

# La Confianza Agotada en el Espacio Cibernético Común\*

DR. ROGER HURWITZ, PHD

Las autoridades responsables de formular una política reconocen cada vez más la necesidad de contar con acuerdos para regular los comportamientos cibernéticos a nivel internacional. En el 2010, el Grupo de Expertos Gubernamentales sobre Desarrollos en los Campos de Información y Telecomunicaciones en el Contexto de la Seguridad Internacional de las Naciones Unidas recomendaron “el diálogo entre los estados para discutir normas relacionadas con el uso del estado de la tecnología de información y comunicaciones (ICT, por sus siglas en inglés), para reducir el riesgo colectivo y proteger la infraestructura crítica nacional e internacional”.<sup>1</sup> Desde entonces, Estados Unidos, Rusia, China y otras potencias cibernéticas han propuesto normas para discusión y, en noviembre de 2011, el Reino Unido convocó una conferencia intergubernamental para discutir sobre las “reglas del juego” cibernéticas.<sup>2</sup> Estas actividades son un cambio positivo de la primera década de este siglo, cuando Estados Unidos y Rusia no podían llegar a un acuerdo sobre lo que se debía discutir y el acuerdo internacional existente para el ciberespacio—la Convención de Budapest sobre Delitos Informáticos—no cobró mucha fuerza. La Secretaria del Departamento de Seguridad Interna, Janet Napolitano, destacó en el verano de 2011 que los intentos de contar con “un marco internacional exhaustivo” para gobernar comportamientos cibernéticos aún estaba en una “etapa inicial”.<sup>3</sup> Puede que esa búsqueda sea desconcertante. Adam Segal y Matthew Waxman, miembros del Consejo sobre Relaciones Exteriores, advierte que “la idea de negociar en un final un tratado de seguridad cibernética mundial y exhaustivo es un sueño imposible”. Según su opinión, las diferencias en ideologías y prioridades estratégicas evitarán que Estados Unidos, Rusia y China lleguen a acuerdos significativos: “Con Estados Unidos y las democracias europeas en un extremo y China y Rusia en otro, los estados discrepan marcadamente en cuanto a temas tales como si las leyes de guerra internacionales y la autodefensa deben aplicar a los ataques cibernéticos, el derecho a bloquear información de los ciudadanos y los papeles que actores privados o cuasi privados deben desempeñar al gobernar la *Internet*”.<sup>4</sup>

Este ensayo se une a ese pesimismo con base en un modelo más extenso de la crisis emergente en el ciberespacio. El argumento esencial es que mantener un ciberespacio seguro significa sostener un espacio común que beneficie a todos los usuarios, pero su sobreexplotación por parte de usuarios individuales resulta en la muy conocida tragedia del espacio común”.<sup>5</sup> Aquí el recurso común que se puede agotar es la confianza, mientras que los usuarios son naciones, organizaciones e individuos cuyos comportamientos en el ciberespacio no están sujetos a una autoridad central. Sus acciones, que dañan el bienestar de otros usuarios, disminuyen la confianza y la cantidad de sobreexplotación de un recurso común. La tragedia del espacio común se emplea repetidamente como un argumento para la privatización y en retrospectiva para justificar el cercamiento de tierras de los capitalistas agrícolas ingleses en los siglos XVII y XVIII. No obstante, tal tragedia no es inevitable, inclusive cuando los usuarios de un espacio común se suponen sean sensatos en el sentido de maximizar el interés propio. La finada politóloga Elinor Ostrom recibió el Premio Nobel en economía por determinar casos y condiciones en las que, en ausencia del control del gobierno, los usuarios exitosamente se auto organizan para el uso sostenible de un espacio común.<sup>6</sup> Lamentablemente, tal como se discute a continuación, el estado

\* Reimpreso de nuestra AU Revista Strategic Studies Quarterly, Vol 6, Nº 3, Fall 2012.

actual del ciberespacio y sus usuarios no cumple con la mayoría de las condiciones que exhortan esa autoorganización. Ambas posibilidades de las tecnologías cibernéticas—es decir, la manera como las tecnologías hacen posible su uso—y las mentalidades de los usuarios contribuyen al resultado desfavorable.

Incorporar los obstáculos a los acuerdos internacionales dentro de esta perspectiva más amplia hará resaltar los procesos de varios niveles, complejos y transformativos que el ciberespacio les presenta a los estados y a otras entidades que lo administrarían. No es un ámbito pasivo en el que los estados pueden ir en busca de sus intereses preexistentes competitivos o en conflicto, sino uno cuyas tecnologías y aplicaciones que cambian rápidamente crea oportunidades para el conflicto. Además, motiva la cooperación. Por consiguiente, la siguiente sección crea el modelo del ciberespacio como un sistema social basado en un espacio común—un “sistema socio-ecológico” (SES, por sus siglas en inglés) y un “recurso de uso común” (CPR, por sus siglas en inglés) para emplear la terminología de Ostrom—que se puede sostener pero también agotar. La identificación de la confianza como este “recurso” y las implicaciones de su agotamiento recibirán atención particular. En la tercera sección se revisan las variantes que Ostrom y sus colegas han descubierto que fomentan la autoorganización y las evalúa con respecto al ciberespacio. En la última sección se analiza cuáles de las variantes del modelo actualmente desalientan que la autoorganización se puede cambiar en una dirección más alentadora mediante acciones factibles por parte de agentes, eliminando así algunos obstáculos para lograr acuerdos internacionales. También se analiza cómo los estados, a falta de estos cambios, pueden responder unilateralmente a las crisis de la seguridad cibernética.

## Los retos del espacio común cibernético

Gobernar un recurso de uso común accesible, o CPR, es un problema de acción colectiva, ya sea que la meta es la explotación sostenible de la industria pesquera o el uso seguro y beneficioso del ciberespacio. Para los CPR naturales, donde ocurre la regeneración de existencias, se necesitan algunos límites en el uso por parte de individuos por cantidad o clase, a menos que el uso final sobrepase la “capacidad de carga”. Esto agota el recurso por debajo del nivel al cual los procesos naturales pueden sostenerlo para una explotación provechosa. Tal como se discute a continuación, esta necesidad de limitar la explotación también puede aplicarse a recursos hechos por el hombre, o artificiales, como el ciberespacio. Limitar o regular el uso por lo regular requiere un estado preexistente u otra autoridad con poder coercitivo, en cuyo territorio se encuentra el CPR—por buenos motivos. Aunque los usuarios podrían aceptar la necesidad de contar con límites, los usuarios individuales están tentados a excederlos creyendo que una presión accidental en el recurso es insignificante con respecto a su sostenibilidad. Además, individuos que se dan cuenta de las infracciones de sus vecinos no estarían dispuestos a sancionarles por temor a represalias. No obstante, Ostrom encontró muchos casos en que las personas administraron exitosamente un CPR sin la necesidad de intervención o privatización por parte del estado. Al analizar esos casos, ella conceptualiza el CPR como que existe dentro de un contexto de las prácticas socioeconómicas y culturales de sus usuarios. Estas prácticas inciden tanto en las opciones de los usuarios individuales acerca de explotar el CPR y en la posibilidad de su regulación colectiva de sostenerlo. Juntos, el CPR y el contexto social, constituyen el sistema socioecológico (SES, por sus siglas en inglés).

Uno se preguntaría cómo un ámbito puede ser un espacio común cuando cada porción de su sustrato físico le pertenece a alguna organización o estado a diferencia de, por ejemplo, los océanos, el espacio aéreo internacional y el espacio exterior. Varias respuestas son útiles para perfeccionar nuestra noción de un espacio común cibernético y cualesquier acuerdos internacionales que lo protegerían. Lawrence Lessig aludió a un modelo de transporte de comunicación por *Internet* que incluye capas para el sustrato físico, los paquetes o sobres electrónicos para

la información y el contenido en sí de la información. Él identificó el espacio común con la capa de paquete, a la cual todos tienen derecho al acceso y a la cual todos pueden contribuir, de manera que cualquier flujo de paquetes cierra el espacio común.<sup>7</sup> Desde este punto de vista, el espacio común cibernético es similar a los océanos o el espacio aéreo internacional, con el derecho de paso siendo la inquietud principal de los usuarios.<sup>8</sup> En un final Lessig y otros basaron esta idea del espacio común cibernético en el derecho humano de acceso a la información y libertad de expresión. También resonó con nociones de libertad de movimiento, innovación global para la *Internet* y una esfera evolutiva de información mundial en la que todos pudiesen participar—con la resonancia captada en una palabra: “abierta”. Esfuerzos como *Wikipedia*, *Creative Commons*, cursos gratis de MIT y la blogósfera emergente podrían crear un segundo espacio común—uno de contenido. Con el cambio de milenio, Lessig se percató que esos esfuerzos eran amenazados por empresas de contenido de medios de comunicación, con sus interpretaciones amplias de derecho de autor a expensas del uso justo y su reclutamiento de autoridades estatales para el trato draconiano de presuntas infracciones a los derechos de autor. Él pasó por alto el argumento de una necesidad de proteger el agotamiento de los recursos intelectuales al invocar la imagen de Thomas Jefferson de una vela cuya luz no es disminuida al prender otra vela—un tropo para el Siglo de las Luces que sintetiza la promesa de la *Internet*. El drama en desarrollo fue en el cambio de organizaciones avariciosas utilizando las posibles fechorías de unos cuantos individuos como un pretexto para privatizar la propiedad intelectual común y socavar el acceso necesario para sostener una cultura de *Internet*.<sup>9</sup>

Esta idea de “un espacio común cibernético” apareció hace más de una década, cuando la población en línea era un décimo de su tamaño actual y estaba concentrada en América del Norte y Europa occidental, donde a la *Internet* se le consideraba como otro lugar en una ecología de información y comunicación rica y ligeramente regulada. Sin embargo, pasaba por alto que la *Internet* ya la estaban usando grupos en una lucha violenta contra algunos estados—separatistas chechenos contra Rusia—e inclusive estados liberales ya estaban excluyendo el acceso y la distribución de cierta información, como por ejemplo la pornografía infantil. Desde ese entonces, el uso del ciberespacio, que ahora se extiende mucho más allá de la *Internet*, se ha tornado un problema de seguridad nacional tan omnipresente (“securitización”) o una amenaza a la estabilidad del régimen, que ahora muchos gobiernos filtran o bloquean ciertos flujos de paquetes, por ende reemplazando el espacio común cibernético principal con sus propios recintos “seguros”.<sup>10</sup> No obstante, la visión de un espacio común cibernético notifica partes significativas de las políticas cibernéticas de Estados Unidos y muchos de sus aliados y las posturas que toman con respecto a la regulación internacional del ciberespacio. La adopción más notable es la del Departamento de Estado en cuanto a la libertad en la *Internet*—los derechos de habilitación cibernética del activismo cívico—pero el énfasis en la interoperabilidad global, la no interferencia por parte de estados con paquetes atravesando sus territorios y las decisiones en cuanto a la tecnología de *Internet* llevadas a cabo por tecnólogos en lugar de autoridades políticas son también significativas.<sup>11</sup>

Sin embargo, un CPR más fácil de identificar, de acuerdo con el modelo SES de Ostrom, es el ancho de banda, el cual puede ser agotado por un *spam*—una sobreexplotación del recurso—resultando en una entrega degradada de comunicaciones más valiosas. Los *spammers* han sido comparados con los contaminantes industriales del espacio común de los recursos naturales porque ellos también le transmiten al público en general las externalidades negativas de sus acciones, ya sean en la forma del tiempo de espera de los usuarios en una red saturada o costes adicionales para más ancho de banda, filtros *antispam*, etc.<sup>12</sup> El fenómeno del *spam* se puede generalizar a las consecuencias del agotamiento del “sentido de seguridad” del público en general; como un producto secundario de los fraudes y robos de identidad en línea al nivel individual y ataques a la infraestructura, como Stuxnet, a nivel nacional. Estas incitan demandas amplias para medidas de ciberseguridad, que son gastos. El suministro de esas medidas, que por lo regu-

lar dan poco resultado, tiene poco efecto en refrenar las amenazas, disminuye la eficacia económica de las comunicaciones y control basado en la cibernética. En vista de que la capacidad de la *Internet* de disminuir los costes en las transacciones es considerada uno de sus beneficios principales para el desarrollo económico y social, los posibles costes elevados de la seguridad cibernética son retos para muchos estados y organizaciones, quizás tan retos como las consecuencias de ataques a falta de una seguridad adecuada.<sup>13</sup>

## El ciberespacio como sistema social

Relacionado muy de cerca con esa inseguridad está el descenso en la confianza pueblo o social, que podría identificarse como el recurso de uso común fundamental en el SES cibernético. Jacques Bus concuerda con el sociólogo Nicolas Luhmann en explicar la confianza como “un mecanismo que disminuye la complejidad y le permite a las personas lidiar con los niveles elevados de incertidumbre y complejidad de la vida (contemporánea)”. Él agrega lo siguiente,

la confianza amplía la capacidad de las personas de poder relacionarse exitosamente con un mundo real cuya complejidad e imprevisibilidad es mucho mayor de lo que somos capaces de aceptar. En este sentido es un mecanismo necesario para que las personas vivan su vida: para comunicarse, cooperar, llevar a cabo transacciones económicas, etc. Enriquece la vida del individuo al exhortar actividad, audacia, aventura y creatividad y enriqueciendo el alcance de las relaciones del individuo con otras personas.<sup>14</sup>

La noción de la confianza de los ciudadanos, como se emplea en este documento, también incluye la confianza de las personas en las instituciones, leyes, gobierno e infraestructuras de sus sociedades. La confianza de los ciudadanos con respecto al ciberespacio exhorta a los individuos y a las organizaciones a tener acceso y poder ser consultados entre sí en línea, y que a su vez permite el efecto de red en el ciberespacio; o sea, las externalidades positivas creadas a medida que más personas participan en la red y ocurren más interacciones. Esto es consistente con los hallazgos de científicos sociólogos de correlaciones positivas fuertes entre la confianza de los ciudadanos y el crecimiento económico.<sup>15</sup>

La confianza del pueblo en el ciberespacio incluye la confianza en las personas y en las organizaciones con las que los individuos lidian a través de tecnologías digitales y la honradez de las tecnologías en sí. La confianza en otros en línea es problemática porque esos otros podrían ser anónimos o identificados parcialmente, y el contexto de las interacciones con ellos es opaca o confusa. Puede estar respaldada por suposiciones acerca de las inquietudes de otros sobre la reputación y el compromiso con funciones y mecanismos en línea, como por ejemplo certificados y clasificaciones, que pueden confirmar afirmaciones hechas por otros. Sin embargo, últimamente, la confianza en el ciberespacio puede tornarse tensa por la publicidad de las diferentes amenazas cibernéticas mencionadas anteriormente, el fracaso de organizaciones y gobiernos de disuadirlas y el compromiso de los mecanismos de seguridad en línea, como certificados robados. Además, la confianza de los ciudadanos se ve afectada porque muchos usuarios están conscientes que sus actividades en línea se están vigilando, ya sea para la explotación comercial en occidente o para identificar disidentes políticos en países autoritarios.

Estos abusos podrían mermar la confianza del pueblo—o sea, la voluntad agregada de los usuarios de entrar en línea—muy parecido a la sobreexplotación por parte de algunos de sus usuarios que agota un CPR. Desde este punto de vista, la confianza de los ciudadanos es un buen rival cuyo consumo por un usuario disminuye la cantidad de consumo disponible por otros. Por analogía, los abusos en curso contra una cantidad decreciente de confianza del pueblo podrían dar lugar a una provisión no satisfactoria de beneficios en línea que la confianza de los ciudadanos permite. En términos concretos, los individuos y las organizaciones que le temen al delito cibernético, a las invasiones de la privacidad, etc., disminuirían en gran medida su uso de las

redes digitales para transacciones económicas, intercambio de información e interacciones sociales. Pero a diferencia de los recursos de uso común, como los bosques y la industria pesquera, la confianza del pueblo en el ciberespacio no siempre es un buen rival. Las interacciones en línea mutuamente beneficiosas se sostendrán y aumentarán, y éstas son tan numerosas a los niveles individual e institucional que a menudo los abusos se pasan por alto o se olvidan rápidamente. Por consiguiente, hay pocas pruebas de personas saliendo del ciberespacio o evitando sitios populares con políticas de privacidad controversiales. Aún, en algunos países democráticos, los ciudadanos relevantes han exigido que los proveedores de servicio e investigación refrenen el rastreo; algunos gobiernos ya han respondido con políticas regulatorias que obligarán a los compiladores y analistas de datos a hacer ajustes. Estas acciones se pueden interpretar como situaciones en las que los usuarios defienden un CPR acudiendo a la autoridad actual en busca de liderazgo y establecimiento de normas. Ellas muestran que para sostener la confianza en el ciberespacio requiere, además de tecnologías de seguridad, reglas, prácticas transparentes, normas de responsabilidad y medios de compensación aceptables a los usuarios. Los esfuerzos internacionales de lograr acuerdos para proteger y sostener el ciberespacio tendrán, por lo tanto, que tomar en cuenta esas inquietudes, hasta cierto punto. Puede que ese no sea un reto formidable. En vista de que las “aplicaciones” cibernéticas se han tornado indispensables para muchos usuarios, puede que sean aseguradas, por lo menos momentáneamente, por pasos pequeños y superficiales por parte de los proveedores o reguladores, inclusive avisos sobre la política, botones de “inhabilitar” y nuevos, y quizás incomprensibles, acuerdos de servicio. En otras palabras, el ciberespacio ya no es un ámbito aparte para sus usuarios, un lugar para visitar cuando uno lo decide, como un lugar para turistas, sino que ha penetrado y vuelto a tejer la tela de nuestras vidas.<sup>16</sup>

Podría decirse que los *spammers*, hackers, recopiladores de datos, pandillas de delincuentes, activistas cibernéticos y agencias estatales que amenazan la confianza de los ciudadanos no buscan destruir la *Internet* o congelar el ciberespacio—no más que los campesinos quienes supuestamente pastoreaban excesivamente el espacio común querían degradarlo. La obra de Ostrom implica que dos tipos de agentes dañan el CPR: los cazadores furtivos fuera del grupo que mantiene al SES y los miembros del grupo que sobrepasan sus derechos al CPR. En este caso, los delincuentes cibernéticos, los terroristas y ciertos activistas—por ejemplo Lulzsec—serían los cazadores furtivos en el ciberespacio. En la imaginación popular, y a menudo en sus propias imaginaciones, ellos ocupan la imagen de piratas—individuos o grupos fuera de los países y más allá de las leyes de las naciones.<sup>17</sup> De hecho, algunos analistas opinan que la cooperación internacional para contener esos grupos se puede realizar fácilmente y constituye el primer paso hacia acuerdos más exhaustivos sobre el ciberespacio. Por supuesto, en calidad de cazadores furtivos o parásitos, estos grupos no buscan la destrucción del ciberespacio, ya que eso los “dejaría sin trabajo”.

El segundo tipo incluye gobiernos, proveedores de servicio en línea, corporaciones multinacionales y otros—las susodichas partes interesadas—quienes reconocen la necesidad de contar con límites pero que con frecuencia hacen alarde de esos límites en busca de intereses individuales. Inclusive estados que diseñan armamento cibernético para dañar las infraestructuras y gobiernos basados en la cibernética que espían a sus ciudadanos en línea valoran su propio uso del ciberespacio a la vez que planifican restringir su uso por otros. La ambivalencia resultante de muchos gobiernos quizás se capta mejor en un documento blanco chino reciente que celebra la *Internet* por permitir el desarrollo económico y social, destaca su uso haciendo propaganda de los ciudadanos y en campañas contra la corrupción provincial, pero estipula que

ninguna organización o individuo puede producir, duplicar, anunciar o propagar información [en la Internet] que contenga lo siguiente: estar en contra de los principios cardinales establecidos en la Constitución; poner en peligro la seguridad del estado, divulgar secretos de estado, socavar el poder del estado y poner en peligro la unificación nacional; dañar el honor e intereses del estado; instigar el

odio o la discriminación étnica y poner en peligro la unidad étnica; poner en peligro las políticas religiosas del estado, propagar ideas heréticas o supersticiosas; propagar rumores, interrumpir el orden social y la estabilidad; diseminar material obsceno, pornografía, apuestas, violencia, mal trato y terror o participar en actos delictivos; humillar o calumniar a otros, abusar los derechos legales e intereses de otros; y otros contenidos prohibidos por la ley y las regulaciones administrativas.<sup>18</sup>

Desde este punto de vista, el problema estratégico con la *Internet* no es su uso doble si no sus muchos usos. Tantos, de hecho, que esfuerzos unilaterales como las inspecciones profundas de paquetes para refrenar los “usos no deseados” en sí amenazan la estabilidad y sostenibilidad del ciberespacio.

Actores sofisticados que amenazan la confianza del pueblo en el ciberespacio podrían prever las consecuencias adversas de sus actos. Además, podrían calcular que cualquier daño que hagan, la disminución de la confianza del pueblo será moderada o las ganancias en usar la *Internet* aún serán tan grandes que la confianza de los ciudadanos y la accesibilidad mutua permanecerán por encima de algún umbral mínimo. Como ya se ha destacado, tendencias recientes apoyan ese cálculo. Sin embargo, hasta el punto en que su conducción no se puede ni generalizar ni continuar indefinidamente—o sea, sin consecuencias devastadoras—a la pregunta, “¿Qué sucedería si todos siempre actuasen como usted?”, ellos tienen que responder, como Yossarian, “Sería un gran tonto si no lo hiciera”. La alternativa es que todos los yossarianos actúen juntos para cambiar la situación. Bajo las condiciones actuales, ¿es eso posible en el ciberespacio? ¿Puede una cantidad significativa de actores relevantes abandonar prácticas que lo amenacen y comprometerse con reglas que lo sostengan?

## Variables de la autoorganización

Ostrom y sus socios han identificado 10 variables críticas para la autoorganización en un sistema socioecológico—es decir, reglas de uso eficaces y que se cumplan para un recurso de uso común en ausencia de una autoridad estatal.<sup>19</sup> Cada variable se explica a continuación, algunas veces con citas directas de Ostrom (ya sea en letra cursiva o entre comillas), mientras que la manifestación en el ciberespacio se describe y evalúa con respecto a su efecto en la autoorganización. Los efectos alentadores, desalentadores y neutrales son identificados por +, −, ó 0, respectivamente. Las variables tienen que ver con las propiedades de los recursos que se explotan en el SES y las características de la población de usuarios. De conformidad con la observación que la confianza del pueblo en el ciberespacio depende de la fiabilidad de su *hardware* y *software*, al igual que el comportamiento de sus usuarios, sus propiedades se toman en cuenta al evaluar las variables relevantes.

Como se verá, las explicaciones de Ostrom de los efectos de las variables en cuanto a la posibilidad para la autoorganización son consistentes con un modelo actor racional: la probabilidad de la autoorganización aumenta mientras más su contribución para sostener el recurso de uso común exceda los costes de lograr que agentes firmen acuerdos y hacer cumplir los acuerdos. Por lo tanto, mientras más bajos sean esos costes, habrá mayor probabilidad para la autoorganización. La suposición con respecto a su proceso es que los estados a través de acuerdos multilaterales establecerían reglas y regulaciones para el ciberespacio; ellos harían cumplirlas directamente o le otorgarían el poder a una agencia internacional para hacerlo.

### Tamaño del Recurso (−)

Recursos grandes con fronteras poco definidas disuaden la autoorganización a causa de los costes elevados de definir fronteras, vigilar su uso y rastrear las consecuencias de la mala conducta.

El tamaño del ciberespacio, según lo miden varios billones de dispositivos conectados a la *Internet*, disuade definir sus fronteras y vigilar los comportamientos en él. Como experimento de reflexión, supongamos que las “fronteras” para un ciberespacio fiable fueron definidas por una lista gigante mantenida centralmente de varios billones de dispositivos seguros verificados, con “seguros” designándolo libre de *malware* o que no ha participado en espionaje u otras operaciones de penetración. Sería necesario actualizar continuamente esta lista para acomodar los dispositivos que se le agregan a la *Internet* y la verificación recurrente de dispositivos seguros, porque cualquiera estaría vulnerable a un ataque de un anfitrión falsificando un dispositivo seguro. Este método sería muy costoso y tan solo parcialmente eficaz en inspirar la confianza de los usuarios; algunos ataques son tan furtivos que solamente se descubren después que ha ocurrido, si acaso.

Trazar las fronteras y vigilar el comportamiento puede ser más factible, económico y convincente si los gobiernos nacionales asumen la responsabilidad de los dispositivos y los usuarios en sus territorios certificando las máquinas y otorgándoles credenciales a los usuarios. Entonces, medios unilaterales y multilaterales podrían proteger los ciberespacios nacionales definidos. Esos medios incluyen la implementación de “*firewalls* nacionales” y la reducción de portales nacionales, pasaportes cibernéticos para los usuarios y la asignación de direcciones IP consecutivas para territorios específicos. Esas medidas no detendrían todos los ataques externos y explotaciones dentro de un ciberespacio nacional, pero facilitarían definir el origen de los ataques y responsabilizarían a las autoridades en el estado donde originó un ataque.<sup>20</sup>

El sistema resultante extendería el principio de la soberanía nacional—la piedra angular de las relaciones internacionales contemporáneas—hacia el ciberespacio<sup>21</sup> y aumentaría el control de los estados sobre las actividades en línea de sus residentes. Algunos estados, inclusive unas cuantas democracias liberales en occidente, ya han adoptado o abogado por algunas de esas medidas para lidiar con las amenazas a la seguridad cibernética. Sin embargo, muchos gobiernos, organizaciones y usuarios individuales se opondrán al pleno desarrollo del sistema por varias razones. Primero, sancionaría la fragmentación de la *Internet* en muchas “*internet* en un país” con una consiguiente restricción de comunicaciones globales. Ese proceso ya presagiado en China, Irán y otros países autoritarios, atrasaría los esfuerzos de crear un espacio común para la discusión de temas tales como el cambio climático, conocimientos científicos e investigaciones médicas en una agenda global. Segundo, las corporaciones multinacionales y otros agentes de la globalización, inclusive administradores económicos en países autoritarios, considerarán que este sistema es un obstáculo para la economía global en la que los negocios en cualquier parte pueden tener abastecedores y usuarios en todas partes. Para ellos, un aspecto particularmente amenazante de la proyección de soberanía nacional hacia el ciberespacio es la posible restricción en el movimiento de recursos de información. Tercero, los defensores de derechos humanos se opondrán a conceder el derecho a definir un ciberataque a gobiernos nacionales, ya que sus definiciones pueden incluir una amplia serie de contenido, tal como se mencionó anteriormente con respecto a China, al igual que códigos maliciosos. Cuarto, los encargados de formular las leyes probablemente dudarán si los gobiernos aceptarán la responsabilidad de los ataques cibernéticos que originan en sus territorios bajo este sistema. Esas dudas se pueden basar en las prácticas actuales de los gobiernos que alegan ignorar de dónde provienen los ataques o que no cuenta con los medios para reprimir todos los ataques.

Por último, las fronteras nacionales en el ciberespacio son una manera de analizar minuciosamente el espacio común y privatizar los pedazos. En vista de que este espacio común es una red, su desmantelamiento involucra una pérdida de valor. O sea, la suma de los valores de las partes será menos que el valor del total original. La pérdida se definirá en diferentes maneras, pero su anticipación motivará una resistencia amplia a la idea de fronteras cibernéticas nacionales. No obstante, la idea pone de relieve preguntas acerca del carácter del espacio común cibernético: si es una capa fina de comunicaciones en, y a la larga reducida a, entidades y jurisdicciones geofísicas diversas, o si provee conjuntos de experiencias—un modo de ser—en la que los usuarios

podiesen adquirir entidades nuevas que trascienden la identidad nacional. Jacques Bus analiza la pregunta, afortunadamente libre de los acostumbrados panegíricos acerca de la *Internet* aplandando el mundo:

La globalización, evidentemente impulsada por ICT nuevos y la red, crea un entendimiento y por ende más confianza mediante la propagación de información sobre la historia y la reputación de las sociedades, las características de las sociedades y las vidas de las personas viviendo en ciertas sociedades, y permitiendo la comunicación mundial fácil. Puede que de hecho esto conlleve a un desgaste adicional del concepto que “el animal humano está mejor en casa”. Puede que posiblemente lleve a la necesidad de contar con una visión completamente nueva de las sociedades y su unión y el papel que la confianza debe desempeñar en esto.<sup>22</sup>

### Número de Usuarios (–)

Mientras más sea la cantidad de usuarios de un CPR, los costes de transacción de unirlos y que estén de acuerdo con el cambio serán mayores. Por lo tanto, el tamaño del grupo desalienta la autoorganización, pero “su resultado en la misma depende de otras variables SES y los tipos de tareas de gestión previstas”.

Los dos mil millones de personas que ya tienen acceso a la *Internet* constituyen el grupo de usuarios más grande en la historia de la humanidad. Ellos deben tener la oportunidad de expresar sus inquietudes en cualesquier negociaciones internacionales sobre los usos del ciberespacio, ya que en muchos casos estas inquietudes probablemente serán diferentes a las del gobierno y otras partes interesadas poderosas. Por ejemplo, los usuarios en lucha contra sus propios gobiernos de hecho rechazarían que esos gobiernos representaran sus intereses con respecto al anonimato, el rastreo en línea y el contenido permitido. Por otra parte, reuniones mundiales recientes sobre el cambio climatológico y el ciberespacio en sí han demostrado que los procesos que están abiertos a grupos que alegan representar los intereses de los ciudadanos individuales rápidamente se pueden tornar difíciles de controlar, consumen mucho tiempo y son poco productivos. Por ese motivo, una interpretación de la soberanía nacional, por cada estado que represente legítimamente los intereses de sus ciudadanos, es no solo oportuna sino justa.

Lamentablemente, inclusive esta estratagema no disminuirá las partes interesadas relevantes a una cifra razonable. Las negociaciones tendrán que incluir representación de los sectores industriales, especialmente ICT, y organizaciones internacionales representadas, al igual que los estados, ya que ellos pueden ofrecer no solo el conocimiento técnico para informar sobre las propuestas sino también bloquear las implementaciones de cualesquier acuerdos a los que se hayan llegado sin ellos. Tal como sugiere Ostrom, la cifra de las partes involucradas puede que no determine en sí la dificultad de llegar a un acuerdo. En cambio, cuando hay más partes involucradas, especialmente cuando los temas son complejos, habrá una mayor cantidad de reclamos concurrentes que toman tiempo reconciliar, si es que se pueden reconciliar. Todas las negociaciones para la Convención de la ONU sobre el Derecho del Mar (CDM), que regula otro espacio común, duraron una década a pesar de basarse en siglos de derecho marítimo y estar más confinadas a asuntos de soberanía del estado. Hay mucha menos tradición jurídica para la cibernética y, hasta ahora, no ha habido ningún esfuerzo concertado para armonizar leyes cibernéticas a nivel estatal. Por lo tanto, la Convención de Budapest sobre el delito cibernético, que ha sido muy limitada y orientada regionalmente, ha sido lenta en lograr el acatamiento, y muchos de sus signatarios han enumerado varias reservas.<sup>23</sup> Quizás algún alivio de estas posibilidades desalentadoras lo podría proveer el ciberespacio en sí, en que el conjunto de opiniones, consultas y negociaciones ahora se pueden llevar a cabo virtualmente al igual que en persona. Al organizar la

información, reducir los costes de transacción y agilizar las comunicaciones, las herramientas cibernéticas podrían permitir la toma de decisiones acerca de sus propios futuros.

### Unidad móvil de recursos (-)

*A causa de los costes de observar y administrar un sistema, la autoorganización es menos probable con unidades móviles de recursos... que con unidades fijas, tales como árboles y plantas o agua en un lago.*

Hay tres tipos de dispositivos de movilidad que hacen que su vigilancia sea difícil y costosa. Primero, como ya se ha mencionado, la condición de un dispositivo puede cambiar rápidamente de “seguro” a “comprometido”, a menudo descubriendo el cambio más tarde, si se descubre. Segundo, durante su transcurso, los ataques y las explotaciones cibernéticas a gran escala típicamente desplegarán diferentes máquinas ubicadas en direcciones IP diferentes y emplazamientos geofísicos. Por ejemplo, durante un ataque distribuido de denegación de servicio distribuido (DDoS, por sus siglas en inglés) en sitios del gobierno estadounidense, los sitios de mando y control (C2) se afirma emigraron de computadoras en Corea del Sur a algunas en Chicago y Berlín. Por lo tanto, cualquier vigilancia o defensa específica a un ataque, como bloquear posibles sitios C2, probablemente incluirá jurisdicciones múltiples con problemas de coordinación consiguientes. Investigaciones posteriores serán similarmente complicadas y la atribución inevitablemente incierta. Como resultado, las partes en un acuerdo que prohíban esos ataques no pueden depender de la vigilancia para verificar que están cumpliendo con el acuerdo o para identificar infractores. Tercero, el surgimiento de la computación móvil en la forma de *laptops*, *smartphones* (teléfonos inteligentes) y tabletas ha aumentado en gran medida la superficie de ataque del ciberespacio y la tarea de cualquier programa de seguimiento en el futuro. La movilidad física de estos dispositivos también significa que durante su vida útil están expuestos a una variedad de amenazas cibernéticas y entornos de vigilancia y a cambios en su propio estatus de seguridad. Serán más vulnerables que una máquina atada a un solo servidor dentro de una organización que cuenta con una seguridad cibernética competente. Son más propensos a la penetración, el robo de su información y el compromiso. Una vez comprometidos, se pueden convertir en portadores para redes comprometedoras a las cuales se conectan más tarde, algo parecido a las intranets empresariales.<sup>24</sup>

### Importancia de los recursos para los usuarios (+)

*En casos exitosos de autoorganización, los usuarios o bien dependen del recurso para gran parte de su sustento o le asignan un valor elevado a la sostenibilidad del recurso.*

Un incremento de actividad alrededor del mundo incluye la creación, recopilación, embalaje, uso y distribución de la información. *La Internet* y otras partes del ciberespacio son esenciales para estas actividades. Varias ponencias del gobierno sobre la seguridad cibernética son claras al reconocer la importancia económica, social, cultural y científica del ciberespacio. Al hacer un llamado para la “creación de una cultura de seguridad cibernética global”, la Asamblea General de la ONU reconoció

la contribución cada vez mayor efectuada por las tecnologías de información en la red a muchas funciones de la vida cotidiana, el comercio y el suministro de bienes y servicios, investigación, innovación y el espíritu empresarial, y al flujo libre de información entre los individuos y las organizaciones, gobiernos, negocios y la sociedad civil.<sup>25</sup>

Inclusive regímenes autoritarios en Irán, Egipto y en otras partes quienes enfrentaron protestas masivas organizadas por medios cibernéticos han titubeado cerrar la *Internet* en sus propios países a causa de la dependencia de sus economías en la misma.

Sin embargo, gobiernos y diplomáticos, han sido menos claros en reconocer cuán fundamental la confianza del pueblo es para el ciberespacio. Al solicitar discusiones sobre normas internacionales para el ciberespacio, el grupo de la ONU de expertos gubernamentales adoptó principalmente una perspectiva de seguridad nacional: El delito cibernético y otros tipos de amenazas cibernéticas son perjudiciales para las funciones gubernamentales, económicas y sociales; la falta de un entendimiento común sobre las intenciones detrás de ciertos comportamientos en el ciberespacio puede crear conflictos que pueden intensificarse y amenazar la seguridad internacional.<sup>26</sup>

### Productividad del Sistema (+)

*Si un recurso ya se ha agotado o es muy abundante, los usuarios no verán la necesidad de administrar en el futuro. Los usuarios necesitan observar algo de escasez antes de invertir en la autoorganización.*

El crecimiento del delito cibernético, el índice de ataques y explotaciones, la proliferación del *malware* y las amenazas a la infraestructura cibernética crítica han planteado preguntas sobre si los beneficios del ciberespacio se pueden sostener bajo las prácticas de seguridad actuales. Esas preguntas claramente motivan los diferentes llamados para acuerdos internacionales sobre el comportamiento ciberespacial. Jacques Bus destaca que la posibilidad de que los estados estén detrás de muchas de las amenazas cibernéticas “es prueba de la urgencia de llegar a acuerdos internacionales sobre refrenamientos en y la defensa contra ataques cibernéticos y de contar con una cooperación internacional para controlarlas”.<sup>27</sup> Después de identificar la confianza del pueblo como un recurso escaso en el ciberespacio, Bus continúa expresando que, “Los sectores público y privado tienen que trabajar juntos a nivel internacional para crear una infraestructura bien balanceada de tecnología y leyes/regulación que les otorgue a los ciudadanos la confianza de usar las oportunidades del nuevo mundo digital”.<sup>28</sup> En un discurso pronunciado en la Conferencia sobre Seguridad en Munich en el 2011, el ministro de relaciones exteriores británico, William Hauge, hizo conexiones similares:

*Estamos trabajando con el sector privado para garantizar una infraestructura crítica segura y fuerte y la base de destrezas fuertes necesarias para sacarle provecho a las oportunidades económicas del espacio cibernético, y para crear una concienciación sobre las amenazas en línea entre los miembros del público. Pero al ser globales, las amenazas cibernéticas también requieren una respuesta colectiva. En Gran Bretaña creemos que ha llegado el momento de comenzar a buscar un acuerdo internacional sobre las normas en el ciberespacio.*<sup>29</sup>

### Previsibilidad de la dinámica del sistema (0)

*La dinámica del sistema necesita ser lo suficiente predecible de manera que los usuarios puedan calcular qué sucedería si ellos estableciesen leyes particulares o territorios a los que no se puede entrar.*

Las consecuencias de no contar continuamente con una regulación internacional son más predecibles que el efecto del acuerdo y vigilar en busca de algunos patrones de comportamiento. Con el deterioro de la confianza del pueblo en el ciberespacio, la expansión del uso—en términos de tiempo invertido, aplicaciones y dependencias—disminuirá y eso estará acompañado por menos crecimiento o disminución en los incentivos para el desarrollo. Algunos usuarios puede que ya hayan reducido su uso de las redes públicas para la transmisión crítica de datos; algunas organizaciones han reducido el número de puntos de acceso o portales para ellos. Estas medidas puede que crezcan hacia la separación y la fragmentación generalizadas—fenómenos que le quitan valor al ciberespacio.

Proyectar la pérdida en valor de un ciberespacio vulnerable en comparación con uno seguro es problemático porque hay diferentes modelos para evaluar el valor socioeconómico de las redes cibernéticas. No obstante, parece razonable suponer que a medida que usuarios nuevos provenientes de estratos económicos inferiores y países menos desarrollados, el valor económico de las redes aumentará a un régimen más bajo que en las etapas iniciales de su crecimiento.<sup>30</sup> Esa tendencia cuenta con implicaciones mixtas para la autoorganización. Primero, los proveedores tendrán pocos incentivos para aumentar sus inversiones en la seguridad cibernética—especialmente si los costes de seguridad corresponden a la cantidad de usuarios. Pero la falta de acción por parte de los proveedores pondría más presión en los gobiernos para que busquen acuerdos que disminuyan las amenazas. Por otra parte, la tendencia también sugiere que cualquier retiro de los usuarios no disminuirá inicialmente el valor de la red. Por lo tanto, hasta que la situación se considere intolerable y no solamente mala, los gobiernos, conscientes de los costes de los acuerdos, podrían resistir la presión y demorar la autoorganización, a pesar de que su pueblo exige acción.

### Liderazgo (0)

*Cuando algunos usuarios de cualquier tipo de sistema de recursos cuentan con destrezas empresariales y son respetados como líderes locales como un resultado de la organización previa para otros fines, la autoorganización es más probable.*

Al liderazgo le faltan negociaciones a nivel estatal, potencialmente productivas, pero no por falta de actores que han desempeñado papeles en organizar el ciberespacio. Durante la última década, *Internet Corporation for Assigned Names and Numbers (ICANN)* (Corporación para la Asignación de Nombres y Números en *Internet*) ha provisto la administración competente, aunque criticada frecuentemente, de las asignaciones de ámbitos y supervisión de los registros. Ha acomodado el crecimiento espectacular de la *Internet* y las demandas comerciales que lo acompañan con un rediseño de políticas para dominios de nivel superior. Si bien no ha sido particularmente abierta a la participación popular especificada en su modelo de múltiples grupos interesados, ha retenido la confianza de los proveedores de servicio y el respeto de la mayoría de los estados, tal como lo comprueba la restricción de la ONU de buscar participación en la administración de la *Internet*. Pero la ICANN no es un especialista en normas y carece de las destrezas políticas y la influencia para reconciliar los intereses en competencia entre los estados en cuanto a comportamientos cibernéticos y seguridad. Además, muchos estados la consideran una herramienta de la política estadounidense.

La *Internet Engineering Task Force (IETF)* (Fuerza de Tarea de Ingeniería de *Internet*) ha ejercido liderazgo en los protocolos de *Internet*, en su mayoría como el endosante de normas. Su propia historia es un ejemplo de autoorganización entre las partes interesadas para la gestión de un espacio común, pero su proceso amorfo de toma de decisiones es un modelo difícil para las negociaciones en cuanto a refrenar las actividades de seres humanos. En todo caso, no está calificada para estar al frente de esas negociaciones, su ámbito está limitado al ámbito técnico, su importancia en ese ámbito ha disminuido a medida que las inquietudes ahora se enfocan más en aplicaciones móviles y otras capas más allá de su alcance, y su membresía aún es estadounidense y europea en su mayoría.<sup>31</sup>

El *International Telecommunications Union (ITU)* (Sindicato Internacional de Telecomunicaciones), la agencia de la ONU responsable del ICT, tiene la ambición de estar al frente de la formulación de políticas y la administración del ciberespacio, y estuvo a cargo de la organización de la *World Summits on the Information Society (WSIS)* (Cumbres Mundiales sobre la Sociedad de la Información), que se enfocaba en aspectos menos trascendentes: usos del ciberespacio orientados hacia el desarrollo, gobernanza de la *Internet*, reducción de brechas digitales. Considerada en occidente como una herramienta para los intereses políticos rusos y chinos, carece de credibili-

dad política para asumir el liderazgo en aspectos difíciles tales como espionaje cibernético, derechos de información y así por el estilo. Probablemente también carece de capacidad tecnológica; las normas de seguridad cibernética que creó y promovió en colaboración con la *International Organization for Standardization (ISO)* (Organización Internacional para la Estandarización) resultaron ser costosas y poco viables.

### Normas/Capital Social (+)

Si los usuarios comparten normas de reciprocidad y confían entre sí lo suficiente para acatar acuerdos, enfrentarán costes de transacción más bajos al llegar a acuerdos y monitorear. La globalización económica en curso y la ausencia de guerras interestatales importantes pudiesen sugerir que las potencias principales están desarrollando estructuras de reciprocidad adecuadas y mecanismos para evitar conflictos. De hecho, esta evaluación es sustentada por los temores expresados en los llamados para normas cibernéticas que los malos entendidos acerca de los comportamientos ciberespaciales podrían desencadenar conflictos no deseados. No obstante, no llevar a cabo negociaciones sobre regulaciones ambientales suscita dudas que a las negociaciones sobre el ciberespacio les vaya mejor, especialmente en vista de que las grandes potencias tienen diferencias ideológicas sobre el ciberespacio, tan grandes como las diferencias entre los intereses económicos que bloquean las resoluciones de los problemas ambientales.

En términos generales, los políticos rusos y chinos buscan extender el principio de soberanía nacional al ciberespacio estableciendo una norma de que el estado sea el árbitro final en asuntos relacionados con el ciberespacio en su territorio.<sup>32</sup> Desde una perspectiva occidental, sus motivos son controlar el espacio ideacional que las redes cibernéticas le permiten a sus pueblos y evitar averiguaciones en cuanto al uso de la cibernética por sus gobiernos o representantes para campañas militares, espionaje político, espionaje industrial y delincuencia. No obstante, recuerden que las tradiciones políticas en Rusia y China, inclusive en los días antes del comunismo, les otorgaba el poder a las autoridades estatales de decidir qué debían pensar sus ciudadanos, y que el principio de soberanía nacional bloquea a extranjeros de interferir con el ejercicio de ese poder. Además, los funcionarios rusos están plenamente conscientes que los insurgentes o terroristas chechenos han empleado tecnologías cibernéticas en sus luchas violentas contra Rusia. Entonces, una *Internet* descontrolada puede ser políticamente amenazante y fácil de explotar por rivales externos, en particular en Estados Unidos. Por ejemplo, cuando protestas alimentadas por la cibernética ocurrieron en Rusia, Vladimir Putin, el premier, candidato presidencial y blanco de las protestas, catalogó esas protestas como la labor de “enemigos extranjeros”.<sup>33</sup> Desde este punto de vista, extranjeros facultando disconformidad dentro de un país no es una contribución al debate público; es “guerra de información” llevada a cabo para debilitar regímenes al punto de mayores adaptaciones con extranjeros o inclusive el derrumbe. En el 2008 Rusia, China y otros integrantes de la *Shanghai Coordination Organization (SCO)* (Organización Coordinadora de Shanghai) ya habían acordado prohibir apoyar o auspiciar la diseminación de información potencialmente perjudicial. En septiembre de 2011, en lo que parecía ser una respuesta al apoyo por parte de gobiernos extranjeros y diásporas al activismo cibernético en el mundo árabe, Rusia propuso que los países anotaran las actividades en línea de sus residentes sospechosos de esas diseminaciones.

En cambio, Estados Unidos y sus aliados de la OTAN tienden en sus declaraciones a considerar el ciberespacio como una institución central para la economía global, un medio para el intercambio mundial científico y cultural, un espacio común para el debate político y el desarrollo y un medio social. En vista de esta variedad de funciones, de ahí también el modelo de múltiples partes interesadas para el control y defensa del ciberespacio, con los estados siendo un tipo de parte interesada, junto con las organizaciones no gubernamentales, proveedores de servicios, compañías ICT, entidades de infraestructura crítica, usuarios empresariales y usuarios individuales. Pero en vista de que el ciberespacio, particularmente la *Internet*, es víctima de ataques y ex-

plotaciones de delincuentes, terroristas e inclusive estados, en virtud de su autoridad y capacidades, los estados tienen la responsabilidad principal de proveer la seguridad necesaria sin dañar los intereses de otras partes interesadas. La diseminación de normas y tratados, tales como la *Budapest Convention on Cybercrime* (Convención de Budapest sobre el Delito Cibernético), son instrumentos para cumplir con esa responsabilidad, al igual que la promoción de una cultura y capacidades de seguridad cibernética alrededor del mundo.<sup>34</sup>

Este enfoque, combinado con una visión de la *Internet* de hace una década, hace caso omiso de los cambios demográficos y tecnológicos que están rehaciendo el ciberespacio y las expectativas para él: el cambio de cientos de millones de usuarios concentrados en América del Norte y Europa conectados a la *Internet* a través de computadoras a billones de usuarios con la mayor parte en el sur y el este de Asia conectados a través de dispositivos móviles y el surgimiento de una *Internet* de cosas. Como resultado, aquellas prácticas que una vez parecían estar en el interés de todos ahora son controversiales y refutadas.<sup>35</sup> India, Brasil y América del Sur—las voces principales en asuntos cibernéticos entre los países “no alineados”—quieren que estos cambios sean reconocidos como partes principales concedidas en cualesquier negociaciones. Por consiguiente, favorecen la transferencia de autoridad lejos de agencias orientadas hacia la tecnología, reflejando el modelo de partes interesadas múltiples, inclusive ICANN e IETF, hacia una agencia más orientada hacia la política, posiblemente bajo la ONU, aunque no necesariamente la ITU, que le concede a cada estado una misma voz.

### Conocimiento del SES (+)

*Cuando los usuarios comparten un conocimiento común de atributos SES relevantes, cómo sus acciones los afectan entre sí y otras reglas empleadas en SES, ellos percibirán costes de organización más bajos.*

Los diversos llamamientos para reglas cibernéticas reflejan el conocimiento de los encargados de formular leyes que ciertos comportamientos trastornan las actividades normales, siembran la desconfianza del pueblo y amenazan la sostenibilidad del ciberespacio. Su disposición para discutir problemas más allá de los delitos cibernéticos reconoce que aquellos que se comportan mal pueden incluir sus propios gobiernos y ciudadanos. Por lo tanto, se necesitan menos tiempo y dinero para despertar la conciencia o convencer a los escépticos que hay un problema y que la cooperación internacional puede ayudar a resolverlo. Elegir qué se va a hacer requiere más conocimiento de las dependencias entre los diversos procesos en el ciberespacio, particularmente cómo las posibilidades tecnológicas afectan los comportamientos sociales (de los agentes). Los esfuerzos de contar con reglamentación ambiental muestran que aquellos que se sienten amenazados por la propuesta de soluciones amplias y exhaustivas se opondrán, inclusive si se les ofrecen pagos adicionales. Entonces el problema de que el espacio tiene que degradarse con la selección de algún blanco cuya solución propuesta podría lograr tracción, ayuda a reducir el nivel general de la inseguridad cibernética y crear confianza entre los diversos agentes, permitiendo así la búsqueda de otros blancos. Una sugerencia frecuente es que los estados cooperan para reprimir las pandillas de delincuentes cibernéticos negándoles sus medios de cobrar en efectivo sus robos. Esta sugerencia comprende que (a) la dependencia de las pandillas en ciertos bancos y (b) el delito cibernético sirven como un laboratorio de desarrollo y prueba para malware que más tarde será utilizado por las agencias de inteligencia en algunos estados. Menos conocido es el hecho de cuán fuerte estas agencias dependen de las pandillas y, por lo tanto, los incentivos que sus estados necesitan para cooperar con la propuesta.

### Normas de Opciones Colectivas (0)

*Cuando los usuarios cuentan con la autonomía total al nivel de opción colectiva para diseñar y hacer cumplir algunas de sus propias reglas, tienen costes de transacción más bajos al igual que costes más bajos en defender el recurso contra la invasión por otros.*

Esta variable implica que mientras más personas puedan considerarse a sí mismas como los autores de las reglas que se esperan ellos acaten, más personas acatarán esas reglas. Esto es importante para la seguridad cibernética y la confianza del pueblo en el ciberespacio, porque una buena “higiene en la computadora” a los niveles institucional e individual puede eliminar una cantidad considerable de delitos y explotaciones, quizás tanto como un ochenta por ciento.<sup>36</sup> Lamentablemente, la cantidad de usuarios y la dispersión de su representación pareciera excluir la participación del pueblo en formular leyes, tal como se mencionó anteriormente. Por consiguiente, los usuarios podrán ver su acatamiento a las reglas como parte de un esfuerzo global interdependiente para sostener el ciberespacio y, por lo tanto, para su propio beneficio. Las directrices que reciban de los superiores probablemente justificarán las reglas solamente en términos de proteger al individuo o la organización.

### Cambiando las variables y respuesta en caso de una crisis

Los valores de las variables de Ostrom, resumidas en la tabla a continuación, no favorecen la autoorganización en el SES cibernético. Las condiciones no son oportunas para acuerdos productivos, que se puedan poner en vigor bajo los cuales las partes interesadas, especialmente los estados, limiten sus comportamientos cibernéticos que merman la confianza. Tal como lo indican los valores positivos para las variables “importancia del recurso” y “productividad del sistema”, las expresiones generalizadas de temor por el futuro del ciberespacio han suscitado interés en esos acuerdos. Sin embargo, no se debe esperar nada más allá hasta que los valores de algunas variables tecnológicas y otras variables sociales cambien. Podría decirse que la búsqueda ahora de un acuerdo global exhaustivo o una alternativa a los acuerdos entre aquellos que “piensan igual” será contraproducente. Probablemente profundizará la desconfianza entre las potencias cibernéticas principales y desalentará compartir el conocimiento útil del SES cibernético. Ese parece ser el resultado principal de la reciente conferencia en Londres sobre las “reglas del juego” cibernéticas.<sup>37</sup>

Variable	Valor
Tamaño del recurso	-
Número de usuarios	-
Unidad móvil del recurso	-
Importancia del recurso	+
Productividad del sistema	+
Previsibilidad de la dinámica del sistema	0
Liderazgo	0
Normas/capital social	+
Conocimiento del SES	+
Normas de opciones colectivas	0

Varias medidas factibles podrían mejorar las perspectivas para acuerdos eficaces o sostener la confianza del pueblo en el ciberespacio. Consideren lo siguiente.

### Crear Gestión de Identidad Global

Jacques Bus recomienda la creación de un “sistema fidedigno interoperable y global para la identificación y autenticación” como esencial para la confianza entre los usuarios de *Internet*.<sup>38</sup> Los estados, inclusive algunas democracias liberales, ya les están exigiendo identificación a los usuarios de *Internet*. La interoperabilidad de las normas locales facilitaría, de ser necesario, la identificación de un usuario de un dispositivo enlazado a la *Internet* en cualquier lugar. Los usuarios tendrían su anonimato o privacidad bajo este régimen, ya que diferentes sitios y transacciones exigirían diferentes grados de divulgación. Los regímenes autoritarios podrían identificar más fácilmente a personas en redes cibernéticas de resistencia, pero encontrarían que están mejor al no identificar a aquellos que muestran una resistencia no violenta, mientras tratan de identificar y reprimir los violentos. Esa estrategia podría canalizar a los opositores hacia redes no violentas y darles a los regímenes más espacio para respirar. Su restricción en este aspecto podría permitirles a los estados que apoyan a sus opositores a cooperar en el sistema de identificación. En términos de las variables de Ostrom, la gestión de la identidad disminuye algunos de los efectos nocivos de la movilidad del recurso.

### Aumentar la participación del pueblo en la seguridad cibernética

Las discusiones sobre las políticas de seguridad cibernética en públicos informados y relevantes pueden tener el efecto doble de poner presión en los gobiernos nacionales respectivos e involucrar a esos pueblos en los procesos de formulación de políticas. La resolución de la ONU para la “creación de una cultura global de seguridad cibernética” prevé que la seguridad cibernética nacional tendrá una participación amplia de la sociedad, inclusive la del sector privado, la sociedad civil, el mundo académico e individuos, pero permanece callada con respecto a las funciones de formulación de políticas para los actores no gubernamentales. Las asociaciones públicas-privadas que ya han surgido en Europa y América del Norte parecen estar enfocadas en coordinar esfuerzos a nivel empresarial y compartir información, sin criticar ni cambiar las políticas. Pero a los miembros no gubernamentales, particularmente cualquier corporación transnacional (TNC, por sus siglas en inglés), por ejemplo *Freedom House*, se les debe exhortar que sugieran reglas. Muchos han experimentado ataques cibernéticos en una variedad de entornos legales y tecnológicos y probablemente saben mejor que los observadores o gobiernos cuáles leyes y prácticas cibernéticas deben armonizar con los países como parte de los acuerdos internacionales.

The Internet Governance Forum (IGF) (Foro de la Gobernanza de *Internet*), un órgano consultivo establecido por la ONU y basado en un modelo de partes interesadas múltiples, también podría utilizarse para que el pueblo hiciese aportes en las conversaciones a nivel global sobre las reglas para el ciberespacio. En sus reuniones se han discutido temas sobre la seguridad cibernética pero hasta el momento ha dejado en manos de los gobiernos nacionales y agencias especializadas las propuestas para la política. Pero el IGF podría utilizar herramientas y técnicas cibernéticas, tales como sondeos en línea y colaboración del público para recopilar y agregar opinión pública acerca de reglas y regulaciones necesarias en cualquier acuerdo futuro.

### Creando la Confianza mediante la Cooperación Internacional en una Tarea “Fácil”

Aunque puede que acuerdos exhaustivos sobre los comportamientos en el ciberespacio fuesen inalcanzables, la cooperación internacional en algunas amenazas cibernéticas y emergencias puede ser fuerte y eficaz, por ejemplo, la respuesta mundial al gusano *Conficker* y la alianza de trabajo de los CERT de Japón, China y Corea del Sur. En estos casos, la cooperación se basa en “normas invisibles” o compromisos compartidos entre los tecnólogos cibernéticos, pero le puede dar alguna confianza a los formuladores de política que están observando a sus países colaborando juntos sobre los problemas cibernéticos. Por lo tanto, su confianza puede crecer con más

casos donde un reto provoca un compromiso profesional ampliamente compartido y la cooperación resultante logra algo de éxito. Algunos delitos cibernéticos parecen ser candidatos aptos para el reto, notablemente la pornografía infantil, el fraude de bajo nivel, y el robo de identidad. Sin embargo, hay una necesidad que alguna agencia esté al frente de promover la urgencia de reprimir el delito seleccionado.

Este artículo ha empleado el reduccionismo económico para argumentar que no se dan aún las condiciones para llegar a y hacer cumplir acuerdos internacionales sobre los usos del ciberespacio. El argumento sostiene que si las personas que explotan un espacio común saben que la explotación exagerada degradará ese espacio común, ellos pueden acordar a limitar su comportamiento, siempre y cuando los costes de llegar a un acuerdo y hacerlo cumplir sean asequibles. En este argumento, la autolimitación está en servicio del interés personal—sostener sus propios beneficios del espacio común. En lo que respecta al actor, ya sea un individuo, organización o nación, el ciberespacio es tan solo otro ámbito donde busca su propio interés personal. El ciberespacio, por supuesto, es mucho más rico. Se ha convertido en la base y el medio para reorganizar gran parte de la vida contemporánea social, económica, cultural e intelectual en los países desarrollados. Provee un medio principal para una conversación global sobre asuntos compartidos. En la medida en que retenga la confianza del pueblo, el ciberespacio cultiva nuevos lazos sociales e identidades que aumentan los preexistentes, como la nacionalidad. Por todo ello, exige algo de lealtad.

Inclusive sus defensores no piensan que un acuerdo cibernético internacional protegería lo suficiente a estados, organizaciones e individuos de los diferentes ataques que surgen en el ciberespacio. Aunque un tratado sería una restricción en sus signatarios y facilitaría las sanciones de sus infractores, una defensa cibernética adecuada al nivel estatal aún exigiría resistencia (endurecimiento) de las redes digitales, especialmente aquellas que apoyan la infraestructura crítica; resistencia de las organizaciones que probablemente serían atacadas y disuasión razonable con respecto a los no signatarios. A falta de un acuerdo(s) internacional, la dependencia en esos otros componentes aumentaría moderadamente. Además, en vista de que las redes digitales son necesarias para la globalización económica, los estados continuarán cooperando en el plano técnico con respecto a la gobernanza de la *Internet* al menos hasta el punto de garantizar la interoperabilidad al nivel global. Esa cooperación no se extenderá a controlar el espionaje industrial, proteger infraestructuras de información crítica o garantizar la libertad de información, tres temas que han surgido recientemente como los focos de desconfianza entre los estados. Estos y otros problemas cibernéticos al nivel internacional probablemente se discutirán en un futuro a medio plazo en una manera fragmentada y gradual—la estrategia para salir del paso. Estos no son necesariamente malos resultados, y pocos usuarios experimentarán alguna pérdida de los beneficios del ciberespacio. Por otra parte, la inseguridad ahí continuará, y la oportunidad de forjar la confianza del pueblo a un nivel global habrá pasado. □

#### Notas

1. *Un General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"* (Asamblea General de la ONU, "Informe del Grupo de Expertos Gubernamentales sobre los Desarrollos en el Campo de la Información y las Telecomunicaciones en el Contexto de Seguridad Internacional) A/65/201, 30 de julio de 2010, <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.
2. Para un repaso de la conferencia en Londres, consultar a Peter Apps, "Disagreements on Cyber Risk East-West 'Cold War'" ("Desacuerdos sobre el Riesgo Cibernético y la 'Guerra Fría' Este-Oeste"), Reuters, 2 de febrero de 2012, <http://www.reuters.com/article/2012/02/03/us-technology-cyber-idUSTRE8121ED20120203>.
3. "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and OSCE Forum for Security Cooperation" (Declaraciones de la Secretaria Napolitano ante el Comité Conjunto del Consejo Permanente OSCE y el Foro OSCE para la Cooperación de la Seguridad), Comunicado de prensa del Departamento de Seguridad Interna, 1º de julio de 2011, <http://www.dhs.gov/ynews/speeches/2011-napolitano-remarks-osce-council-austria.shtm>.

4. Adam Segal y Matthew Waxman, “Why a Cybersecurity Treaty Is a Pipe Dream” (Por qué un tratado de seguridad cibernética es un sueño imposible), *Council on Foreign Relations (Consejo sobre Relaciones Exteriores)*, 27 de octubre de 2011, <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>.

5. Consultar a G. Hardin, “Tragedy of the Commons” (Tragedia en el espacio común), *Science* 162 (1968): 1243–48, para una formulación clásica del argumento.

6. Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action (Gobernando el espacio común: La evolución de instituciones para la acción colectiva)* (Cambridge, UK: Cambridge University Press, 1990); Ostrom et al., “A General Framework for Analyzing Sustainability of Social-Ecological Systems” (Un marco general para analizar la sostenibilidad de los sistemas socioecológicos), *Science* 325, no. 5939 (24 de julio de 2009): 419–22.

7. Lawrence Lessig, “The Public Domain” (El ámbito público) *Foreign Policy*, 30 de agosto de 2005, [http://www.foreignpolicy.com/articles/2005/08/30/the\\_public\\_domain](http://www.foreignpolicy.com/articles/2005/08/30/the_public_domain).

8. Para esa analogía, consultar Abraham Denmark y James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (El espacio común en pugna: El futuro del poder estadounidense en un mundo multipolar) (Washington: Center for a New American Security, 2010).

9. Al emplear la sociedad de una aldea del espacio común inglesa como su metáfora rectora, los defensores de una Internet donde la información fluye libremente puede que hayan tenido tendencias hacia una visión idílica o prelapsaria. En una revisión desdeñosa de Lewis Hyde, *Common as Air (El espacio común como aire)* (New York: Farrar, Straus, and Giroux, 2010), la labor de uno de esos defensores, David Wallace-Wells, cita la evaluación de E. P. Thompson en su obra clásica *The Making of the English Working Class (La creación de la clase laboral inglesa)* (New York: Vintage Books, 1966) esa cultura agraria inglesa antes del cercamiento era “intelectualmente vacante...y evidentemente pobre”. Hacer caso omiso que el cercamiento obligó a las personas a abandonar sus tierras y no mejoró las vidas de los que quedaron atrás, Wallace-Wells sostiene por analogía que estamos sentenciados a una esterilidad cultural sin los cercamientos de derechos de autor amplios en su “The Pirate’s Prophet: On Lewis Hyde” (El profeta del pirata: Sobre Lewis Hyde) *Nation*, 15 de noviembre de 2010, <http://www.thenation.com/article/155619/pirates-prophet-lewis-hyde?page=0.0>.

10. Para la securitización de la cibernética en Estados Unidos, consultar M. Dunn Cavelti, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Seguridad cibernética y la política de la amenaza: Esfuerzos de EE.UU. de asegurar la era de información) (New York: Routledge, 2008). Para tipos y extensión de las prácticas de cercamiento, consultar Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering (Acceso denegado: La práctica y política de filtrar la Internet global)* (Cambridge: MIT, 2008); y Deibert et al., editores, *Access Controlled (Acceso controlado)* (Cambridge: MIT, 2010).

11. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Estrategia internacional para el ciberespacio: Prosperidad, seguridad y transparencia en un mundo interconectado)* (Washington: The White House, May 2011), [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf). También consultar Secretaria de Estado Hillary Clinton, “Remarks on Internet Freedom” (Comentarios sobre la libertad de la Internet), 21 de enero de 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>. La denuncia prominente del Departamento de Estado del filtrado motivado políticamente por gobiernos extranjeros lo llevó a oponerse a los proyectos de ley del Congreso contra la piratería (SOPA y PIPA) que hubiesen exigido el filtrado motivado comercialmente de sitios web extranjeros.

12. “Jo Twist, Web Guru Fights Info Pollution,” *BBC News*, 13 de octubre de 2003, <http://news.bbc.co.uk/2/hi/technology/3171376.stm>. La intención de otro tipo de consumo exorbitante de ancho de banda, la denegación de servicio distribuido, es infligir directamente otros tipos de costes, tales como reputación, financieros o políticos, en sus blancos al obligar a los servidores de red del blanco a fallar bajo la aglomeración de demandas de servicio. La DDoS puede escalar al nivel de un problema de seguridad nacional, como fue el ejemplo del ataque en el 2007 a los sitios web gobierno estonio e infraestructuras críticas.

13. Discusión de los obstáculos y costes de una seguridad “adecuada” para las tecnologías intrínsecamente vulnerables del ciberespacio están más allá del alcance actual. Además de los costes para personal de seguridad cibernética, se incluyen costes mucho menos estimables para modernizar las culturas empresariales. Muchas empresas, especialmente en el sector financiero, han optado por diferir esos costes y tratar cualquier pérdida al delito o espionaje cibernético como costes de actividades comerciales, a la vez que intentan ocultar esas pérdidas por temor a los costes a sus reputaciones. Cuando este artículo fue a imprenta, supe que L. Jean Camp, “Reconceptualizing the Role of Security User” (Reconceptualizando el papel que desempeña el usuario de seguridad) *Daedalus* 140, no. 4 (2011): 93–107, también aplica el análisis de Ostrom de autoorganización al reto de la seguridad cibernética. Sin embargo, el enfoque de Camp es en las posibilidades de los usuarios finales individuales de formar comunidades a menor escala en las que compartir información sobre amenazas cibernéticas e higiene cibernética se practican eficazmente.

14. Jacques Bus, “Societal Dependencies and Trust” (Dependencias sociales y confianza) en Hamadoun Touré et al., *The Quest for Cyber Peace (La búsqueda del ciberespacio)* (Geneva: International Telecommunications Union, 2011), 18.

15. *Ibid.*, 19, citando a Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (Confianza: Las virtudes sociales y la creación de la prosperidad) (New York: Free Press, 1995), y Robert Putnam et al., *Making Democracy Work: Civic Traditions in Modern Italy* (Haciendo que la democracia funcione: Tradiciones cívicas en la Italia moderna) (Princeton, NJ: Princeton University Press, 1993). Para un ejemplo negativo, consultar a Anthony Padgen, “The Destruction of

*Trust and Its Economic Consequences in the Case of Eighteenth-Century Naples*” (La destrucción de la confianza y sus consecuencias económicas en el caso de Nápoli en el siglo XVIII) en *Trust: Making and Breaking Cooperative Relations (Confianza: Estableciendo y rompiendo relaciones cooperativas)*, editor, Diego Gambetta (London: Basil Blackwell, 1988), 127–41.

16. El uso de los iraníes de las redes anónimas Tor sugiere que algunos usuarios necesitan tanto la cibernética que inclusive una cantidad pequeña de reconfirmación los provocaría regresar a utilizar aplicaciones comprometidas anteriormente, a pesar de los riesgos involucrados. Las gráficas para el uso están adulteradas, mostrando que inmediatamente después que las autoridades iraníes anunciaron un bloqueo o vigilancia de un sitio Tor en particular, la cantidad de usuarios iraníes en la red baja precipitadamente. Luego se vuelve a reponer después que los creadores de Tor anuncian una solución a las medidas iraníes. Consultar <https://metrics.torproject.org/users.html?graph=direct-users&start=2010-11-28&end=2012-02-26&country=ir&dpi=72#direct-users>.

17. Daniel Heller-Roazen, *The Enemy of All: Piracy and the Law of Nations (El enemigo de todos: La piratería y las leyes de las naciones)* (Cambridge: MIT Press, 2008).

18. Oficina de Información del Consejo Estatal de la República Popular China, “*The Internet in China*” (La Internet en China), 8 de junio de 2010, [http://www.china.org.cn/government/whitepaper/node\\_7093508.htm](http://www.china.org.cn/government/whitepaper/node_7093508.htm).

19. Elinor Ostrom, “*General Framework for Analyzing Sustainability of Social Ecological Systems*” (Marco general para analizar la sostenibilidad de los Sistemas Socioecológicos), *Science* 325 (24 de julio de 2009): 419–22.

20. Una opinión de “responsabilidad estatal” es elaborada en el borrador ruso para una “*Convention on International Information Security*” (Convención internacional sobre la seguridad de la información), presentada en la *Second International Meeting of High-Level Officials Responsible for Security Matters* (Segunda reunión internacional de funcionarios de alto nivel responsables de los asuntos de seguridad), Ekaterinburg, Russia, 22 de septiembre de 2011, <http://2012.inforum.ru/2012/files/konvencia-mib-en.doc>. Un problema con cualquier plan que les asigna responsabilidad a los estados por los comportamientos cibernéticos de sus vecinos es que muchos estados carecen de la concienciación de la seguridad cibernética, la capacidad y las destrezas de computación forense. Este problema y el papel que desempeñan muchas naciones avanzadas tecnológicamente de ayudar a que los menos avanzados incrementen sus capacidades son reconocidos en *US International Strategy for Cyberspace* (Estrategia Internacional Estadounidense para el Ciberespacio) y la Resolución de la Asamblea General de la ONU, “*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*” (Creación de una cultura global de seguridad cibernética y evaluación de los esfuerzos nacionales por proteger las infraestructuras de información crítica) A/Res/64/211, 17 de marzo de 2010, <http://www.citizenlab.org/cybernorms/ares64211.pdf>.

21. Chris Demchak y Peter Dombrowski, “*Rise of a Cybered Westphalian Age*” (Surgimiento de una era westfaliana cibernética) *Strategic Studies Quarterly* 5, no. 1 (Primavera 2011), 32–61.

22. Bus, “*Societal Dependencies and Trust*” (Dependencias sociales y confianza) 21.

23. Stein Schjøllberg, “*Wanted: a United Nations Cyberspace Treaty*” (Se busca: Un tratado ciberespacial de las Naciones Unidas) en Andrew Nagorski, editor, *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway* (Disuasión cibernética global: Opiniones de China, Estados Unidos, Rusia, India y Noruega) (New York: EastWest Institute, 2010), 11.

24. Ellen Nakashima y William Wan, “*In China, Business Travelers Take Extreme Precautions to Avoid Cyber-Espionage*” (En China, viajeros comerciales toman precauciones extremas para evitar el espionaje cibernético) *Washington Post*, 26 de septiembre de 2011, [http://www.washingtonpost.com/world/national-security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/GIQA6cR0K\\_story.html](http://www.washingtonpost.com/world/national-security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/GIQA6cR0K_story.html). Consultar también a Joel Brenner, *America the Vulnerable* (Estados Unidos, el vulnerable) (New York: Penguin Press, 2011), 61ff.

25. Resolución 64/211 de la Asamblea General de la ONU: “*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*” <http://www.citizenlab.org/cybernorms/ares64211.pdf>.

26. UN General Assembly Resolution 65/201: “*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*” <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.

27. Touré et al., *Quest for Cyber Peace*, 16.

28. *Ibid.*, 25.

29. Discurso del Secretario de Relaciones Exteriores William Hague, “*Security and Freedom in the Cyber Age—Seeking the Rules of the Road*” (Seguridad y libertad en la era cibernética—buscando las reglas del juego) discurso ante la Conferencia de Seguridad en Munich, 4 de febrero de 2011, <http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682>.

30. Según la famosa ley de Metcalfe, el valor de una red es en proporción al número de conexiones cruzadas entre sus usuarios  $N$ , o sea  $N^2$ . El crecimiento (o descenso) en valor con cada usuario que se une (abandona) la red es en proporción a  $2N$ . La ley de Leek que es más extrema, iguala el valor de la red con el número de audiencias específicas que se pueden formar del número de usuarios, v.gr., el número de conjuntos secundarios menos el conjunto nulo de  $N$  o  $2N^2$ . Por lo tanto el valor de la red se duplicaría increíblemente (o se dividiría en la mitad) con cada usuario que se une (o abandona) la red. Una solución más razonable, especialmente para redes grandes, asume el uso diferencial por aquellos en la red. Consistente con las leyes de energía (fenómenos a largo plazo), se supone que el uso disminuya de forma exponencial con la demora en unirse a la red. El uso o transacciones sobre los usuarios  $N$  describe una hipérbola, con los primeros en unirse son los que más usan la red. El beneficio acumulativo, por ende el valor de la red, es entonces proporcional al área debajo de la curva o el logaritmo natural de  $N$  ( $\ln N$ ). El incremento (descenso) en el valor de la red con cada persona que se une (o abandona) es significativamente menos que el calculado por la ley de Metcalfe, y el

cambio es que disminuye en lugar de aumentar. Por lo tanto, si para el proveedor de la red el coste de adquirir un usuario es fijo, se llegará a un punto en la disminución de ganancias del valor.

31. Mi agradecimiento a Phillip Hallam-Baker por la discusión sobre este punto.

32. Borrador Ekaterinburg.

33. Michael Bohm, “*Putin Chasing Imaginary American Ghosts*” (Putin persigue fantasmas estadounidenses imaginario) *Moscow Times*, 9 de febrero de 2012,

<http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html><http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html>.

34. Ver Resolución 62/211 de la Asamblea General de la ONU: “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures,” adoptada el 17 de marzo de 2010.

35. Ronald Deibert y Rafal Rohozinski, “*Contesting Cyberspace and the Coming Crisis of Authority*” (Contienda en el ciberespacio y la crisis venidera de la autoridad) en Deibert et al., *Access Contested* (Acceso impugnado), 21–41.

36. Brenner, *America the Vulnerable*, 239–44; y Brenner, comunicación personal, 2010.

37. Apps, “Disagreements on Cyber Risk East-West ‘Cold War.’”

38. Bus, “Societal Dependencies and Trust,” 24.



**El Dr. Roger Hurwitz**, PhD, es un científico investigador en el Computer Science and Artificial Intelligence Laboratory (CSAIL) (Laboratorio de Ciencias Computacionales e Inteligencia Artificial [CSAIL] de MIT), profesor emérito en el Canada Centre for Global Security Studies (Centro de Estudios de Seguridad Global de Canadá) en la Universidad de Toronto, y fundador de Explorations in Cyber International Relations (ECIR) (Exploraciones en Relaciones Cibernéticas Internacionales [ECIR]), un programa de Iniciativa de Investigación Minera en Harvard y MIT. Entre sus obras actuales se encuentra la investigación de normas cibernéticas internacionales, el desarrollo de sistemas computacionales para datos de eventos y ontología cibernética, y creación de modelos de las complejidades de incidentes cibernéticos de gran repercusión. La labor del Dr. Hurwitz es sufragada por la Office of Naval Research (Oficina de Investigaciones de la Armada). Cualquier opinión, hallazgo y conclusiones o recomendaciones que se expresan en este artículo son las del autor y no necesariamente reflejan la opinión de la Oficina de Investigaciones de la Armada.