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

CC BY NC ND

* 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.).	*On War*	"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.).	*El arte de la guerra*	"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 […] Sírvete 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).	*El libro de los cinco anillos*	"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).	*Las 36 estrategias chinas*	"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).	*The Principles of War*	"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).	*The Foundations of the Science of War*	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]).	*On Guerrilla Warfare*	"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).	*UK Defence Doctrine Joint Doctrine Publication 0-01 (jdp 0-01)*	"Surprise is the consequence of confusion induced by deliberately or incidentally introducing the unexpected".
Antigua Unión Soviética (US Army, 1984, Sección 2-2).	*Fm 100-2-1: the soviet army: operations and tactics*	"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).	*U.S. Army Field Manual: Operations (FM 100-5)*	"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).	*Manual de Estrategia Militar General (3-4)*	"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 acompaña 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 (Beevor, 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 (Beevor, 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 *Ransomeware 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 trasporte 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-honeynet), 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 repuesta 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 habérsele 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 deprenda 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 arrebata 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. 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.