Revista de Administración Pública

INAP

Regímenes para la ciberseguridad

Alejandro Pisanty

Resumen: En el presente trabajo se problematiza la definición de Ciberseguridad Nacional, considerando el estado del arte en la consideración de actores nacionales y no nacionales, y las relaciones con actividades como las del delito organizado y la posible negación de gobiernos sobre la actuación de actores no nacionales que los impliquen o favorezcan. Se describen los regímenes aplicables a la gobernanza de la ciberseguridad: el multilateral o intergubernamental, el multisectorial o "multistakeholder" que se ha formado especialmente en gobernanza de Internet, y un régimen híbrido o ecléctico que impera en el ámbito operativo actual. Se comparan las características de dichos regímenes, como las Cibernormas y la Medidas Constructoras de Confianza, para concluir atendiendo a la acción de estados poderosos que apalancan acciones en unos y otros regímenes para ganar espacios estratégicos. Finalmente se atrae la atención del Estado mexicano a esta temática en beneficio de los intereses nacionales.

Palabras clave: Ciberseguridad, Seguridad Nacional, gobernanza de Internet, gobernanza multisectorial, gobernanza "multistakeholder"

Cybersecurity regimes

The definition of National Cybersecurity is scrutinized, considering the state of the art in the study of national and non-national actors, and relationships with activities such as organized cybercrime and the possible plausible deniability of governments with respect to non-national actors who implicate or favor them. Regimes applicable to cybersecurity governance are described: multilateral or intergovernmental; multistakeholder as has emerged in Internet governance; and a hybrid or eclectic regime which applies to the present operational environment. The characteristics of these regimes are compared, as are Cybernorms and Confidence Building Measures, to finish attending to the action of powerful states which leverage their actions from one regime to the other thus gaining strategic spaces. Finally, the attention of the Mexican state is attracted to this problem in benefit of the national interest.

Keywords: Cybersecurity, National Security, Internet governance, multistakeholder governance

Fecha de recepción: 11 de marzo de 2019
Fecha de aceptación: 9 de abril de 2019

Revista de Administración Pública

INAP

Regímenes para la ciberseguridad*

Alejandro Pisanty[1]

1. Introducción

En el presente texto intento reflejar conceptos de la teoría de regímenes internacionales sobre la gestión de la ciberseguridad, especialmente en lo que se refiere a seguridad nacional. Con ello propongo proveer un marco de referencia para la toma de decisiones que considere las diferentes formas de organización que existen en torno a la seguridad en sistemas computacionales y redes de telecomunicaciones, así como la gobernanza de Internet y permita orientar a diferentes organismos del Estado y de la sociedad en su actuación.

* Esta investigación se llevó a cabo con apoyo del Departamento de Física y Química Teórica y de la Coordinación de Asignaturas Sociohumanísticas de la Facultad de Química de la UNAM. La Lic. Fátima Cambronero, de la Internet Society y la firma Ríos Abogados, S.C. hizo una lectura crítica de una versión inicial del presente artículo, que contribuyó a lo poco bueno que el mismo podrá ofrecer. Asumo la responsabilidad del resultado agradeciendo a la vez su colaboración.

1 Doctor en Química por la Universidad Nacional Autónoma de México y profesor de tiempo completo de la Facultad de Química de la UNAM. Estudios postdoctorales en el Instituto Max-Planck de Investigaciones sobre el Estado Sóido, Stuttgart, Alemania. Su actividad se refiere a la gobernanza de Internet y de la tecnología en general; relaciones ciencia-tecnología-sociedad; Sociedad de la Información, e-gobierno y educación o e-learning; y estrategias digitales nacionales, regionales y locales. Ha impartido cursos en la UNAM, el INAP, el ITAM, INFOTEC y el CIDE. Ha sido funcionario de la UNAM y de organismos internacionales como ICANN y la Internet Society.

La seguridad de las sociedades actuales enfrenta nuevos riesgos con el desarrollo y acceso generalizado a Internet. El término "ciberseguridad" se utiliza para describir el complejo de interacciones entre el ciberespacio y la seguridad personal, pública y nacional. En el presente trabajo describo los regímenes dominantes para el análisis de la ciberseguridad (multilateral y multisectorial o "multistakeholder") y añado a consideración otros dos, el de "Administración de TI" y el de "Cibernormas", explicando su relación con los dos primeros. Describo la efectividad relativa de cada uno de ellos en el tratamiento de la ciberseguridad en diferentes planos. Previamente y para entender mejor esa evaluación, describo algunos problemas que son específicos a la ciberseguridad, como la ventaja estructural del atacante sobre la defensa, el problema de atribución del origen del ataque, y algunos problemas emergentes. Finalmente oriento la discusión para que el análisis realizado en el texto sirva a la formulación y ejecución de estrategias de ciberseguridad a nivel nacional aunque también en formas aplicables a las regionales y locales, en contraste con las propuestas de organismos internacionales como la Organización de Estados Americanos (OEA).

2. Ciberseguridad

2.1 Definiciones

Sería conveniente empezar con una definición de "ciberespacio" y aun esta tarea aparentemente sencilla encuentra muchas dificultades. En una época no lejana el ciberespacio estaba definido por computadoras, ante todo, algunas de ellas conectadas a redes. Hoy es casi sinónimo de Internet, aunque preferimos reservar este nombre para la interconexión global de redes accesibles unas desde otras, utilizando un sistema normalizado (el protocolo IP) y un espacio único de direcciones numéricas IP (IPv4 o actualmente también IPv6). Muchas lecturas del término "Internet" abarcan también los recursos computacionales, los dispositivos móviles, los sistemas de información e incluso a los usuarios y sus prácticas.

¿Y el ciberespacio? "casi lo mismo pero más", el universo de sistemas y personas conectados por medio de telecomunicaciones (digitales en su mayoría), del que

Internet sería vehículo (en la definición restrictiva), subconjunto (en la definición más lata) y paradigma, en una definición de ciberespacio asimilada a la de Sociedad de la Información de Castells.

La palabra "ciberseguridad" engloba significados muy diferentes para distintos actores sociales, y su polisemia varía a lo largo del tiempo. Puede referirse a la seguridad de los sistemas informáticos o a toda afectación de la seguridad (física, personal, pública o nacional) que provenga de sistemas informáticos y computacionales o de Internet. Puede ser considerada materia de trabajo de los técnicos informáticos o de las representaciones nacionales en la ONU, motivo de angustia por el futuro de los niños o materia de frío análisis actuarial en una compañía de seguros.

En este artículo dejaré jugar esta polisemia, acotándola al avanzar pero dejando una "ambigüedad creativa", como el experto diplomático Markus Kummel (2004) caracteriza a amplios campos del lenguaje diplomático. Una definición oficial de referencia es "la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada" (México, Gobierno de, 2011). Esta definición se ha considerado tanto más general como más particular que la de "seguridad de la información", lo cual ilustra las dificultades que estamos discutiendo.

Para fines operacionales, desde luego, las definiciones mejor acotadas se refieren a los activos de información, de cuya protección deriva el diseño de la protección de los datos y documentos, las bases de datos, los sistemas de información computacionales, las computadoras y las redes. Los atributos de la información que deben ser administrados en esta protección son, en la definición más ceñida generalmente aceptada, integridad, autenticidad y confidencialidad; definiciones más amplias incluyen ciertamente la disponibilidad y en muchos casos el no-repudio (Daltabuit, 2007)

Las dificultades actuales para acotar la definición de ciberseguridad provienen que conforme más y más

sistemas humanos y sociales dependen de la computación y de Internet, es posible afectar objetos físicos, personas, sistemas de la sociedad y sociedades enteras a través de la afectación o manipulación de sistemas informáticos. Características específicas de Internet facilitan aún más esta interacción entre lo "cíber" y el resto de los sistemas de las sociedades: apertura, masificación, capacidad de ocultar u ofuscar la identidad, carácter transjurisdiccional, reducción de barreras y reducción de fricción. Cada una de éstas tiene efectos positivos universalmente apreciados, y aspectos que en distintas sociedades son mayor o menormente considerados negativos.

En muchos casos los efectos de Internet en la seguridad (personal, pública, nacional; patrimonial, reputacional, física) se deben además a las "affordances" o "prestaciones" descritas por Nancy Baym (Baym, 2015) como alcance, estructura temporal, colapso contextual, y amplificación. En este nivel estamos hablando de "psyops" ("operaciones psicológicas"), "guerras de información" como las descritas por Arquilla y Ronfeldt ((Arquilla, 1993) en la corporación RAND, o, en términos más llanos, de propaganda y subversión.

Otro factor que complica el tratamiento de la ciberseguridad, especialmente en tanto que seguridad nacional, es que la mayor parte del conocimiento existente sobre seguridad nacional parte de la premisa de que ésta se dirime entre Estados. En ciberseguridad el papel de actores no estatales (Kello, 2013) en la ejecución o como blanco de acciones hostiles llega a condicionar las capacidades del Estado. Ejemplos de este condicionamiento o de capacidad activa son: el delito organizado, el terrorismo, empresas privadas que poseen capacidades e información necesarios para la acción del Estado, empresas cuyos activos son el blanco de acción de actores estatales y grupos de la sociedad civil o de la comunidad técnica, sin cuya participación el Estado no tiene la capacidad de actuar defensivamente.

Es imprescindible añadir que el enfoque generalmente aceptado para administrar la seguridad es el de gestión o administración de riesgos (Corona, 2019), (Kure, 2018). La palabra "seguridad" tiene una alta carga emotiva

que obnubila los análisis. La gestión de riesgos, por el contrario, permite enunciar explícitamente los riesgos, cuantificarlos en probabilidad e impacto, y aplicar diversas técnicas como evasión, reducción, transferencia del riesgo, la detección de eventos, respuesta, mitigación, ejecución de planes de contingencia y recuperación de la continuidad de las operaciones. En una gestión racional las medidas siguen un principio de proporcionalidad con base en una relación costo-beneficio.

2.2 Ámbitos

Una de las dificultades que derivan del uso polisémico de la palabra "ciberseguridad" es que abarca ámbitos muy diversos, en los cuales los actores, los problemas y las soluciones son diferentes. No está exento de complicaciones el hecho de que estos ámbitos estén concatenados y si bien algunos problemas se pueden definir claramente como pertenecientes a cada uno de los ámbitos, las fronteras entre éstos no son tajantes.

Los principales ámbitos de la ciberseguridad son seguridad personal, seguridad pública y seguridad nacional. En el primero imperan la confidencialidad, la intimidad, la protección de datos personales, el patrimonio y la reputación; en el segundo la palabra clave es "delito" y por lo tanto prevención, persecución, legislación, procedimientos policiales, judiciales y penales, investigación forense; la seguridad nacional, por último, se refiere, al hablar de ciberseguridad, a la estabilidad del Estado y la seguridad de la nación, su independencia y autonomía, la preservación de la soberanía, la funcionalidad, estabilidad y seguridad de las infraestructuras críticas y la capacidad de operación de la sociedad en su conjunto y la del Estado y el gobierno en particular. Más que en los tradicionales dominios de tierra, mar, aire y espacio, en ciberseguridad las infraestructuras y operaciones críticas incluyen entes privados, como banca e industria.

Como se señaló en un párrafo anterior estos ámbitos están concatenados. Una afectación a cuentahabientes de la banca mediante "phishing" puede afectar sólo a unos cuantos y constituir un problema de seguridad personal y quizás de seguridad pública. El mismo ataque, llevado a

gran escala, puede llevar a suspender el funcionamiento de las estructuras financieras de un país, por muchos días, y generando no sólo su suspensión, sino incertidumbre acerca de su estabilidad; en un caso así el ataque ya no sólo afecta a las personas o a los negocios sino al país entero y se convierte en un problema de seguridad nacional. En dirección inversa, un ataque delictivo masivo puede ser propiciado por un Estado pero éste podrá negar su intervención, culpando a delincuentes no controlados. El ataque a las infraestructuras de Estonia (Ottis, 2008), que ya ha alcanzado estatura de histórico, es un buen ejemplo.

2.3 Problemas

Algunos problemas característicos de la ciberseguridad son los siguientes:

2.3.1 Ventaja estructural del atacante

La naturaleza de Internet (Pisanty, Principios fundamentales y gobernanza de Internet, 2016), (Pisanty, Llámame Internet, 2018;) da una ventaja estructural al atacante (Gartzke, 2015), Internet como dominio bélico es diferente de los dominios terrestre, naval, aéreo y espacial, ya que es un medio íntegramente construido por el hombre, y cuyas estructuras y reglas son por tanto un producto humano. Esta consideración invitaría a preguntar si es posible reestructurar Internet para que favorezca al defensor o al menos reduzca la ventaja del atacante. Lamentablemente –para el lector que se ponga del lado de la defensa– no hay esperanza alguna de revertir la situación en ningún horizonte temporal razonable. Sí son posibles algunas inversiones de la ventaja del atacante, pero hasta ahora temporales y locales.

La ventaja del atacante en Internet se basa en que es posible tener acceso a la red y operar en ella sin que se exija identificación o autenticación alguna, y por ello sea fácil amplificar los recursos del ataque en múltiples puntos, así como ocultar o al menos ofuscar –como se dice en la jerga técnica– la identidad del atacante, de tal manera que éste se considera exento de riesgo de respuesta o castigo y por ello está fuera del alcance de la disuasión. En cambio los recursos que interesa atacar están centralizados o al menos ubicados en posiciones fijas y conocidas– el sitio Web o

los sistemas informáticos internos de un banco, de un gobierno, de un ejército– están montados en computadoras y éstas se identifican mediante direcciones IP que terminan por ser conocidas, ya por ser públicas por necesidad del servicio, ya por ser posible identificarlas mediante sucesivas operaciones de reconocimiento de la red por parte de los atacantes.

Otro factor decisivo que da ventaja al atacante es que en muchos tipos de ataque, el atacante instala software en los sistemas del defensor con antelación y sin que sea detectado. En el momento del ataque el software es activado con una señalización simple y subrepticia. Las actividades preparatorias del ataque pueden pasar desapercibidas o ser subestimadas.

En otros sentidos –en capas más altas de la arquitectura de Internet– se reproduce la ventaja del atacante sobre el defensor. Los dispositivos de acceso a Internet y a las operaciones matemáticas necesarias para violar las barreras criptográficas son a la vez cada vez más poderosos, cada vez más baratos, cada vez más accesibles aun para los inexpertos, y cada vez más dispersos y fáciles de ocultar (esto último utilizando, por ejemplo, la red TOR (McCoy, 2008), originalmente concebida para proteger el anonimato de personas que pudieran estar en situaciones de persecución política). En cambio el defensor protege sistemas cada vez más complejos, cada vez más expuestos, dependientes de cada vez más usuarios cuya capacitación es insuficiente, con activos de valor e importancia crecientes, sin un aumento proporcional de presupuestos y personal capacitado, en otras palabras, exponiendo una superficie de ataque cada vez mayor.

Cuando las defensas mejoran y en consecuencia incrementan el costo del ataque directo, el atacante recurre a la ingeniería social (Allen, 2001) o se resigna a realizar un ataque de negación de servicio. Mientras cada atacante está obsesivamente dedicado a una función específica y altamente especializada en el ecosistema criminal, y el número de atacantes se multiplica, el número de defensores apenas crece y desde luego no lo hace en proporción a los activos que defiende ni al número de atacantes. Los defensores, además, deben

ocuparse de todos los posibles ataques. Los factores de escala son totalmente desfavorables a la defensa. Una combinación particularmente perversa de ataque propiamente cibernético e ingeniería social se presenta en el "ransomware" (Richardson, 2017)) que "secuestra", toma como rehén, criptográficamente los sistemas de la víctima y ofrece –sin necesariamente cumplirlo– devolver a la víctima el control de sus recursos a cambio de un pago.

La naturaleza de los ataques informáticos favorece la existencia de un amplísimo espectro de atacantes, entre criminales o incluso aficionados individuales y actores estatales de pleno derecho. Entre estos extremos se cuentan atacantes avanzados y bien financiados que pueden atacar a nombre de un Estado, por encargo de éste, o para favorecerlo sin previo acuerdo.

El delito organizado en el ciberespacio se estructura en líneas similares al del espacio físico (estando, además, cada vez más imbricados ambos aspectos); son característicos: actores especializados, funciones separadas, células herméticas y escasamente comunicadas (Stanislakwski, 2004), condiciones de acceso que levantan una barrera casi intraspasable para su penetración por fuerzas del orden.

El uso de espacios y canales secretos de comunicación, el cambio constante de ubicación (virtual o física), el establecimiento de confianza mediante mecanismos de fuerza entre personas intrínsecamente no confiables (como lo ha documentado magistralmente Diego Gambetta (Gambetta, 2009). El uso de criptomonedas y otras aplicaciones de las cadenas de bloques, son otras constantes comunes entre el delito cibernético y el delito organizado en espacio físico.

2.3.2 Cyber-to-physical

Se podría plantear una visión "inocente" de la ciberseguridad en la que se considerara que los activos informáticos no alcanzan el valor crítico de los activos físicos de las sociedades, una visión que Lucas Kello llama "clausewitziana" (Kello, 2013), en la que el territorio, las personas y las instalaciones son los objetos de la actividad

bélica, y los sujetos son ejércitos bajo mandos nacionales. En esta visión el ciberespacio y la ciberseguridad serían irrelevantes o de importancia secundaria. Sin embargo, de manera creciente la actividad en el cibersepacio tiene alcances en el territorio, las personas y las instalaciones físicas.

No se trata solamente de amenazas relativamente abstractas –la dificultad para el pago de nóminas en todo el país sigue siendo considerada, para sorpresa de este autor, como un problema menor que la pérdida parcial de control territorial– sino también de la posibilidad de que los atacantes impidan el funcionamiento de las redes eléctrica o de agua, produzcan explosiones o liberación de substancias tóxicas en fábricas y ductos, dirijan el funcionamiento de dispositivos médicos contra los pacientes, produzcan colisiones en el transporte público masivo, y otras formas de afectar físicamente a la población y reducir el control del gobierno sobre el territorio (véase, por ejemplo, Yampolsky, 2015).

A esto debe añadirse el uso bidireccional cíber-físico-cíber, es decir, apoderarse del control de dispositivos físicos como cámaras de videovigilancia para usar sus procesadores y conexiones a la red como vehículos para ataques cibernéticos, como ha pasado en 2017 en algunos casos muy sonados de *botnets* (Kolias, 2017).

El "problema de atribución" (Tsagourias, 2012) es uno de los puntos torales de la ciberseguridad, que la hace enormemente diferente de las consideraciones conocidas para la seguridad en espacio físico, y complica especialmente el nivel de seguridad nacional.

Atribuir un ataque a un agresor es la premisa fundamental de la defensa y de la retaliación. Si no se sabe quién ataca es muy difícil defenderse, pero sobre todo es muy difícil realizar un contraataque o una acción contra otros activos que sirva como medida para infligir daño al enemigo. El contraataque debe ser creíble, pronto y eficaz para que su sola posibilidad disuada a posibles atacantes. En delito cibernético, la atribución es extremadamente importante para iniciar y hacer efectiva la acción legal contra el delincuente; en seguridad nacional, la atribución no sólo debe identificar al individuo o grupo atacante, sino que

debe poder asociar su acción a la de un Estado contra el cual dirigir el contraataque o los recursos diplomáticos pertinentes.

En los siguientes párrafos vamos a explorar la posibilidad y consecuencias de atribuir un ataque que ya ha ocurrido a una persona en específico y determinar las acciones que un Estado debe emprender en consecuencia, para entender las limitaciones de la atribución y las consecuencias de dichas limitaciones.

En general los medios técnicos de Internet sólo permiten rastrear de manera fidedigna el origen de un ataque hasta una dirección IP. Ésta, suponiendo primero que no haya sido falsificada ("spoofeada" en el argot técnico), habrá sido asignada a un ISP (proveedor de servicios de acceso a Internet), del cual suele ser posible conocer su identidad y nacionalidad. El ISP puede o no compartir con un investigador forense más información, como los datos del cliente que tuvo asignada la dirección IP en el momento de interés y la ubicación física del equipo, dependiendo de la capacidad técnica del ISP, disponibilidad de la información, retención de datos, y legislación y prácticas de protección de datos personales (que impide compartir información) y de colaboración con las autoridades (que lo permite). Todo esto asume que se ha logrado atravesar la que puede ser una espesa barrera de indirección que oculta la dirección IP real desde la que se origina un ataque.

En la hipótesis de que se conozca la información descrita en el párrafo anterior, el problema de atribución puede haber quedado acotado pero no necesariamente estará resuelto. Incluso cuando se tiene la fortuna de contar con información fidedigna acerca del equipo específico del que efectivamente partió la acción informática del ataque, los medios técnicos por sí solos no bastan para atribuir a una persona específica el ataque, ya que el equipo puede haber estado comprometido y bajo control de alguien externo, o no puede comprobarse quién usó el equipo en el momento en cuestión.

Y aun suponiendo que, ahora combinando métodos informáticos y técnicas policiales y de inteligencia, se pueda atribuir el ataque a una persona u organización, ésta podrá negar haber actuado bajo órdenes de un Estado,

si cuenta con la suficiente "plausible deniability" (Office of the Historian, 1946). La investigación puede continuar por años pero la respuesta puede ser exigida en un corto plazo. Además, incluso en el caso de que el Estado capture el dispositivo, como ha ocurrido en actos de terrorismo o subversión cometidos desde dentro del territorio, el Estado puede estar sujeto a que un particular (el fabricante del teléfono) pueda y quiera aplicar medidas criptográficas para revelar el contenido de las comunicaciones relacionadas con la investigación. Peor aún, en muchos casos esta información no existe, simple y llanamente, por diseño de los protocolos y de los servicios.

Resulta así que el gobierno de un país puede tener identificado un ataque sufrido por entes en su territorio y no estar en condiciones de atribuirlo de manera suficientemente precisa a un actor estatal externo como para emprender una acción que dé respuesta en especie; y al no existir esta amenaza en forma contundente y en corto plazo, el Estado atacado tiene escaso poder de disuasión sobre posibles atacantes.

2.3.3 Definición de actos de guerra

La respuesta a un ataque por parte de un gobierno o Estado depende no sólo del problema de atribución, sino también en la definición de un acto de guerra en el ciberespacio, o a partir de éste, y la doctrina que rige la respuesta.

La definición de actos de guerra en el ciberespacio está a debate al momento de realizar la presente investigación. Diversos organismos internacionales, entes académicos y gobiernos están tratando de alcanzar definiciones claras pues de esta claridad dependerá la precisión de la doctrina de defensa y contraataque de las partes atacadas. Una referencia común en esta materia es el "Manual de Tallinn" (Manual, 2017).

Como en párrafos anteriores, la definición de un acto de guerra se ve complicada por la diversidad de posibles agresores y su relación con un gobierno determinado (Klimburg, 2017). Depende además de cuán crítico consideren distintas entidades que debe ser un ataque de origen cibernético para considerarlo un acto de guerra.

Se suele ilustrar el espectro de posibles definiciones haciendo mención de ejemplos como que el ataque interrumpa o altere el funcionamiento de los equipos de un hospital de tal manera que ocasione pérdida de vidas; ésta podría ser una consecuencia no sólo de un ataque enfocado a los dispositivos sino algo mucho más genérico, una interrupción en el abasto eléctrico.

Otros posibles actos bélicos serían la suspensión de servicios vitales como el abasto de agua, electricidad o combustibles, o transporte. La interferencia con las elecciones está también sometida a consideración. ¿Cuándo es esto un acto de guerra, cuándo se puede afirmar que es un acto promovido o realizado por un gobierno al que habrá que considerar hostil? El ataque pudo venir desde un territorio cuyo gobierno esté combatiendo a los atacantes, y el país destino y el país origen del ataque podrían identificar un enemigo común en lugar de considerarse uno a otro como hostiles.

Debe considerarse también una distinción que induce un momento de sobriedad: algunos ataques a la soberanía de una nación se pueden propagar a través del ciberespacio, incluso hacerlo en formas inéditas e insidiosas, pero deben ser analizados como propaganda, operaciones psicológicas, intervención, subversión, y deben ser tratados a partir de esa naturaleza fundamental. El tratamiento de estas actividades en el ciberespacio debe estar supeditado a las leyes, tratados, políticas y prácticas pertinentes de forma sustantiva, y referirse a las redes solamente como medio comisivo. La amplificación, la facilidad de acceso, el ocultamiento del origen, etc., se tratarán como agravantes o atenuantes según el caso.

2.3.4 Confianza

Bajo el rubro "confianza" encontraremos una enorme cantidad de problemas; cuando menos los siguientes:

2.3.4.1 Confianza entre Estados

La base de todas las consideraciones en materia de ciberseguridad en tanto seguridad nacional es la ausencia de confianza total entre los Estados. De existir

esta confianza, ningún país percibiría que está en riesgo de agresión por un tercero, y si lo estuviera, disiparía sus dudas por vías pacíficas. En cambio, la competencia entre países por motivos económicos o políticos, las diferencias ideológicas o religiosas, versiones diferentes de la historia sobre la autoridad sobre un territorio, motivos de raíz étnica y muchísimos otros, las múltiples raíces históricas, económicas, políticas, sociales y culturales de la guerra, se manifiestan en la ausencia de confianza como base de las relaciones internacionales.

La historia es también fuente de lecciones para la construcción de confianza y de relaciones entre actores que no se pueden basar en plena confianza. Desde luego una de las bases de estas últimas es la identificación y persecución de objetivos comunes, como puede ser la subsistencia del sistema en su conjunto, la ausencia de conflicto bélico de gran escala, etc.

La Guerra Fría proveyó nuevas lecciones de construcción de relaciones con base en desconfianza o confianza limitada, mediante la disuasión proveniente de la ”doctrina MAD”, “destrucción mutua asegurada”, entre las potencias nucleares, que a su vez dio lugar a un gran sistema de alianzas de alcance global. Como lo han señalado Klimburg y otros autores, la analogía con la amenaza nuclear no se puede extrapolar fielmente al ciberspacio.

La señalización de las intenciones de los actores es mucho menos clara en el ciberespacio y por ello, y las otras razones ya descritas en este texto como las capacidades de los actores subnacionales, la impredecibilidad del alcance de los ataques, etc., no ha sido posible todavía construir un sistema estable de relaciones basadas en confianza limitada. Una importante escuela en el régimen de Cibernormas (Pawlak y Barmpalou, 2017) y el trabajo del “Best Practice Forum” sobre Ciberseguridad del Foro sobre Gobernanza de Internet de la ONU, (Hoorenbeck, 2018) dedica esfuerzos extraordinarios al diseño de CBM, “confidence building measures” o medidas de construcción de la confianza, para acotar el riesgo de daños que escalen rápidamente hasta quedar fuera de control en el caso de una confrontación en el ciberespacio.

2.3.4.2 Confianza entre ciudadanos y autoridades del Estado

En todas las condiciones de potencial agresión al Estado, sea ésta por otro Estado o por actores subnacionales propios o ajenos, la capacidad de acción del Estado depende de la confianza, el control, o ambos, con el que cuente en su relación con los actores internos. En ciberseguridad la acción encubierta (y descubierta) del Estado contra los ciudadanos, como la intervención no autorizada de comunicaciones, la provocación y engaño a través de "bots", "trolls" y otras herramientas, y su ocultamiento, erosiona corrosivamente esta base de confianza, de manera especialmente crítica ya que ocurre en el mismo dominio operacional de Internet, redes y computadoras.

La continuidad entre las acciones relacionadas con el delito cibernético, la seguridad personal y pública, y las acciones de agresión contra la nación y el Estado diluye la sensación de seguridad del ciudadano ante el Estado, y su confianza en el mismo. El argumento que expresa "si no tienes nada que ocultar no tienes nada que temer", o "si se solicita la intervención de las comunicaciones o la penetración de las actividades de una persona u organización es que están efectuando acciones presumiblemente delictivas" pierde su poder cuando se considera que el Estado, el gobierno, o alguna parte de éste actúa fuera de la ley. En países como México donde no hay una tradición sólida de confianza en el imperio del Estado de Derecho, y donde se conoce la penetración de las autoridades y los cuerpos policíacos por elementos delictivos, se vuelve difícil alcanzar acuerdos nacionales sobre ciberseguridad basados en confianza.

2.3.4.3 Confianza entre los sectores

Para la gobernanza multisectorial del ciberespacio, como la indican las prácticas probadas y los mandatos de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la construcción de confianza entre los sectores privado, social, público, académico y técnico es fundamental. En su ausencia es difícil que construyan acuerdos sólidos, operables y de la profundidad necesaria.

Entre otras medidas de construcción de confianza para las estrategias nacionales y locales de ciberseguridad, son indispensables la transparencia, la declaración de conflictos de interés y la vigilancia constante. Al mismo tiempo es también indispensable llevar a cabo eventos y acciones con resultados que prueben las bases de la confianza y permitan que ésta se profundice y arraigue, y vuelvan inaceptables los costos de faltar a ésta.

2.3.4.4 Confianza entre actores críticos

Un nexo que no puede faltar en la construcción de ciberseguridad es la confianza entre ciertos sectores críticos que deben compartir información y actuar conjuntamente para la preparación y la respuesta a incidentes. Los CERTs (equipos de respuesta a emergencias en cómputo) y CSIRTs (equipos de respuesta a incidentes de seguridad en cómputo), la banca, las áreas de seguridad informática de las empresas y de entes públicos y de la sociedad civil, la prensa, los proveedores de servicios especializados y las fuerzas del orden deben contar con mecanismos de comunicación y coordinación en los cuales cuenten con la confianza de transmitir información de amenazas y ataques, vulnerabilidades de software, sistemas y redes, y acciones.

La dificultad de construir esos espacios de confianza se acentúa dado que por un lado esa confianza no existe respecto a otras acciones hostiles, como el delito en espacio físico, y por otro lado, los medios de comunicación y coordinación son informáticos, también doblemente sujetos a riesgos.

2.3.5 Tecnologías exponenciales

En algunas esferas se conoce como "tecnologías exponenciales" a las que significativamente amplifican capacidades del ser humano, como la inteligencia artificial, la impresión 3D, la robótica, y tecnologías no informáticas como la manipulación genética (López-Portillo Romano, 2018).

Éstas tienen el potencial de transformar los análisis y las acciones de ciberseguridad tanto del lado del defensor como del atacante; por ejemplo algunas

formas de Inteligencia Artificial ya existentes pueden contribuir a identificar patrones que conduzcan a detectar vulnerabilidades técnicas, físicas o humanas en el blanco de un ataque, o, *contrario sensu*, ayudar al defensor a identificar patrones y anomalías en el tráfico de Internet que le permitan iniciar una alerta por un posible ataque y así evitarlo.

3. Regímenes

Entre muchas posibles definiciones de régimen seleccionamos la de Krasner (1082): "conjunto de principios, normas, reglas y procedimientos para la toma de decisiones, implícitos o explícitos, alrededor de los cuales convergen las expectativas de los actores en un área dada de las relaciones internacionales".

Se puede simplificar el estudio de los regímenes aplicables a la ciberseguridad reduciéndolo a dos, el multilateral y el multisectorial ("multistakeholder" o MSH en este texto), que ha sido reconocido entre otros autores como Franda (2001). Sin embargo, por razones que me propongo hacer evidentes en el texto, se gana precisión y riqueza de análisis si consideramos cuatro regímenes: el multilateral o intergubernamental; el de la administración de TI (tecnología de información, o TICs, tecnologías de información y comunicación); el de cibernormas (que es en parte una extensión del multilateral, con variaciones importantes), y el multisectorial característico de la gobernanza de Internet. Es aportación original del presente trabajo reconocer como un régimen específico el de Administración de TI.

El régimen multilateral es parte fundamental de nuestra realidad contemporánea. Lo definen los principios de soberanía e identidad territorio-nación y los mecanismos de la diplomacia y los tratados. En años recientes y desde los otros regímenes también se le llama "de Westfalia" (Scholte, 2017), en referencia al tratado del mismo nombre que hace unos siglos definió las bases ya citadas, o "de Clausewitz" para al menos un autor notable, (Kello, op. Cit.) que reconoce también a la conducción de la guerra como un asunto exclusivo de los Estados. Son característicos de este régimen los instrumentos bilaterales y multilaterales de acuerdo entre países y

organismos como la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA) (característico de los organismos regionales) o la Unión Internacional de Telecomunicaciones (característica de los organismos especializados), así como la Organización para la Cooperación y el Desarrollo Económico (OCDE), organismo emblemático de los "clubes" u organismos basados en afinidad.

Me refiero al "régimen de Administración de TI" para describir el conjunto de entidades, operaciones, decisiones y políticas que se presentan en el nivel operacional de la seguridad informática como generalmente se practica en gobiernos, empresas, universidades y otras organizaciones. Éste no es un régimen formalmente constituido a pesar de que lleva la principal carga de proteger los recursos informáticos de la sociedad. Miles de técnicos, abogados, administradores y directivos organizan las políticas internas de las empresas, adquieren y desarrollan software y sistemas de información, capacitan personal, adquieren, instalan y operan sistemas de detección y de prevención de intrusiones, administran y operan redes, servidores, servicios en la "nube", contratos de tercerización, se certifican ante entidades públicas y privadas, y un sinfín de otras actividades. Frecuentemente encuentran en las leyes un obstáculo donde deberían encontrar un apoyo. Parte de este sistema se formaliza en entidades llamadas CERT (Computer Emergency Response Team) y CSIRT (Computer Security Incident Response Team) y en los departamentos de seguridad informática, o a cargo de la misma, en gobiernos, empresas y organizaciones civiles. Lo caracterizan el dinamismo, el pragmatismo y su orientación a la solución de problemas.

El régimen de Cibernormas es una extensión del régimen multilateral, que incorpora partes del de Administración de TI, de la academia, y del "multistakeholder". Se centra en la búsqueda de normas internacionales que rijan a los Estados en su conducta internacional en materia de ciberseguridad, con algunas analogías a la Convención de Ginebra y a acuerdos de limitación de las armas nucleares y otros conducentes al control de armamentos. Se presenta en organizaciones y mecanismos multilaterales no globales como el de Cooperación de Shanghai (formado por China, Rusia,

Uzbekistán y Kazakhistán, con adiciones y observadores como Pakistán e India, y más recientemente México), y al interior de la ONU mediante el GGE (Grupo de Expertos Estatales) formado por la Asamblea General y que tuvo un sonado fracaso en junio de 2017 (Henriksen, 2019), complemento a los Estados, proviene de académicos distinguidos como, de manera ejemplar, Ronald Deibert y el fallecido Roger Hurwitz (Hurwitz, 2013-14); (Hollis, 2002); (Osula, 2016) y (Klimburg, 2017), las universidades en las que trabajan, gobiernos como el de los Países Bajos y algunas otras organizaciones.

El régimen multisectorial o "multistakeholder" caracteriza especialmente a la gobernanza de Internet. Lo constituyen numerosos mecanismos y organizaciones en los que fundamentalmente se distinguen agrupamientos de gobiernos, industria, sociedad civil, academia y comunidad técnica; en algunas organizaciones estos dos sectores se consideran bien dentro de la sociedad civil, bien transversalmente a los otros. Dependiendo del tema del que se ocupan, estas organizaciones y mecanismos tienen diversos grados de formalización. Así por ejemplo ICANN (Internet Corporation for Assigned Names and Numbers), a cargo de la coordinación técnica de los identificadores centralmente coordinados de Internet (nombres de dominio, direcciones IP y parámetros de protocolos técnicos), se constituye como un organismo privado no lucrativo, basado íntegramente en instrumentos consensuales del derecho privado, con mecanismos formales de toma de decisiones, elección o designación de funcionarios, recurso y reversión de decisiones, y penalización por faltas a sus propias norma. En cambio el IGF (Internet Governance Forum o Foro sobre Gobernanza de Internet) requiere un aparato normativo menos complejo, ya que se limita a organizar un evento anual y debates a lo largo del año entre los distintos sectores. Los mecanismos de este régimen se caracterizan por una aspiración de agilidad, relevancia y equidad, sin oponerse a las leyes y mecanismos multilaterales o de cibernormas, y dando un amplio reconocimiento a la comunidad operacional, como la descrita como "administración de TI" en párrafos anteriores. Se orienta a la solución de problemas, convoca a todos los actores relevantes, y si bien enfrenta un conocido problema de "déficit democrático", lo compensa mediante apertura, transparencia y rendición de cuentas. Basa su

legitimidad en la combinación de eficacia y reconocimiento de las partes interesadas. Le rigen además un principio de subsidiaridad y uno de racionalidad técnica.

Una caracterización reciente del régimen que rige en gobernanza de Internet ha sido provista por Scholte (2017) y la describe como transescalar, transectorial, difusa, fluida, con mandatos superpuestos, jerarquías ambiguas y la ausencia postsoberana de una autoridad única y consistente. A esta caracterización se debe añadir el factor heurístico y que la selección natural evolutiva entre los mecanismos y organizaciones activos en gobernanza de Internet se base en un criterio de legitimidad, fundado a su vez en la efectividad de las organizaciones para cumplir con sus mandatos.

Las características citadas se describen brevemente de la manera siguiente:

1. Transescalar: atraviesan múltiples escalas, por ejemplo desde la de un número limitado de servidores raíz del DNS (13) o de países (alrededor de 200) hasta los más de 3 millones de personas conectadas, o el incontable número (posiblemente decenas de millones) de dispositivos o de cuentas de servicio.
2. Transectorial: en gobernanza de Internet participan los sectores público, privado y social, con un papel específico también para las comunidades generadoras y operadoras de tecnología ("comunidad técnica") y la comunidad académica, que pueden ser transversales a los sectores citados y ello en forma variable según el país y con el paso del tiempo. Dentro de cada uno de estos sectores hay subdivisiones, por ejemplo en el sector privado distinguimos intereses complementarios y contrapuestos entre los operadores de redes, los proveedores de servicios en línea, las empresas que utilizan Internet para sus negocios, etc.
3. Difusa: la gobernanza de Internet tiene fronteras difusas en tanto que algunos asuntos son resueltos en formas inmediatas y locales y de manera informal mientras que su escalamiento ante diversos factores puede llevar a mecanismos más formales, en otras geografías, etc.

4. Fluida: el "locus" y la forma de organización para resolver diversos problemas en gobernanza de Internet varía rápidamente en el tiempo y según las partes involucradas. Organizaciones como ICANN han sufrido varias reestructuraciones y cambios de reglas tan fundamentales como abandonar su dependencia de la supervisión del gobierno de Estados Unidos en tan solo 20 años; la IETF ha modificado sus métodos y estructura, los registros de nombres de dominio nacionales y muchas otras entidades se reorganizan y adaptan constantemente. Surgen estructuras nuevas como el APWG en el momento en que son requeridas y se abandonan cuando dejan de ser útiles o son substituidas por otras que lo sean más.
5. Mandatos superpuestos: no es infrecuente que diversas organizaciones o mecanismos tengan mandatos simultáneamente en determinados asuntos. Así, por ejemplo, hay una superposición entre ICANN, los registros de nombres de dominio, la OMPI, organizaciones arbitrales, asociaciones de empresa, autoridades nacionales de propiedad industrial e intelectual, y la OMC, para temas de propiedad industrial en nombres de dominio.
6. Jerarquía difusa: no hay una jerarquía definida ni permanente entre las organizaciones y mecanismos de gobernanza de Internet. Así por ejemplo en materia de nombres de dominio los ccTLDs reciben autoridad delegada de ICANN, pero no requieren reconocerla para todas sus actividades, tratando en muchos casos los asuntos directamente con sus gobiernos y comunidades nacionales. En algunos casos ICANN actúa reconociendo formal o implícitamente la autoridad de la IETF (para el establecimiento de estándares); en otros la IETF confía plenamente en la autoridad delegada en ICANN (para la asignación de parámetros y el registro de sus valores, en la unidad llamada IANA).
7. Ausencia postsoberana de una autoridad única y consistente. No existe una autoridad única para todos los asuntos de Internet. El sistema en operación está conformado por diversas entidades, cada una de las cuales tiene algún grado de autoridad –a veces sólo poder de convocatoria para debates,

como el IGF– en un ámbito específico, como se menciona en la característica de superposición de ámbitos de competencia, y en otras es subordinada. En algunos casos la autoridad es formal como en la ISO-3166-MA que a su vez deriva su lista de parámetros de la Oficina de Estadística de la ONU; en otros, informal como el APWG. Sólo algunas entidades de alcance nacional pueden reclamar una autoridad legal delegada por un proceso parlamentario y elecciones de un gobierno.

8. Heurística: a las características identificadas por Scholte, añado la muy importante de que las organizaciones y mecanismos de gobernanza de Internet se diseñan y operan alrededor de la solución de un problema o conjunto pequeño de problemas a cuya solución pueden contribuir eficazmente: la IETF para la normalización técnica de Internet; W3C para la Web; ICANN para eliminar la discrecionalidad y descentralizar la gestión de los identificadores coordinados; APWG para atacar el "phishing", y así sucesivamente.
9. Legitimidad basada en efectividad: la otra característica de los mecanismos de gobernanza de Internet que añado a la lista de Scholte es la legitimidad por vía de la efectividad. Siguiendo quizás el viejo "mantra" de la IETF "no tenemos presidentes ni reyes ni votos, sólo tenemos consensos fuertes y programas funcionando", la legitimidad de las organizaciones –cuya aceptación se demuestra por el acatamiento de sus mandatos, el recurso a sus decisiones, la participación en sus procesos– se basa en su capacidad de resolver de manera efectiva los problemas. Para mantener su legitimidad las organizaciones y mecanismos deben evolucionar constantemente y asegurar la participación de las partes interesadas de manera completa y a través de representaciones efectivas, así como tener procesos, archivos y operatividad conmensuradas con las características deseadas de las soluciones, como certeza, velocidad, amplitud de consulta, capacidad de implementarlas, y otras.

Otras organizaciones de este régimen involucradas en ciberseguridad son la IETF (Internet Engineering Task Force); el M3AAWG (Messaging, Malware and Mobile Anti

Abuse Working Group) y el APWG (Anti-Phishing Working Group), así como ISOC (Internet Society) (Pisanty, The vexing problem of oversight, 2015)

Ciberseguridad bajo los distintos regímenes

TI. En el régimen de Administración de TI, la ciberseguridad es una consideración constante en un número creciente de formas. Pasó de ser una característica superpuesta a las actividades en Internet a ser una consideración de diseño desde el principio de cada desarrollo de sistemas. En licitaciones y contratos, así como en instrucciones internas, se considera a la seguridad de los sistemas como una de los principales "requerimientos no funcionales" de los desarrollos.

El gobierno de la función de ciberseguridad en este régimen está basado principalmente en experiencia, comunicación entre las partes, acuerdos para compartir información, desarrollo de capacidades, normas técnicas y normas organizacionales. Los estándares de la familia ISO 27000, los de gestión informática como COBIT e ITIL, los del NIST (National Institute of Standards and Technology, de Estados Unidos), la norma MAAGTIC-SI (Manual Administrativo de Aplicación General en Tecnologías de la Información y Comunicación y Seguridad Informática, del Gobierno Federal mexicano) y otros relacionados dan normas de conducta a los administradores de redes y sistemas que les permiten mantener seguros sus sistemas, desde el desarrollo de software y la adquisición de sistemas hasta las operaciones más sensibles, pasando por los contratos de tercerización para servicios administrados, "cómputo en la nube", contratación y promoción de personal, aseguramiento de calidad y numerosos otros aspectos.

El marco normativo de esta gobernanza tiene múltiples fuentes: leyes como las cláusulas de Colaboración con las Autoridades de la Ley Federal de Telecomunicaciones y Radiodifusión (México) y las de Protección de Datos Personales; los Decretos de Austeridad del Gobierno Federal mexicano desde el año 2000, que orientan a la tercerización de servicios informáticos; contratos colectivos del personal en empresas y gobiernos; reglamentos y políticas de gobiernos nacionales y

subnacionales; contratos con proveedores y clientes; normatividad sectorial, como es el caso en banca, sector salud en algunos países, leyes fiscales; normas técnicas internacionales generalmente aceptadas y sus versiones y variantes nacionales; políticas públicas como la EDN (Estrategia Digital Nacional) y el acuerdo de colaboración informal y permanente que forma parte fundamental del tejido de Internet ((Sullivan, 2016).

3.1 Multilateral

3.1.1 Unión Internacional de Telecomunicaciones (UIT)

La gobernanza de la ciberseguridad en el marco de la UIT se puede considerar centrada en la Resolución 45 de Doha, 2006 (UIT, 2006), que es a su vez una evolución de los acuerdos para el combate al correo electrónico comercial no solicitado ("spam"), y que ha pasado por versiones y revisiones en las Conferencias y Asambleas de la UIT sobre telecomunicaciones internacionales (WCIT), normalización técnica (WTSA) y sobre Desarrollo (WTDC) así como el cauce al que éstas llevan, las Conferencias de Ministros Plenipotenciarios conocidas también como Plenipots o PP-xy donde xy es el número abreviado del año de la Conferencia, por ejemplo PP-10 se llevó a cabo en 2010.

Debe recordarse que la gobernanza de la UIT reside en los Estados Miembros, cuyas decisiones son las únicas resolutivas. En años recientes se ha transferido una parte de la capacidad de decisión a los sectores (Telecomunicaciones, Radio y Desarrollo), incrementado la participación de los Miembros Sectoriales, y ampliado el alcance de organizaciones que pueden presentarse a las Asambleas y Conferencias y participar en los Grupos de Estudio, pero las decisiones finales son intergubernamentales. Otro objeto de fricción con otros sectores proviene de que los documentos de la UIT son accesibles solamente para miembros autorizados mediante claves celosamente custodiadas, a diferencia de los de las organizaciones de la comunidad Internet, disponibles ampliamente.

El alcance de estas Resoluciones se traduce a nivel nacional a través de la naturaleza vinculante o no de los

instrumentos normativos de la UIT, su Constitución y sus Reglamentos como el Reglamento de Telecomunicaciones Internacionales. La traducción entre el nivel global y el nacional se transmite también a través de organismos regionales como CITEL (Conferencia Interamericana de Telecomunicaciones) y sus contrapartes en otras regiones del mundo.

Los puntos contenciosos para el desarrollo de estas resoluciones derivan de aspectos estratégicos, aspectos tácticos, aspectos técnicos y aspectos políticos. Los aspectos técnicos se refieren a la capacidad de los Miembros Sectoriales y los Países Miembros de implementar las medidas, considerando que los Miembros Sectoriales son operadores de redes de telecomunicaciones que no siempre son los ISPs. Los aspectos políticos están determinados por factores como la formación de bloques regionales, la formación de bloques de afinidad de países y Miembros Sectoriales promotores de un modelo de mercado abierto y competitivo contra otros basados en proteccionismo, y su imbricación con la formación de bloques y negociaciones en asuntos ajenos a la UIT. Los aspectos estratégicos y tácticos pasan del interés en la substancia de las Resoluciones a la persecución de fines como la obtención de votos para los cargos de elección de la Unión y otros organismos.

En la historia de la Resolución 45 han sido contenciosos diversos asuntos: las referencias a la libertad de expresión, que para Estados Unidos y países afines es un valor fundamental que la propia ciberseguridad debe contribuir a preservar, pero a la vez puede verse limitado por la inspección de comunicaciones requerida para algunos proyectos de seguridad, y que por otra parte, para otros países no debe ni ser mencionada en este contexto; las referencias a la privacidad, tema en el que Estados Unidos se opone al enfoque normativo europeo basado en leyes de protección de datos personales y más recientemente el "derecho al olvido", mientras que por otra parte, numerosos gobiernos incluido el de Estados Unidos se oponen al enfoque de países como China, Vietnam y el bloque árabe que no prevé llevar la protección a la privacidad a este nivel; la mención de y colaboración con otros organismos, especialmente los multisectoriales como la IETF o ICANN; y el carácter

vinculante de las resoluciones. El personal y algunos líderes de la UIT se empeñan en reafirmar en cada párrafo la preeminencia de la Unión en el seguimiento de la Cumbre Mundial sobre la Sociedad de la Información y en citar a la Unión a la vez que excluyen a la UNESCO y otras organizaciones y ramas de la ONU.

El resultado es una resolución extensa en antecedentes y parca en extremo en contenido propiamente resolutivo: "*Resuelve instruir al Director de la Oficina de Desarrollo de las Telecomunicaciones:* 1. Organizar, en conjunto con el Programa 3 y con base en contribuciones de los miembros, reuniones de Estados Miembros y Miembros Sectoriales para discutir maneras de aumentar la ciberseguridad, incluyendo, *inter alia*, un memorándum de entendimiento para reforzar la ciberseguridad y combatir el spam entre Estados Miembros interesados; 2. Informar de los resultados de estas reuniones a la conferencia plenipotenciaria de 2006."

El impacto de hecho sobre la ciberseguridad es muy limitado, ya que depende de que los gobiernos de los Estados Miembros y los Miembros Sectoriales efectivamente den operación a las Resoluciones. Generalmente la comunidad de los regímenes multisectorial y de Administración de IT no las requieren y las Resoluciones sólo se utilizan para justificar leyes y decisiones gubernamentales en algunos países, más frecuentemente en los que tienen una operación gubernamental menos participativa o abiertamente autoritaria.

3.1.2 ONU

La ONU presta atención creciente a Internet, la Sociedad de la Información y el ciberspacio a través de muchos de sus organismos. En la década 1990-2000 el Programa de las Naciones Unidas para el Desarrollo tuvo un papel activo en la promoción del acceso a Internet. La UNESCO ha competido con la UIT por el liderazgo en materia de Sociedad de la Información, en el que actualmente se ocupa de temas como acceso al conocimiento, libertad de prensa y de expresión, y educación, mientras que la UIT obtuvo y conserva el liderazgo a través de su control sobre la Cumbre Mundial sobre la Sociedad de la Información (2003-2005) y sus mecanismos de

seguimiento. Las Relatorías Especiales sobre Libertad de Expresión y más recientemente sobre Privacidad han tenido incidencia importante al menos a nivel declarativo sobre estos temas, con paralelos productivos en regiones como la de las Américas, en este caso a través de la OEA (sobre la cual se trata en el punto 3.1.3).

En la Asamblea General de la ONU y tanto en el Primer como en el Segundo Comité, y en sus órganos administrativos como ECOSOC, se presta también atención al uso pacífico del ciberespacio. Para abreviar referiremos solamente el trabajo del GGE, Grupo de Expertos Gubernamentales, que ha buscado establecer un conjunto mínimo de reglas de coexistencia pacífica y de limitación del alcance sobre seguridad nacional de las acciones en el ciberespacio. El GGE es un grupo cerrado que emite poca información acerca de los resultados de su trabajo y casi nula sobre sus procesos. De acuerdo con noticias internacionales, en junio de 2017 interrumpió sus trabajos ante la imposibilidad de alcanzar acuerdos.

Los acuerdos que se buscaban en el GGE, para alimentar posibles resoluciones de la Asamblea General, se orientan a reglas para la coexistencia en el ciberespacio, la definición de los actos bélicos y la prohibición o autorización de determinadas acciones entre los Estados. Buscan además limitar el daño que las acciones bélicas en el ciberespacio pueden producir sobre la población civil; por ejemplo, prohibirían el ataque a redes y sistemas de instalaciones hospitalarias y escolares. Establecerían un marco para la determinación de atribución de origen de ataques y para la pertinencia, oportunidad, necesidad y proporcionalidad de las medidas de respuesta de los Estados cuyos territorios o sistemas fueran atacados. Las limitaciones a la propaganda y a la subversión, a la intercepción de comunicaciones y al espionaje, y a la interferencia en la vida privada o en el ejercicio de derechos ciudadanos parecen ser los obstáculos que han resultado insalvables. Con miembros como Estados Unidos, Rusia, China y Cuba, el contraste entre expresiones a favor de la vigencia del Derecho Internacional en el ciberespacio o en contra de la militarización del mismo, algunas sustanciales y otras retóricas, es posible apreciar que este Grupo haya encontrado dificultades para avanzar.

3.1.3 Organismos regionales y especializados

Entre los organismos regionales de interés para las propuestas multilaterales de gobernanza del ciberespacio cabe destacar para los fines de este trabajo a la Organización de Cooperación de Shanghai, ya mencionada y a la OEA. También son importantes la OCDE, la Unión Europea, APEC y ASEAN; en beneficio de la extensión del trabajo no serán tratadas.

La Organización de Cooperación de Shanghai parte de una reunión entre China (que la lidera), Rusia, Uzbekistán y Kazakhiztán para explorar reglas de convivencia multilaterales entre países afines, a iniciativa de China. Se han reunido al menos dos veces en forma amplia y pública y ha incorporado a India y Pakistán como miembros, estableciendo así un territorio amplio y sobre todo una población cercana en número a la mitad de la humanidad. Otros países, entre ellos México, se han incorporado como observadores. El propósito explícito de la Organización es el orden basado en reglas en el ciberespacio, plasmado en un Código de Conducta para la Seguridad de la Información acordado entre sus miembros (sin que haya entrado en vigencia hasta ahora).

Aquí la palabra clave es "seguridad de la información"; su insidiosa polisemia será analizada en la sección de conclusiones.

Como se puede ver en la declaración de esta organización después de su reunión de 2017 en Xinhua (y una nueva reunión, la 4ª. Conferencia Mundial en Wuzhen llevada a cabo en diciembre de 2017) el alcance que China busca es mucho más amplio que la cooperación para la seguridad de la información; propone reformas sustantivas a la gobernanza del ciberespacio y de Internet, con un fuerte sesgo multilateral (honrando sólo de manera nominal al multisectorial) con el propósito de limitar a los actores no gubernamentales a nivel global y servir de marco legitimador de legislación, políticas y acciones coercitivas en el plano nacional. China intenta, además, extender su visión desde el mecanismo de Shanghai a los BRICS (asociación formada por Brasil, Rusia, India, China y Sudáfrica) y otros espacios donde su presencia es asimétricamente relevante.

Por su parte la OEA se ha aproximado al tema de ciberseguridad en al menos dos proyectos, no independientes, el mecanismo CICTE contra el terrorismo (Comité Interamericano contra el Terrorismo) y el impulso a la creación, país por país, de una Estrategia Nacional de Ciberseguridad (ENCS). El CICTE extiende sus alcances en el ciberespacio a la vigilancia e intercepción de comunicaciones potencialmente relacionadas con el terrorismo y por ello se expande al ámbito del delito organizado.

El programa para promover las ENCS está a cargo de la Gerencia para la Seguridad Cibernética de la OEA y se distingue por una actividad constante en eventos regionales y locales, la promoción de un texto normalizado para que alimente y constituya el documento de ENCS en cada país, la contratación y publicación de un diagnóstico del estado de madurez de seguridad cibernética de cada país de la región, y una activa alianza con las grandes empresas transnacionales que dominan los mercados de equipo para redes y de software. Hasta ahora ha logrado la incorporación de Jamaica y Colombia en la emisión de sus respectivas ENCS.

Es importante también mencionar a la GCCS (Global Conference on Cyberspace, Conferencia Global sobre el Ciberespacio) cuyo origen es multilateral, y cuyo trabajo se trata más adelante en el rubro de Cibernormas.

También es indispensable mencionar el Convenio de Budapest o Convención Europea contra el Delito Cibernético, un instrumento multilateral por excelencia para la cooperación internacional para prevenir y perseguir el delito cibernético. Éste, como ya lo hemos expuesto, no se debe identificar con la ciberseguridad pero ciertamente es un componente importante, y el Convenio de Budapest es un instrumento valioso intrínsecamente y un experimento en marcha del que se puede aprender mucho para otros aspectos de la ciberseguridad entendida como seguridad nacional.

En los últimos cinco años también ha cobrado importancia la actividad del Ministerio del Exterior del Reino Unido, y de organismos constituidos en ese país que colaboran con dicho Ministerio, como el Global Cyber

Security Capacity Center (GCSCC) que opera en la Universidad de Oxford (GCSCC 2018, https://www.oxford-martin.ox.ac.uk/cybersecurity/)

3.2 Multistakeholder y gobernanza de Internet

El concepto de gobernanza "multistakeholder" alcanzó sus actuales niveles de publicidad a partir de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), al convertirse la participación de todos los sectores, en pie de igualdad, en la norma deseable para la gobernanza de Internet. De hecho la gobernanza de Internet ya constituida seguía esta norma desde tiempo atrás, sin invocarla necesariamente por su nombre; y los procesos de gobernanza multisectorial se han aplicado a muchos otros ámbitos como el medio ambiente, el deporte, las finanzas, algunos productos agrícolas y alimentos, la pesca y la ganadería. Con fuertes raíces en el trabajo de Elinor Ostrom para la gobernanza de los bienes comunes, y con modificaciones para dar lugar a la intervención de los gobiernos formalmente constituidos y para adaptarse a la existencia de derechos de propiedad, la gobernanza multisectorial ha logrado avances significativos. tanto en la teoría como en la práctica, en la última década y es un horizonte ineluctable hacia el futuro.

En materia de ciberseguridad, los procesos multisectoriales se alimentan del régimen de Administración de TI y sus actores, y de mecanismos y organizaciones novedosos como la IETF (Internet Engineering Task Force) o ICANN. Los aprendizajes de las últimas dos décadas nos indican que las organizaciones y mecanismos multisectoriales exitosos son heurísticos, acotados a problemas definidos, plurales, abiertos y adaptables. Combinan reglas formales e informales, procuran el consenso más que la unanimidad o la votación por mayorías simples, se mantienen dentro del marco de las legislaciones existentes a la vez que pueden impulsar su armonización e innovaciones normativas, y se revisan a sí mismos con frecuencia para asegurar que su legitimidad por reconocimiento de los actores relevantes y por la eficacia de sus resultados se preserven y expandan.

El ejemplo más elaborado de gobernanza multisectorial de Internet es ICANN (ICANN, 2019, https://icann.org).

Esta organización, encargada de la coordinación central de las políticas que afectan al Sistema de Nombres de Dominio, la distribución de direcciones IP y el registro de parámetros de protocolos de la IETF, reúne a comunidad técnica, gobiernos, empresas, sociedad civil, y academia. Las empresas a su vez aparecen agrupadas en función de la estructura del mercado de nombres de dominio, en "constituencies" de registros (operadores de bases de datos centrales de nombres de dominio de primer nivel), registradores (empresas que comercian con esos registros), intereses de propiedad intelectual y marcas, operadores de redes y empresas usuarias de los nombres de dominio. En el marco de los nombres de dominio los intereses no comerciales, principalmente institucionales y de la sociedad civil organizada, se presentan en dos grupos que constituyen el grupo rector no-comercial; y respecto a un marco más amplio, los usuarios, comerciales o no, participan a través de la comunidad "At Large". Los gobiernos se agrupan en el GAC, Comité Asesor Gubernamental, y la comunidad técnica forma parte de diversos grupos asesores específicos como el de Seguridad y Estabilidad y el de operadores de servidores raíz, además de la representación formal de la IETF y grupos afines en funciones de enlace en el Consejo Directivo.

ICANN produce políticas que reducen las posibles arbitrariedad y discrecionalidad en la gestión de la raíz del Sistema de Nombres de Dominio, mediante procesos formales cuyos efectos tienen impacto global en diversos negocios a lo largo y ancho de Internet. Por ello, cuenta además con procedimientos que pueden llevar a la revisión e incluso reversión de algunas de sus decisiones. Atendiendo a la naturaleza global de Internet, sus procesos de decisión combinan reuniones en diversos lugares del mundo con discusiones a través de Internet que evitan favorecer asimétricamente a los participantes con mayores recursos económicos.

La incidencia directa de ICANN en ciberseguridad se da a través de la estabilidad, seguridad y resiliencia del Sistema de Nombres de Dominio a su cargo; de la seguridad en la asignación y uso de las direcciones IP; y en la promoción de tecnologías como DNSSEC y otras que permiten dar seguridad a la operación de Internet en general. Además,

el desarrollo y cumplimiento de las políticas de ICANN contribuye a limitar los abusos de los nombres de dominio que acompañan a diversos delitos como el "phishing" y el comercio fraudulento.

La IETF, por su parte, ha incluido consideraciones de seguridad en el desarrollo de los protocolos técnicos de Internet desde sus tiempos fundacionales, y los formalizó como requisito en 2003 (Rescorla) En el origen, Internet estaba orientada ante todo a la comunicación entre nodos de la red. La seguridad de la información fue considerada siempre una prioridad y, en una paradoja que sólo es aparente, por ello no se convirtió en un principio de diseño como sí lo fueron la interoperabilidad y la apertura. El principio "de punta a punta" establece que criterios como la seguridad deben ser atendidos en los nodos, no en la red, abreviado como "red tonta, orilla inteligente". Internet se usó desde un principio para conectar sitios que procesaban información sensible; los mecanismos para protegerla evolucionaban rápidamente, como lo hacían también aquellos orientados a atacarla. Insertar los mecanismos de defensa en el interior de la red obligaría a reemplazos constantes para sobrevivir a fuerzas progresivamente superiores en el ataque. Por ello las consideraciones de seguridad se introdujeron sólo cuando fue posible proveerlas de una manera más estable. Así en la actualidad la IETF ha normalizado numerosos mecanismos que impiden diversos ataques, como los "de hombre en medio" la escucha pasiva permanente de canales por intervenciones no autorizadas (Farrel). En extensión de estas consideraciones, la gobernanza multisectorial de la ciberseguridad es la ruta al futuro.

Diversas funciones pueden conllevar un peso y participación mayor de un grupo de actores; por ejemplo, la persecución de delitos debe seguir a cargo de las fuerzas del orden legítimas y legales, la intervención de comunicaciones debe seguir pautas legales (además de principios de necesidad y proporcionalidad), la operación de redes debe continuar a cargo de las empresas autorizadas, y el desarrollo de sistemas residir en la comunidad técnica. La sociedad civil puede realizar contribuciones muy diversas, desde marcar la agenda en temas de privacidad hasta vigilar que la acción de las autoridades se mantenga dentro de la legalidad. La operación de CERTs y CSIRTs, cuyo origen está en el régimen de Administración de TI y es orgánico a

la comunidad Internet, puede también ser multisectorial, con diversos pesos para los participantes en las decisiones según se trate de entidades a cargo de la seguridad nacional, académicas, bancarias, etc.

3.3 Cibernormas

El régimen de Cibernormas es una variante del régimen multilateral en el que diversas fuentes, además de algunos gobiernos, impulsan la creación de un orden normativo para las relaciones entre Estados en el ciberespacio. El producto deseado por estos promotores es un conjunto de instrumentos normativos internacionales que regulen qué pueden hacer los Estados ante posibles hostilidades. Como se ha mencionado antes, un tratado global o varios regionales o multilaterales, de naturaleza vinculante, limitarían los alcances de las acciones hostiles, preservarían la vida y salud de la población civil, asegurarían la necesidad, debida atribución y proporcionalidad de medidas defensivas y retaliatorias ante ataques presuntos o comprobados, controlarían el comercio de software y dispositivos de posible uso hostil a la manera del Tratado de Wassenaar (Granick, 2017), y otros beneficios. La diferencia con el régimen estrictamente multilateral estriba en la inclusión, en diversos grados, de actores no gubernamentales. Hasta ahora éstos residen principalmente en instituciones académicas del ámbito de las Relaciones Internacionales, donde los análisis de la hostilidad en el ciberespacio llevan a conclusiones alarmantes y a un llamado a la acción para evitar las peores consecuencias. Hace falta tiempo para asimilar la revolución tecnológica que representa el ciberespacio y explorar la posibilidad de construir una arquitectura de disuasión similar a la que originaron las armas nucleares. Las comunidades técnica y de gobernanza de Internet observan con cierto escepticismo estos esfuerzos ya que aprecian que se encuentran lejos de los teatros operacionales ya existentes y resulta difícil que se alimenten mutuamente ambas perspectivas. Un resumen de la situación en la intersección de los regímenes de gobernanza de Internet y de Cibernormas ha sido producido por Hinojosa (Hinojosa, 2016).

Un evento distintivo en este régimen es la GCCS (Conferencia Global sobre el Ciberespacio) que se inició en Londres, y que en su sesión de La Haya en 2015 se

abrió con particular amplitud a la participación de todos los sectores (si bien conservó sesiones cerradas exclusivas para representantes gubernamentales; de manera notable, entre éstos se encuentran autoridades policiales y de procuración de justicia, no sólo del ámbito de relaciones exteriores). La sesión de 2017 se llevó a cabo en India, con un perfil internacional más bajo que las anteriores. Se preveía que India aprovecharía la Conferencia para desplegar su visión política que favorece nominalmente al enfoque multisectorial en la coordinación de recursos centrales de Internet y otros aspectos donde hay lugar para la flexibilidad, pero insiste en la autoridad gubernamental y multilateral en los temas que afectan directamente a sus intereses nacionales. Esto ocurrió efectivamente, conjuntamente con una tendencia de otros países, como Rusia y China, a manifestarse también en favor de los controles nacionales

4. Consideraciones conjuntas sobre ciberseguridad, regímenes y estrategias nacionales

Hemos señalado arriba la necesidad de problematizar el uso de la categoría "seguridad de la información" en las discusiones sobre ciberseguridad. Los especialistas en seguridad informática se refieren a la seguridad de la información como el valor determinante de su actividad; como dijimos arriba, es a partir de ésta que se determinan las estrategias de protección de su integridad, autenticidad, confidencialidad y disponibilidad, y a partir de ello la seguridad de las bases de datos, sistemas de información, computadoras y redes. Sin embargo en el contexto internacional la misma categoría representa un significado diferente, la regulación del espionaje y el acceso no autorizado de extranjeros a la información protegida del país propio, y de los nacionales bajo tutela del Estado a información, generalmente proveniente del extranjero, a cuya difusión al interior del país el Estado se opone.

La popularidad del término "ciberseguridad" ha tenido vaivenes importantes en distintos contextos. Así, en el Foro sobre Gobernanza de Internet tuvo uso intensivo en 2010, en boca y documentos de la delegación de Rusia, y posteriormente desapareció varios años para, por un lado, aparecer en la Asamblea General de la ONU y por otro, realizar un gradual regreso al IGF. Este fenómeno podría

ser explicado mediante una aplicación de la teoría agente-principal, entendiendo que Rusia habría estado buscando delegar en el IGF como agente la ejecución de su agenda de ciberseguridad, y al no tener el éxito buscado habría cambiado de foro a la Asamblea General con mejores esperanzas de avanzar en ese espacio exclusivamente intergubernamental.

Entre otras conclusiones importantes que han emergido de las discusiones y la literatura reciente (véase especialmente a Klimburg y a Kello, ya citados abundantemente) destacan:

a) Las ENCS deben orientarse a la gestión de riesgos. Con ello procede identificar los activos que la Estrategia busca proteger, los ámbitos en que se encuentran y los procedimientos de gestión de riesgos específicos aplicables a cada uno, para integrarlos en una estrategia de alcance global.
b) Las ENCS deben hacer participar orgánicamente a todos los sectores.
c) Es necesario distinguir entre delito cibernético y ciberseguridad, evitando reducir la segunda a lo primero pero sin desconocer su conexión, como se ha expuesto en el presente texto.

En años recientes se llevaron a cabo trabajos para formular en México una ENCS. Al igual que en otros países, una ENCS es parte y complemento importante para una Agenda Digital como la Estrategia Digital Nacional, que contiene elementos de seguridad desde su formulación en 2013.

El impulso propio de la OEA y sus aliados empresariales ha sido resistido correctamente por el gobierno mexicano en busca de una formulación mejor arraigada y adaptada a las necesidades del país. Se ha emitido una estrategia puntual para el sector financiero, en acuerdo con el Gobierno Federal a través de la Secretaría de Hacienda y Crédito Público (Gobierno de México, 2017; Gobierno de México, 2017), a la que falta mucho para incorporar orgánicamente una construcción multisectorial. También está a debate la adhesión de México al Convenio de Budapest.

Conclusiones

En el más breve resumen de conclusiones podemos decir lo siguiente:

1. La Ciberseguridad Nacional es un problema espinoso, de difícil definición y solución. Entre otros factores que lo vuelven complejo está la continuidad entre afectaciones a la seguridad informática de los sectores privado y público y la continuidad entre las acciones delictivas, propias del marco de la seguridad pública, y las que ponen en riesgo la viabilidad de la nación. La influencia de actores no estatales y la posibilidad de que ésta sea producto de intención o tolerancia de actores estatales capaces de negar creíblemente su participación, se complica con el "problema de atribución" que hace difícil asignar el origen de un ataque a un individuo u organización específicos de manera inequívoca en un tiempo razonable para una respuesta del Estado nacional a otros Estados.
2. Los regímenes tradicionales –multilateral o intergubernamental– no proveen marcos suficientes para la gestión de la Ciberseguridad Nacional. Es importante que el Estado mexicano reconozca el régimen multisectorial y el régimen ecléctico en el que se desarrollan sus propias operaciones y sus relaciones con la sociedad en materia de informática, gobierno electrónico, economía digital, banca, industria y otros sectores.
3. El papel de la sociedad civil organizada, las sociedades profesionales especializadas, y la comunidad técnica de Internet y en general del ramo de Tecnologías de Información y Comunicación, transversal a gobierno, industria y sociedad civil, es indispensable para el avance en Ciberseguridad Nacional.
4. En compañía de todos los sectores, el Estado debe atender a los movimientos de las grandes potencias y otros actores competentes en los regímenes multilateral y multisectorial para evitar que algunos de estos actores encubran o apalanquen sus actividades en uno de los regímenes con las que llevan a cabo directamente o a través de aliados y afines en otro régimen, en detrimento de nuestros intereses.

BIBLIOGRAFÍA

Allen, M. (2001). Social Engineering: a Means to Violating a Compute System. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/paper/529

Arquilla, J. y. (1993). *Cyberwar is Coming!* Santa Monica, CA, US: Rand Corporation. Retrieved from https://www.rand.org/pubs/reprints/RP223.html

Baym, N. (2015). *Personal Connections in the Digital Age* (2 ed.). Politi Press.

Corona, P. (2019). *Guía Práctica para la Gestión de Riesgos en Ciberseguridad.* México: en prensa.

Daltabuit, E. M. (2007). *La Seguridad de la Información.* México: Limusa.

Farrel, S. y. (n.d.). *RFC 7258.* Retrieved from https://tools.ietf.org/html/rfc7258

Franda, M. (2001). *Governing the Internet: the Emergence of an International Regime.* Boulder, CO, EUA: Lynne Rienner Pubs.

Gambetta, D. (2009). *Codes of the Underworld: How Criminals Communicate.* Princeton, NJ, EUA: Princeton.

Gartzke, E. y. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies, 24*(2), 316-348. doi:10.1080/09636412.2015.1038188

Gobierno de México. (2017). Retrieved from https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad?idiom=es

Granick, J. (2017). *Changes to export control arrangements apply to computer exploits and more.* Retrieved from https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more

Henriksen, A. (2019). The end of the road for the GGE process: the future regulation of cyberspace. *Journal of Cybersecurity*, 1-9. doi:10.1093/cybsec/tyy009

Hollis, D. (2002). Private Actors in Public International Law: Amicus Curiae and the Case for the Retention of State Sovereignty. *B.C. Int'l Comp L. Rev, 235.*

Hoorenbeck, M. A. (2018). *Cybersecurity Culture, Norms, and Values - Internet Governance Forum, Best Practice Forum on Cybersecurity.* United Nations Organization. Retrieved from https://www.academia.edu/37417784/Cybersecurity_Culture_Norms_and_Values

Hurwitz, R. (2013-14). Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs: International Engagement*

on Cyber III: State Building on a New Frontier, 17-28. Retrieved from https://www.jstor.org/stable/43134319

Kello, L. (2013, Fall). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security (Quarterly Journal), 38*(2), 7-40.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* London, UK: Penguin Press.

Kolias, G. K. (2017). DDos in the IoT: Mirai and Other Botnets. *Computer*, 80-84.

Krasner, S. (1982). Rebimes and the limits of realism: regimes as autonomous variables. *International Organizations*, 497-510.

Kummer. (2004). *Personal communication.*

Kure, H. S. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Science, 8*(898), 1-29. doi:doi:10.3390/app8060898

López-Portillo Romano, J. R. (2018). *Retos y oportunidades del cambio tecnológico exponencial.* México, México: Fondo de Cultura Económica (FCE).

Manual, T. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, UK: Cambridge.

McCoy, D. B. (2008). Shining Light in Dark Places: Understanding the TOR Network. In N. y. Borisov, *Privacy Enhancing Technologies, PETS 2008, Lectures in Computer Science vo. 5134.* Berlin y Heidelberg: Springer.

México, Gobierno de. (2011). *Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published.* Retrieved from Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published: Gobierno de México, 2011, https://www.gob.mx/wikiguias/articulos/esquema-de-interoperabilidad-y-de-datos-abiertos-de-la-administracion-publica-federal-eida?state=published

Office of the Historian, U. G. (1946). *National Security Council Directive on Office of Speical Projects.*

Osula, A.-M. y. (2016). *International Norms: Legal, Policy & Industry Perspectives.* Tallinn: NATO CCDCOE.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.

ECIW2008 - Proceedings of the 7th European Conference on Information Warfare.

Pawlak, P. y. (2017). Politics of Cybersecurity Capacity Building: Conundrum and Opportunity. *Journal of Cyber Policy*, 123-144. doi:10.1080/23738871.2017.1294610

Pisanty, A. (2015). The vexing problem of oversight. In W. Drake, *The Working Group on Internet Governance - 10th Anniversary Reflections.* Berlin y Johannesburgo: Springer y APC.

Pisanty, A. (2016). Principios fundamentales y gobernanza de Internet. In J. e. Thumfart, *Pensar Internet.* México: Universidad Iberoamericana.

Pisanty, A. (2018). *Llámame Internet.* México: Secretaría de Cultura - EDUCAL.

Rescorla, F. y. (n.d.). *RFC 3552.* Retrieved from https://tools.ietf.org/html/rfc3552

Richardson, R. y. (2017). Ransomware; Evolution, Mitigation and Prevention. *International Management Review, 13*(1). Retrieved from https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

Scholte, A. (2017). The Net and the Nation State. In U. Kohl, *The Net and the Nation State: Multidisciplinary Perspectives in Internet Governance.* Cambridge. doi:10.1017/9781316534168

Stanislakwski, B. H. (2004). Transnational "Bads" in the Globalized World: The Case of Transnational Organized Crime. *Public Integrity*, 155-170.

Sullivan, A. (2016). "The Internet is made with carrots, not sticks". *TechCrunch*. Retrieved from https://techcrunch.com/2016/04/07/the-internet-is-made-with-carrots-not-sticks/

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and security Law*, 229-244. doi:https://doi.org/10.1093/jcsl/krs019

UIT. (2006). Retrieved from
https://www.itu.int/ITU-D/cybersecurity/docs/WTDC06_resolution_45-e.pdf

Xinhua. (n.d.). Retrieved from http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_4.htm

Yampolsky, A. H. (2015). A language for describing attacks on cyber-physical systms. *International Journal of Critical Infrastructure Protection, 8*, 40-52. doi:https://doi.org/1.1016/j.ijcip.201409.003