términos de conectividad al ciberespacio, así como el acceso a información; incluso, si es en detrimento de otros. Este determina, entonces, cuándo los usuarios pueden *usar* el ciberespacio y, por ende, interrelacionarse. Así mismo, influyen lo que estos pueden **encontrar** en el dominio intangible, de modo que fungen como una especie de modelador.
- Al igual que como ocurre con el poder comportamental, el funcional también tiene una serie de *actores reguladores* que se comportan jerárquicamente. Estos son, en orden descendente: 1) El Estado, centro del sistema social moderno, y quien controla los derechos de conexión en un territorio determinado; 2) los PSI, encargados de la distribución del servicio de internet desde el *backbone* hasta el usuario final, y 3) el intermediario, o prestador de servicio a internet temporal para el usuario final.
- El poder funcional y el poder comportamental existen entre todos los tipos de actores mencionados en capítulos anteriores. La forma como se manifiestan puede ser distinta, pero se hallan igualmente presentes entre la legalidad y la ilegalidad.
- En ambos tipos de poder, el comportamental y el funcional, el nivel de influencia será más fuerte cuanto más cerca del Estado se halle la fuente. De igual forma, y de manera inversa, el nivel de conciencia decrecerá mientras más lejos se halle la fuente del usuario final. Cuando el nivel de conciencia es alto, es posible hablar de un poder comportamental o funcional de naturaleza directa, y cuando la relación se invierte, se está ante un carácter tácito.
- El cumplimiento de la influencia que emana de ambos tipos de poder viene acompañado de mecanismos de autoridad y de castigo. Estos serán tanto más drásticos —entendido ello como capaces de afectar la integridad física o jurídica de un actor regulador o usuario final— cuanto más alto sea el nivel de influencia.
- Existen diferencias fundamentales entre los poderes comportamentales y los funcionales. En primer lugar, el funcional es más susceptible de sufrir injerencias de terceros actores exógenos a la relación de poder

visualizada en el flujo. Cuando ello ocurre, estamos ante un incidente de ciberseguridad o ciberdefensa. Y en segundo lugar, la desterritorialización y la dilución de la identidad pueden servir para superar la influencia del Estado en cuanto a lo comportamental, pero no en cuanto a lo funcional. No todos los actores tienen los medios ni los conocimientos para controlar su conexión sin estar sujetos a la jurisdicción territorial de un Estado, lo cual es mucho más complejo para quienes se mueven entre la ilegalidad.

## Capítulo 4

# La sorpresa y el poder en las relaciones interciberespaciales\*

DOI: <https://doi.org/10.25062/9786287602137.04>

**Steven Jones-Chaljub**

Escuela Superior de Guerra "General Rafael Reyes Prieto"

**Citación APA:** Jones-Chaljub, S. (2022). La sorpresa y el poder en las relaciones interciberespaciales. En Jones-Chaljub, S., *Conceptualización del ciberespacio humano* (pp. 79-93). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602137.04>

### 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.

Los actores del ciberespacio son incapaces de tener una plena certeza sobre lo que sucede en el interior de ese entorno, lo cual es singular si se considera que es el único dominio hecho y controlado por el hombre. La razón de esta inhabilidad se desprende de las características del ciberespacio (i.e. desestatalización, dilución de la identidad, desterritorialización e hiperconexión), las cuales, por permitir la interacción de múltiples actores a distancias y velocidades increíbles, sin que exista un verdadero control sobre la identidad, configuran el escenario perfecto para la incertidumbre. Esta incertidumbre, cuando la analizamos más a fondo, tiene una gran semejanza con el impacto psicológico que los doctrinarios, tanto legales como ilegales, atribuyen al “elemento sorpresa”; al menos, así lo demuestran los distintos documentos que se encuentran disponibles para quien sepa buscar (por ejemplo, *Security Paper on the Art of Anti Detection-3*; *Assassin V1.4 User Guide*; *Guía Introductoria Para la Seguridad en Momentos de Inestabilidad Social de Anonymous*, y todos los disponibles en *Vault 7*).

Si en el ciberespacio reina la incertidumbre, y esta guarda mayor relación con la sorpresa, entonces vale la pena preguntarse cómo se manifiesta la sorpresa, cuál es su importancia y qué límites tiene su aplicación en las interacciones interciberespaciales. La razón de indagar es sencilla. La historia nos ha demostrado el valor que ha tenido la sorpresa para zanjar relaciones distributivas que escalan a niveles de conflicto directo dentro del marco del “mundo material”. Ahora bien, dado que el ciberespacio es considerado el quinto dominio estratégico, y que está profundamente arraigado en las sociedades modernas, no existen argumentos para restarle importancia al análisis.

En su empleo durante un contexto distributivo, el “elemento sorpresa” se presta, como se verá más adelante, para afectar las relaciones de poder, al igual que los medios y los modos empleados en ellas. El poder en las relaciones interciberespaciales se manifiesta, de acuerdo con las aproximaciones de este libro,

de una manera *comportamental* y otra *funcional*. La primera describe la forma como se influencia el comportamiento de los usuarios desde el cumplimiento de un sistema de valores predefinido por un conjunto de “actores reguladores”, mientras que la segunda hace alusión a cómo se puede delimitar al ciberespacio, desde lo tecnológico, para afectar las interacciones de los actores y sus resultados recíprocos.

El objetivo de este capítulo es desarrollar teóricamente el “elemento sorpresa”, al igual que analizar la manera como este se emplea, se manifiesta y se comporta en las relaciones de poder comportamental y funcional propias de las interacciones interciberespaciales. De manera anticipada, se pudo entrever que la sorpresa tiene la habilidad para ser un elemento que potencia o debilita las relaciones de poder, pero ello dependerá de la categoría y de la posición del sujeto sobre quien recae el análisis (i.e. recipiendario o ejecutor).

## La sorpresa

La “sorpresa” es uno de los principios fundamentales del ejercicio del poder, independientemente de si ella se manifiesta en la esfera económica, en la política, en la social o en la militar. Esta —al menos, cuando se revisan los textos clásicos— se da por sobreentendida para el lector, y su utilidad solo se destaca para el estratega o mencionando los factores que la hacen posible. Dicha deficiencia en información se ve subsanada en los documentos doctrinarios donde los diferentes ejércitos del mundo establecen sus “principios de la guerra”, como se muestra en la tabla 4.

**Tabla 4.** Definiciones de sorpresa

AUTOR	OBRA	DEFINICIÓN
Von Clausewitz ([2007], s. f.).	<i>On War</i>	“Surprise therefore becomes the means to gain superiority, but because of its psychological effect it should also be considered as an independent element [...] Basically surprise is a tactical device, simply because in tactics time and space are limited in scale. Therefore in strategy surprise becomes more feasible the closer it occurs to the tactical realm, and more difficult, the more it approaches the higher levels of policy [...] The two factors that produce surprise are secrecy and speed”.

AUTOR	OBRA	DEFINICIÓN
Sun Tzu ([1963], s. f.).	<i>El arte de la guerra</i>	"El arte de la guerra se basa en el engaño. Por lo tanto, cuando es capaz de atacar, ha de aparentar incapacidad; cuando las tropas se mueven, aparentar inactividad. Si está cerca del enemigo, ha de hacerle creer que está lejos; si está lejos, aparentar que se está cerca. Poner cebos para atraer al enemigo [...] Ataca al enemigo cuando no está preparado, y aparece cuando no te espera. Estas son las claves de la victoria para el estratega [...] Cuando se entabla una batalla de manera directa, la victoria se gana por sorpresa [...] Solo hay dos clases de ataques en la batalla: el extraordinario por sorpresa y el directo ordinario, pero sus variantes son innumerables [...] Sirvete de una unidad especial para engañar al enemigo atrayéndole a una falsa persecución, haciéndole creer que el grueso de tus fuerzas está muy lejos; entonces, lanzas una fuerza de ataque sorpresa que llega antes, aunque emprendió el camino después" (traducción no oficial del autor).
Miyamoto Musashi ([2014], s. f., p. 88).	<i>El libro de los cinco anillos</i>	"La perturbación sucede en cualquier clase de cosas. Una de las formas en que sucede es a través del sentimiento de estar bajo una aguda presión. Otra es a través del sentimiento de una fuerza irracional [...] Una tercera forma es a través del sentimiento de sorpresa ante lo inesperado. En la ciencia militar a gran escala, es fundamental producir perturbación. Es esencial atacar resueltamente, mientras sus mentes están perturbadas, aprovechad esto para tomar la iniciativa y ganar".
Anónimo (Yuan, 2013, pp. 42,62).	<i>Las 36 estrategias chinas</i>	"Estrategia 6. Fingir ir hacia el Este mientras se ataca por el Oeste [...] Estrategia 8. Aparentar tomar un camino cuando se entra a hurtadillas por otro".
Foch ([2007], 1903, pp. 230-232).	<i>The Principles of War</i>	"La sorpresa consiste en el frío hecho de que el enemigo repentinamente aparece en considerables números, sin que su presencia haya sido conocida con suficiente antelación, y sin que haya sido posible organizar adecuadamente la defensa".
Fuller (1926, pp. 272-273).	<i>The Foundations of the Science of War</i>	In war surprise is omnipresent [...] Surprise should be regarded as the soul of every operation. It is the secret of victory and the key to success [...] The object of surprise is to attack the will of the enemy by accentuating fear [...] a man who is whose mind is dominated by fear is a man in panic, consequently the ultimate end of surprise is to reduce our enemy to a condition of panic in which his moral is totally replaced by his instinct of self-preservation in the most irrational form [...] the means of surprise are: superior direction, superior determination and superior mobility.

AUTOR	OBRA	DEFINICIÓN
Mao Zedong (2007 [1937]).	<i>On Guerrilla Warfare</i>	"Although the element of surprise is not absent in orthodox warfare, there are fewer opportunities to apply it than there are during guerrilla hostilities. In the latter, speed is essential. The movements of guerrilla troops must be secret and of supernatural rapidity; the enemy must be taken unaware, and the action entered speedily [...] The basic method is the attack in a violent and deceptive form".
UK Ministry of Defense (2014, p. 50).	<i>UK Defence Doctrine Joint Doctrine Publication 0-01 (jdp 0-01)</i>	"Surprise is the consequence of confusion induced by deliberately or incidentally introducing the unexpected".
Antigua Unión Soviética (US Army, 1984, Sección 2-2).	<i>Fm 100-2-1: the soviet army: operations and tactics</i>	"Achieve surprise whenever possible. Military operations must be characterized by decisiveness and aggressiveness. Forces must strive continuously to seize and to hold the initiative".
Estados Unidos de América (US Army, 1993, Sección 2-5).	<i>U.S. Army Field Manual: Operations (FM 100-5)</i>	"Strike the enemy at a time or place or in a manner for which he is unprepared. Surprise can decisively shift the balance of combat power. By seeking surprise, forces can achieve success well out of proportion to the effort expended [...] The enemy need not be taken completely by surprise but only become aware too late to react effectively [...] Deception can aid the probability of achieving surprise".
Colombia (FF. MM. de Colombia, 1997, pp. 20-21).	<i>Manual de Estrategia Militar General (3-4)</i>	"Principio de Sorpresa: la sorpresa es un medio de quebrar la energía moral del adversario, y privarlo de la facultad de reflexionar con serenidad, sobre el empleo de su poder de combate, por medio de acciones imprevistas por el enemigo, o el uso de nuevas armas o instrumentos de combate [...] la sorpresa completa será aquella en que el enemigo ignore cuándo y dónde será aplicada".

**Fuentes:** relacionadas en tabla.

A pesar de las diferencias entre clásicos y modernos, es posible identificar entre ellos características comunes que atañen a la "sorpresa": objetivo, impacto psicológico y relación con el engaño. De las definiciones presentadas en la tabla 4 surge, a manera de común denominador, que el empleo de la sorpresa tiene como objetivo lograr una ventaja o un cambio favorable en una situación particular que implique a otro actor, lo cual se logra por medio del impacto psicológico en el adversario y su *desacomodación*.

En el ámbito de la sorpresa, de manera muy similar a como ocurre con el terrorismo y las comunicaciones estratégicas, el impacto psicológico busca generar miedo para que el otro sea más vulnerable a cometer errores que le resulten costosos. La desacomodación, por el contrario, tiene como finalidad despojar al adversario de los elementos que le resultan ventajosos (por ejemplo, terreno, tiempo, etc.), para llevarlo a un contexto menos favorable donde, por no tener un curso de acción preparado, las opciones de comportamiento se reduzcan a la improvisación o la rendición. De igual manera, para que la sorpresa logre el resultado esperado debe estar acompañada por el engaño, y esa, por su parte, es la facultad para hacer creer al otro algo que no es cierto, y así generarle una percepción distorsionada de la realidad.

Las condiciones o los elementos comunes listados, al ser estados de la mente humana, abren la puerta para cuestionar su duración, porque, como dice el viejo adagio, nada es para siempre. Los estados de consternación psicológica, desacomodación y engaño que son causados en el otro para generar el "elemento sorpresa" están condicionados en el tiempo, y es que si no lo fueran se estaría despojando a la contraparte de la posibilidad de sobreponerse y responder. Un ejemplo icónico del empleo de la sorpresa en la historia militar contemporánea es el desembarco de Normandía, el 6 de junio de 1944, también conocido como el Día D (Beavor, 2009).

Durante la Segunda Guerra Mundial, los países Aliados decidieron realizar una operación sorpresa que les permitiese adquirir un punto geoestratégico en el territorio francés dominado por las FF. MM. nazis. Para lograr el desembarco con la menor resistencia posible, las fuerzas aliadas constituyeron operaciones y planes de fachada (por ejemplo, las operaciones Bodyguard y Fortitude), para, con la ayuda de la inteligencia, llevar a los alemanes a pensar que la invasión se desarrollaría en julio del mismo año, pero en el estrecho de Calais, Francia. Aunque los nazis fueron engañados, las fuentes históricas aseguran que Normandía, como punto de inflexión de la guerra, fue el resultado no de la incapacidad de los alemanes para reaccionar a la sorpresa, ni de un estado perpetuo de estupor, sino de la mala ejecución y el exceso de confianza de Hitler en su propio proceso de reacomodación (Beavor, 2009).

Un ejemplo adicional en la historia militar que demuestra cómo la sorpresa tiene un efecto transitorio, y que la ventaja adquirida por esta no necesariamente lleva a una victoria absoluta, fue la guerra de Yom Kippur, en 1973, también conocida como la guerra de Octubre, o la guerra de Ramadán, entre Israel y varios Estados

árabes (i.e. Egipto, Siria, Jordania, Iraq, Arabia Saudita, Libia, Túnez y Argelia). La primera incursión árabe se dio por parte de Egipto y Siria, durante el mes del *Yom Kippur* (judío), o *Ramadán* (musulmán); este es un periodo sagrado, en el cual el empleo de la violencia es moral y religiosamente condenado. Aprovechando que los israelíes estarían ocupados en sus celebraciones religiosas, los países árabes atacaron posiciones de dicho país en los altos del Golán y la península del Sinaí, las cuales habían sido ocupadas luego de la guerra de 1963 (Rabinovich, 2005).

Sin duda alguna, la ofensiva árabe tomó por sorpresa a los israelíes; sin embargo, estos pudieron responder rápidamente el avance hasta contener la amenaza en ambos frentes. El escalamiento de las hostilidades y la intromisión de las superpotencias del momento (i.e. Estados Unidos y la Unión Soviética) terminaron en un cese del fuego y, eventualmente, en la firma de un acuerdo de paz entre Israel y Egipto que aún se mantiene: los Acuerdos de Camp David, de 1978 (Rabinovich, 2005). El éxito de los países árabes, algo que es irrefutable, excepto para unos pocos, se debió no solo al tiempo en que ocurrió el ataque, sino a las señales contradictorias que fueron enviadas a la inteligencia israelí.

Los ejemplos de Día D y la guerra de Yom Kippur, así como ocurre con las emboscadas en la guerra de guerrillas, demuestran que los efectos de la sorpresa duran proporcionalmente al tiempo que requiere el otro para acomodarse a la situación y responder. Mientras más se tarde un actor en reaccionar o en reacomodarse de forma efectiva, más ventaja podrá obtenerse del elemento sorpresa; sin embargo, ello dependerá de la disponibilidad de recursos, del nivel de preparación y del direccionamiento que brinde el liderazgo. Adicionalmente, y una vez el otro se ha recuperado, la sorpresa se esfuma y da paso a otras maneras de proceder: desescalamiento, confrontación directa o retirada, entre otros.

La sorpresa guarda una relación directa con el poder; la sorpresa es un multiplicador de los medios empleados para la adquisición, el control y el ejercicio de este; puede aumentar considerablemente las garantías de éxito y es empleada tanto por los débiles como por los fuertes. En el caso de la Segunda Guerra Mundial, el esfuerzo militar del desembarco en Normandía fue potencializado por la ventana de oportunidad generada por la sorpresa, lo cual permitió a los Aliados hacer frente a una fuerza mayor y que se hallaba en una posición ventajosa; sin embargo, dentro del marco del mismo conflicto, existen múltiples registros de que las fuerzas nazis, consideradas dominantes, usaron la sorpresa para sobrellevar obstáculos: algunos de ellos son la táctica de *Blitzkrieg* y el franqueo de la Línea Maginot a través de Bélgica.

En el caso de la guerra de Yom Kippur, la coalición árabe empleó una combinación de sorpresa y engaño que le permitió ser, al menos temporalmente, más efectiva que las FF. MM. israelíes, las cuales nunca habían sido derrotadas en un conflicto simétrico (por ejemplo, las guerras de 1948, 1956 y 1967). De esta forma, los árabes vieron su poder militar potenciado por medio de la sorpresa, algo similar a lo que vivieron los israelíes años después, cuando bombardearon las instalaciones nucleares del régimen de Assad en Siria.

Ni la sorpresa ni sus elementos listados son exclusivos del “mundo real”: esta es ampliamente utilizada en el ciberespacio. La siguiente sección desarrollará, empleando los conceptos ya desarrollados por este libro, cómo la sorpresa se manifiesta, se emplea y se comporta en las interacciones interciberespaciales. De igual manera, el análisis se extenderá a las relaciones de poder —comportamental y funcional— que se gestan en el interior de ciberespacio.

## La sorpresa en el ciberespacio

Era mayo de 2000, cientos de personas comenzaron a recibir en sus correos personales y empresariales un mensaje que decía “*kindly check the attached LOVELETTER coming from me*”. Este era el comienzo de uno de los *malware* más famosos en la historia: el virus ILOVEYOU, el cual tenía como patrón de propagación el autoenvío a todos los contactos en la lista de correos, para, posteriormente, reemplazar diferentes archivos del sistema que hacían al computador inoperable e imposible de iniciar (Panda Security, 2013).

Lo interesante de ILOVEYOU, la razón por la cual se volvió icónico, no fue emplear una vulnerabilidad desconocida para los fabricantes de Windows, sino apoyarse completamente en la ingeniería social y el engaño para operar y propagarse a escala mundial. Por un lado, el archivo adjunto que contenía el *malware*, bajo el nombre de “LOVE-LETTER-FOR-YOU.txt.vbs”, se hacía pasar por un archivo de texto inocuo —los archivos “.txt” por sí solos no son capaces de ejecutar comandos—. Por otro, los mensajes en el cuerpo de los correos buscaban tentar al usuario, bien fuere por curiosidad genuina o por incredulidad, a abrir el archivo adjunto, que, como indica la terminación “.vbs”, correría los *scripts* que generarían el daño en el sistema.

La forma como ILOVEYOU se comportó y procedió es un símil moderno de la estrategia desarrollada en la Antigüedad por los griegos para tomarse, por medio de un caballo gigantesco de madera que explotaba la curiosidad y la

superstición de la contraparte, la ciudad de Troya. Adicionalmente, el éxito de este *malware* sirvió como inspiración para futuros desarrollos que aprovecharían, como se asevera constantemente en distintos escenarios y en la literatura, el eslabón más débil del ciberespacio: el componente humano. Finalmente, a la pregunta de si este virus tenía los componentes que se requieren para conformar un “elemento sorpresa”, la respuesta es que sí, pero su manifestación no es homogénea a lo largo de toda la lista de víctimas.

ILOVEYOU desató una ola de preocupación generalizada en los diferentes gobiernos del mundo. Si bien el virus, desarrollado en Filipinas, aparentemente no tenía una motivación política o económica, los daños causados por este fueron catastróficos tanto financiera como operacionalmente. Según el testimonio GAO/T-AIMD-00-181, realizado días después de la propagación de ILOVEYOU, por Jack L. Brock (2000), director de Defensa de los Sistemas de Información del Departamento de Estado de los Estados Unidos, ante la Oficina del Fiscal General, ILOVEYOU generó daños superiores a los 10 billones de dólares a compañías, instituciones y gobiernos en todo el mundo (por ejemplo: AT&T, Ford Motor Company, *Washington Post*; Dow Jones, *ABC News*, el Fondo Monetario Internacional y el Parlamento inglés). El impacto en la población no fue menor: hubo un estado de consternación generalizado que se entremezclaba con el temor a abrir cualquier tipo de correo electrónico (Brock, 2000).

El último elemento de la sorpresa presente en ILOVEYOU es la desacomodación. El impacto psicológico que generó el virus, causado por su rapidez y su forma de propagación, llevó a la mayoría de los gobiernos a emitir una orden de desconexión generalizada de sus computadores, a la espera de un parche para Outlook por parte de Windows. La decisión de apagar sus sistemas puede ser considerada un acto improvisado de contención —comportamiento similar al ocurrido en 2017 con el *Ransomware Wannacry*—. El efecto de desacomodación viene como consecuencia del cese de las actividades cotidianas de las organizaciones para crear e implementar, con la mayor brevedad posible, planes de recuperación para sus sistemas, hecho que afecta negativamente la planeación desarrollada en relación con la distribución de tiempo y de recursos.

Cuando leemos el caso de ILOVEYOU se está ante una clara manifestación de poder funcional: un ejercicio donde un actor, exógeno o regulador, busca delimitar las interacciones de otro en el ciberespacio influenciando; particularmente, el tiempo y las respuestas recíprocas. En otras palabras, tanto las acciones que se desprendan de la prestación de un servicio donde hay privilegios que

permiten el control lícito sobre la infraestructura física y tecnológica como todas las que tengan como propósito negar, degradar, interrumpir, destruir o manipular cualquier componente del ciberespacio disfrutado por otro son manifestaciones del poder funcional. Y como ya se mencionó en los capítulos previos, el empleo de este tipo de poder termina generando relaciones distributivas, caracterizadas por una tensión entre imposición y resistencia (por ejemplo, *malware* vs. sistema de defensa); principalmente, por provenir de actores exógenos al flujo de influencia.

Si nos concentramos por un momento en los actores exógenos dentro del marco del poder funcional, es posible identificar que la relación entre poder y sorpresa se manifiesta de dos formas: una *conceptual* y otra *técnica*. En la forma conceptual, esto es igualmente válido en el poder comportamental; la relación es muy similar a las definiciones tradicionales suministradas al principio de este capítulo: evitar que el sujeto objetivo de la manifestación del poder sepa cuándo, dónde y cómo se dará, por así decirlo, el "golpe". La forma técnica, por el contrario, constituye el aprovechamiento de todos los medios y los modos empleados sobre la infraestructura tecnológica para materializar la sorpresa desde lo conceptual, lo que, desde la bibliografía disponible, se puede reducir a vulnerabilidades, acceso y carga útil (en inglés, *payload*).

Las vulnerabilidades son aspectos de un sistema que pueden ser usadas para comprometerlo. Estas pueden provenir de diversas fuentes: por ejemplo, *bugs*, errores o deficiencias en un *software* que causan que el sistema se comporte de manera incorrecta, inesperada o inintencionada; componentes físicos, o *hardware*; configuraciones de seguridad; canales de comunicación y disposición de la red, y comportamientos del personal. Las vulnerabilidades pueden ser conocidas por el fabricante, pero desconocidas para el usuario, lo cual, en caso de existir los parches o las actualizaciones, se vuelve una cuestión de higiene cibernética. Por el contrario, cuando el fabricante no tiene noción de una vulnerabilidad en su propio producto, se está ante lo que se conoce como "día-cero". En el ejemplo del *malware* ILOVEYOU, la vulnerabilidad se encontraba en el servicio de Outlook.

El valor de la vulnerabilidad es permitir el acceso al sistema, lo que equivale a superar las diferentes capas defensivas para poder alterar el total o parte de los datos que se encuentran almacenados, en procesamiento o transporte y constituyen la información. La forma como se explota una vulnerabilidad y se compromete al sistema, al igual que con sus datos y su información, puede ser por

medios físicos (por ejemplo, destruyendo a golpes un disco duro), digitales (por ejemplo, *malware*, etc.) o psicológicos (por ejemplo, ingeniería social, etc.). En los medios digitales —específicamente, el *malware*—, el componente del código que está destinado a causar daño se conoce como carga útil, o *payload*. La forma como el *payload* se compone y se comporta depende de la clase de *malware* que se quiere constituir: virus, troyanos, gusanos, *rootkits*, *ransomeware*, *keylogger* o *grayware*.

La sorpresa toma forma en las vulnerabilidades y la carga útil cuando, aunque suene redundante, estas son empleadas para acceder y dañar exitosamente a la víctima sin que ella o sus defensas detecten al atacante o reaccionen ante él; no, al menos, hasta que este último vea satisfechos sus propios intereses. Ello implica tener un proceso constante de adaptación, pues los medios y los modos para la ciberseguridad van evolucionando —aunque a menor velocidad—, lo cual hace que lo que era útil para un atacante en un momento se vuelva por completo inservible al día siguiente. Cabe mencionar que en el ciberespacio, al ser un entorno que permite el desarrollo equitativo de capacidades, la posibilidad de emplear la sorpresa es igual para el ejecutor y para el objetivo del poder —extremos opuestos en una relación distributiva—.

Un ejemplo de cómo una posible víctima puede usar la sorpresa como elemento defensivo durante una relación de poder funcional con un tercero exógeno a los actores reguladores son las *honeypots*. Estas son un mecanismo de seguridad de la información aislado, y diseñado para atraer y engañar a posibles atacantes haciéndoles creer que están ante un objetivo de alto valor. La manera cómo funcionan es emulando el sistema real al que están asociadas, con la información y los datos correspondientes, así como el comportamiento esperado, para luego estudiar, contrarrestar y responder al atacante; todo, sin comprometer el verdadero sistema o red. Las *honeypots* pueden presentarse en diferentes formatos: bases de datos (por ejemplo, MongoDB-HoneyProxy, Elastic Honey), webs (por ejemplo, Glastopf, Nodepot), servicios (por ejemplo, honeyntp, honeypot-camera, troje), ICS/SCADA (por ejemplo, Conpot, gridpot, scada-honey-net), servidores (por ejemplo, LaBrea, Honeysink Amun TelnetHoney) y una gran cantidad de herramientas para análisis, detección y monitoreo.

Queda una pregunta por responder sobre la relación entre la sorpresa y el poder funcional, y es cómo esta puede convertirse en un elemento que potencializa o debilita las posiciones de los sujetos frente a terceros exógenos. La respuesta dependerá, nuevamente, de la posición del sujeto en la relación y del

nivel de claridad que este tenga sobre sus propios intereses, así como sobre la naturaleza de estos (i.e. cooperativos o distributivos). Un sujeto que tenga claros sus objetivos y vea que la relación de poder es un medio o un obstáculo para estos buscará mejorar su posición. Desde una posición ofensiva, entendida como la de quien emana el poder, la sorpresa permite reducir la resistencia proveniente del objetivo. Por el contrario, con la perspectiva de quien trata de resistir al poder, la sorpresa se vuelve, como en el caso de las *honeypots*, una forma para negar al otro un objetivo de valor, al igual que para menguar los recursos empleados y su intensidad. Puede suceder que un actor que ejerce poder no tenga un interés particular, y esté motivado por el mero deseo de destrucción; en tal caso de irracionalidad, se deberá proceder con un análisis que supera el alcance del presente capítulo.

En el ciberespacio existe, de acuerdo con la aproximación de este libro, otra manifestación del poder, denominada poder comportamental. Este poder delimita lo que los usuarios pueden o no hacer en el ciberespacio, al igual que la manera como lo hacen, por medio del cumplimiento coercitivo de unos criterios establecidos como "válidos" o "correctos". A diferencia del poder funcional, aquí el empleo de la sorpresa no es tan sencillo, pues no existe una forma técnica preponderante, y si se lo aplica indiscriminadamente sobre el sistema de valores, puede tener un efecto pernicioso sobre los elementos que hacen posible la relación de poder: conocimiento y legitimidad.

El poder comportamental en las relaciones interciberespaciales necesita, para su ejercicio y su mantenimiento, la autoridad del actor regulador, la cual, a su vez, se fundamenta en el conocimiento del sistema de valores por parte del sujeto influenciado, así como en el reconocimiento del regulador como ente competente para ejecutar un castigo en caso de violación de los términos. Afectar dicho conocimiento al introducir sorpresivamente elementos al sistema de valores podría hacer que el usuario considere al castigo caprichoso o injusto, y minarse así la legitimidad de la autoridad que lo ejecutó.

Los cuestionamientos a la legitimidad en el ciberespacio no solo ponen en riesgo la posición de autoridad del actor regulador, sino que pueden contravenir sus intereses. Por un lado, se motivan la migración de los usuarios y el empleo de técnicas de dilución de identidad, lo cual tiene implicaciones económicas. Y, por otro, en casos extremos, se abre la puerta para retaliaciones con capacidad para impactar negativamente al actor regulador desde lo tecnológico, lo operacional, lo reputacional y lo financiero. Miremos un ejemplo hipotético:

Supongamos que existe una "comunidad virtual" donde solo es posible llevar a cabo interacciones públicas relacionadas con fútbol: postear en los foros, vender artículos y emitir opiniones, entre otros. Los usuarios que hacen parte de esta comunidad conocen las reglas, y saben que el castigo es escalonado de acuerdo con la cantidad de veces que se incurra en el comportamiento indeseado: la primera vez, con amonestación escrita; la segunda, con *baneo* temporal, y la tercera, con expulsión permanente. Además, imaginemos a dos usuarios: uno que recibió amonestación verbal por publicar información relacionada con el fútbol femenino, algo que no hace parte expresa de las reglas de la comunidad, y otro que fue expulsado cuando solo merecía una amonestación verbal. Ahora, trate cada cual de responderse las siguientes preguntas con la información suministrada: ¿considera usted que el administrador de la comunidad virtual fue justo? ¿Se quedaría en una comunidad donde el administrador actúa caprichosamente? En caso de habersele hecho un daño directo a usted, ¿buscaría una manera de retaliación o de reclamo que subsane su pérdida?

Situaciones como la descrita hipotéticamente son muy comunes en las relaciones interciberespaciales de carácter comportamental, y ponen sobre la mesa otro elemento alusivo al conocimiento: es indispensable para este tipo de poder que los usuarios o los actores reguladores de menor jerarquía sepan el tipo y la magnitud del castigo que implica una violación del sistema de valores. Y es que este poder depende del efecto psicológico de la disuasión; es decir, del hecho de que se reconozca que infringir el sistema de valores puede llevar a un castigo, y que el impacto de este supera cualquier beneficio proveniente del incumplimiento. En tal sentido, y en teoría, el análisis de costo-beneficio realizado por quien se encuentra bajo influencia debe llevarlo a concluir que el daño proveniente del castigo no puede ser gestionado (i.e. evitado, mitigado, transferido o aceptado).

El hecho de que la sorpresa no se emplee para afectar el conocimiento del sistema de valores y el castigo no significa que no pueda ser usada en absoluto en el poder comportamental; esta tiene cabida para influir sobre la percepción que un sujeto tiene de su propia habilidad para gestionar el costo o el daño que se dependa del castigo. Emplear la sorpresa sobre el tiempo, el momento o la circunstancia en los que un castigo es aplicado puede afectar el nivel de incertidumbre para el sujeto sobre quien recae el efecto de la disuasión. Esta incertidumbre arrebató al sujeto su sensación de control de la situación, así como su habilidad para calcular y prepararse, y disminuye, por tanto, la percepción de éxito que pueda tener frente a la efectiva gestión del daño. Si el sujeto considera

que el daño no puede gestionarse, es posible que su análisis de costo-beneficio en una situación de disuasión se incline hacia la obediencia esperada por el actor regulador que emplea el poder. De esa forma, se logra el objetivo de la sorpresa de obtener una ventaja o un cambio favorable en una situación particular que implique a otro actor (Parks & Duggan, 2011).

El rol de la sorpresa como potenciador o debilitador de la relación de poder en el tema comportamental recae directamente en el efecto psicológico que se crea en la disuasión; en otras palabras, potencializa si es posible fortalecer la posición de quien promete una retaliación en el caso de una violación al sistema de valores, y debilita cuando otorga al sujeto sobre quien recae el poder la percepción de que el daño o el costo pueden ser gestionados con éxito. Aunque este análisis será complementado por un capítulo adicional, que desarrolla la racionalidad de los actores en el ciberespacio, puede afirmarse, mientras, que la sorpresa bien puede resultar útil; al menos, para una parte, si se respetan los elementos de conocimiento y legitimidad.

## Lecciones

- La sorpresa tiene como objetivo lograr una ventaja o un cambio favorables en una situación particular que implique a otro actor, lo cual se logra por medio del impacto psicológico en el adversario y su desacomodación.
- La sorpresa tiene una relación directa con el poder. Esta es un multiplicador de los medios empleados para la adquisición, el control y el ejercicio de este, puede aumentar considerablemente las garantías de éxito y es empleada tanto por los débiles como por los fuertes. En el caso de quienes estén en desventaja, la sorpresa permite debilitar las fuentes de donde emana el poder, así como su manifestación.
- La sorpresa no es exclusiva del mundo material: también puede ser empleada en el ciberespacio, dentro del marco de las relaciones interciberespaciales; sin embargo, su utilidad y su manifestación dependerán del tipo de relación de poder que se analice: poder funcional o poder comportamental.
- En las relaciones de poder funcional, la sorpresa tiene una forma conceptual y otra técnica. La conceptual se asemeja a las definiciones del mundo material, mientras la técnica hace referencia a medios y los modos dirigidos a la infraestructura tecnológica para lograr el efecto

psicológico esperado. Esto último termina resumiéndose, generalmente, en acceso, vulnerabilidades y carga útil.

- La sorpresa puede ser empleada por quien ejecuta poder funcional para evitar la resistencia, en cuanto se está ante un contexto distributivo, y por quien defiende, para negar el acceso a un objetivo válido.
- En el poder comportamental, la sorpresa debe ser aplicada con sumo cuidado, pues tiene la capacidad para afectar los cimientos sobre los cuales se sustenta la autoridad del usuario regulador. Así, se debe respetar el conocimiento que el usuario que es influenciado tiene sobre el sistema de valores, al igual que la naturaleza y la magnitud del castigo, pues de lo contrario se puede afectar la legitimidad. Aun así, esta puede ser empleada dentro del efecto psicológico de la disuasión para disminuir la percepción, por parte del sujeto influenciado, de gestión del daño o de costo por incumplimiento.



## 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. *International 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., Rameswaran, 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](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.º15: 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: I Love You*. <https://tinyurl.com/yc58mpph>
- Paquet-Clouston, M., Décarý-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/yc4c3kww>

- 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).
- Senvet. (s.f.). *Terms of service*. <http://servnetshszndci.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.
- Si Yuan, 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](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. *Journal 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?ProvlDs=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](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.





EDITORIAL **ESDEG**

# Conceptualización

## del ciberespacio humano

El ingenio y voluntad están detrás de todas nuestras creaciones. Encontramos soluciones a obstáculos o necesidades de la cotidianidad, incluso desconociendo las consecuencias de su empleo. Ya nos ha ocurrido con la dinamita y la tecnología nuclear, y ahora sucede con el ciberespacio.

El ciberespacio es hasta el momento el único dominio creado por nuestra especie, lo cual resulta sumamente paradójico, considerando que la gran mayoría lo emplea diariamente sin entender su conformación ni las implicaciones en la vida cotidiana. Peor aun, justificamos este desconocimiento al afirmar que este dominio solo atañe a unos pocos que conocen el lenguaje de las computadoras, sin detenernos a pensar que con tener un teléfono celular ya se forma parte del ciberespacio.

Este libro nace como respuesta a esta deficiencia de conocimiento en los usuarios del ciberespacio, pero se desliga de las aproximaciones tradicionales y técnicas para concentrarse en el factor del comportamiento humano en sociedad. Se encuentra dividida en cuatro capítulos: el primero desarrolla el concepto del ciberespacio; el segundo, los actores que en este interactúan y sus motivaciones; el tercero, el concepto de poder, y el último, la sorpresa como un elemento potenciador. Para plantear el argumento se empleó una premisa: mientras las tecnologías de inteligencia artificial no sean realmente eficientes, al final siempre habrá una persona detrás de cada código, plataforma, red, sistema o máquina. Si esto es cierto, el ciberespacio es, indiscutiblemente, un entorno humano que nos atañe a todos y, solo por eso, esta lectura bien vale la pena.



ISBN 978-628-7602-14-4



9 786287 602144