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 partiucularidades. 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-kiddies*	*Hackers* profesionales	Empresas	Terroristas/ insurgentes	Crimen organizado	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-noobs /script-kiddies*	*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	*Rootkits, defacement, spoofing, ransomeware, 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, sross-site scripting, advanced persistent threat* (APT), *account hijacking*.							

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 su 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 maquina 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-Hétu, 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 Escubar 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 Roard*; 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*)—.[1] 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).[2] 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).

---

1 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.

2 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; farc-ep. co; farc-epeace.org; resistencia-colombia.org; frentean.org; y 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.[3] Se le otorga preponderancia a la concepción del territorio bajo la lógica del sistema

[3] 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 geoestacionaria, 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; Liaropoulos, 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 gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos 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 *banneada* 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 vulneren, 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 tranzar 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.

Analógicamente, 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 exacerba 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 disimiles, 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.

Referencias

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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