Revista de Administración Pública

INAP

Esfera ética del ciberconflicto

Mario Vignettes

Resumen: Es necesario iniciar en México el debate de los límites éticos de la ciberseguridad ante la vertiginosa dinámica del mundo digital y la postura estratégica que están adoptando Estados, empresas e individuos alrededor del mundo.

Parte de este debate consiste en explorar la relación que existe entre la ciberseguridad y la ética desde la postura consecuencialista. Para este propósito se utilizan dos constructos básicos: la ciberdefensa activa y el ciberconflicto. Se plantean dos dilemas éticos fundamentales y se sugieren criterios básicos para superarlos. Finalmente se ofrecen cinco conclusiones generales. Esta colaboración es de carácter exploratorio y de ninguna manera puede esperarse respuestas definitivas a cuestionamientos tan profundos como las consecuencias éticas del uso de ciberarmas.

Palabras clave: Ciberdefensa, Medidas Activas, Dilema Ético, Ciberconflicto

Ethical sphere of cyber conflict

Abstract: It is necessary to start in Mexico the debate on the ethical limits of cybersecurity in the face of the vertiginous dynamics of the digital world and the strategic position that

states, companies and individuals are adopting around the world.

Part of this debate is to explore the relationship between cybersecurity and ethics from the consequentialist position. Two basic constructs are used for this purpose: active cyber defense and cyber conflict. Two fundamental ethical dilemmas arise and basic criteria are suggested to overcome them. Finally, five general conclusions are offered. This collaboration is exploratory in nature and in no way can definitive answers to such deep questions as the ethical consequences of the use of cyber weapons be expected.

Keywords: Cyber Defense, Active Measures, Ethical Dilemma, Cyber Conflict

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 16 de febrero de 2019

Revista de Administración Pública

INAP

Esfera ética del ciberconflicto

Mario Vignettes*

1. Enfoque y orientación

México es uno de los países más atacados del mundo desde el ciberespacio. Ello tiene consecuencias negativas en muchos ámbitos y niveles. Es necesario asumir que en el futuro, México requerirá adoptar medidas activas para reforzar la postura de ciberseguridad actual, lo cual implicará una revolución en la cultura estratégica nacional, lo que incluye plantearse y resolver dilemas éticos insólitos para nuestra sociedad.

A partir de los conceptos de ciberdefensa activa y ciberconflicto, se explora la relación entre la ciberseguridad y la ética desde la postura consecuencialista, porque la tradicional postura normativista es incapaz de caracterizar los dilemas que plantea una defensa activa en el ciberespacio. Las conclusiones que se ofrecen son de naturaleza provisional y quizá insuficientes, pero tienen el mérito de abril el debate nacional en la materia.

* Doctor en Derecho por la Facultad de Derecho de la UNAM. Diplomado en Ejercicio Jurisdiccional y Justicia Constitucional impartido por la Suprema Corte de Justicia de la Nación. Integra la planta docente del Instituto Nacional de Administración Pública (INAP) desde 2005. Ejerció profesionalmente la Inteligencia de Estado entre 1995 y 2018. Actualmente es Consultor en evaluación de riesgos y control de crisis.

El ciberespacio

El ciberespacio es un "ámbito intangible, de naturaleza global, soportado por TIC, que es utilizado para la interacción entre individuos y entidades públicas y privadas"[1] o dicho de otro modo, es un entorno "informativo evolutivo, interconectado, vagamente acotado que utiliza métodos de comunicación tecnológicamente gestionados por programas [que] almacenan, transportan, interpretan y median información a través de los dominios virtual y físico, interactuando con comunicación, información, y con elementos cognitivos y sociales"[2]. Permea la vida individual y social con creciente importancia y con repercusiones aún ambiguas.

Lo que sabemos es que su naturaleza ubicua hace obsoleto el concepto de frontera nacional, ya que el ciberespacio comprende a "todas las redes del mundo y cualquier cosa conectada a, o controlada por esas redes"[3]. Ello obliga a replantear las tradicionales categorías analíticas útiles para estudiar la geopolítica. Además, el ciberespacio cruza también las fronteras domésticas con los dispositivos cuyo uso harán realidad los "hogares inteligentes" y con ello, un monitoreo permanente y voluntario de los usuarios-consumidores-ciudadanos.

Precisamente por ello es indispensable contar con una definición de ciberseguridad. La Unión Internacional de Telecomunicaciones señala:

> "Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación,

1 Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

2 David Ormrod y Benjamin Turnbull, "The Cyber conceptual framework for developing a military doctrine", Defence Studies, 2016 Vol. 16, No. 3, Routledg, pp. 208 y 281. El gobierno federal mexicano lo concibe como "Realidad virtual o simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo", Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

3 R. A. Clarke y R. K. Knake, "Cyber war: The next threat to national security and what to do about it, New York, Harperd Collins, 2012, citado en David Ormrod et al., Op cit., p. 284.

> prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
> Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.
> La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio, y la confidencialidad"[4]

El Gobierno Federal mexicano utiliza la siguiente:

> "Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno"[5]

Ninguna incluye la noción "bien público" asociada a la definición de Ciberseguridad. Como toda clase de seguridad, ésta debe ser el desenlace virtuoso de una estrategia gubernamental comprensiva que guíe efectivamente a las instancias gubernamentales, pero sobre todo a la sociedad civil organizada (empresas, universidades, tanques de pensamiento) y a los usuarios individuales.

4 Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es, citado en Enrique Francisco Galindo Ceballos, La seguridad cibernética en el nuevo entorno operativo, Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, p. 186.

5 Gobierno Federal, Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

El ambito ético

Para efectos del este ensayo es necesario delimitar el alcance de tres términos que son contiguos, pero de ninguna manera sinónimos, a saber:

- Axiología es una disciplina filosófica enfocada en la "Teoría de los Valores". Estudia críticamente los valores éticos y estéticos, así como los "disvalores" que se asocian a aquellos. Por tanto, tiene un fuerte sentido teórico y didáctico.
- Moral es una técnica de control social que se caracteriza por ser: heterónoma, abstracta, unilateral y no coercitiva. Estas dos últimas características señalan su diferencia con el Derecho. La moral depende fuertemente del contexto social por lo que en un lugar y una época determinada, cierta conducta individual o colectiva puede ser calificada de inmoral por otra sociedad que se encuentre alejada en el espacio o en el tiempo. La moral está formada por usos y costumbres, es decir, la repetición de actos a través del tiempo que se consideran necesarios o imperiosos para alcanzar algún fin práctico. Por tanto, tiene un fuerte sentido deontológico y colectivo.
- Ética es una disciplina práctica centrada en la conducta humana y en la toma de decisiones en los ámbitos personal o profesional. A lo largo de la historia, se han definido dos grandes posturas que abordan esta disciplina:
  a) La deontológica, que postula que la ética es el estudio del fin de las conductas humanas y de la valoración de los medios para lograrlos. Esta postura, también llamada ´ética normativa´, es la más antigua y cercana a la axiología ya que tiende a considerar que los estándares éticos son absolutos y trascienden a toda circunstancia social o histórica, lo que marca una diferencia sustancial con la moral. Con base en este punto de vista, algunas profesiones o empresas establecen Códigos Éticos[6]. Desde el mismo

6 Esta postura tiene la ventaja de concentrar los «valores compartidos que guían la manera en que un individuo (y una organización) se comporta, y define una cultura institucional». Christopher E. Bailey, "The Intelligence Comunity ethos: a closely regulated profession", v. 3, n. 2, Autumn–Winter, 2012, p. 54. Disponible en: http://journals.fcla.edu/ijie/article/view/83453.

enfoque, el Poder Ejecutivo Federal adoptó un Código de Ética de los servidores públicos federales que incluye reglas de integridad[7] lo cual, sin duda, es meritorio en la medida en que sea conocido y practicado.

b) La consecuencialista, que sostiene que un acto particular es éticamente correcto o incorrecto, juzgando sus consecuencias reales[8]. Esta familia de escuelas éticas está arraigada en la tradición filosófica del utilitarismo. La diferencia más notable con la posición deontológica es que afirma que los estándares éticos son relativos en el tiempo y en el espacio, están vinculados a las circunstancias particulares del tomador de decisiones que designa como 'agente'.

Si bien ambos abordajes tienen cualidades, las características de la de ciberespacio no permiten, como se argumentará más adelante, estudiar con provecho el tema desde la ética deontológica.

2. Globalización y Ciberseguridad

El telón de fondo de cualquier comentario responsable sobre ciberseguridad es la realidad que plantea la globalización. Para Adda, la globalización se caracteriza por la progresiva unificación de los mercados mundiales de bienes, servicios y capitales, así como por una creciente integración mundial de la producción, lo cual genera el debilitamiento de las fronteras físicas y reglamentarias que traban la acumulación a escala mundial del capital[9]. Frente a esta realidad es que todo Estado soberano debe proyectar su poder nacional en promoción de sus intereses nacionales. Sin embargo,

> "Lo que hace a la globalización un componente nuevo y esencial de la seguridad internacional contemporá-

7 Código de Ética de los Servidores Públicos del Gobierno Federal, las Reglas de Integridad para el Ejercicio de la Función Pública, DOF del 20 de agosto de 2015, consultado el 10 de agosto de 2018, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5404568&fecha=20/08/2015

8 Es decir, no futuras, previstas, intentadas o deseadas; independientemente de las intenciones de su autor.

9 Cfr. Adda Jacques: La Globalización de la Economía, Editorial Sequitur, Madrid, 1999, p. 203.

> nea son las cada vez más complejas condiciones bajo las cuales los actores internacionales ejercen poder"[10].

Entre esas complejas condiciones debe contarse la esfera ética del ejercicio de poder, particularmente en el ciberespacio. Tras casi tres lustros, sigue siendo válida la reflexión de Kay en el sentido de que es muy difícil concluir con exactitud la forma en que la globalización impacta a la seguridad. Postula que:

> "Si la seguridad es la búsqueda por la ausencia o la mengua de riesgos en un mundo anárquico, la globalización debe incrementar o decrementar los resultados de seguridad. Si la seguridad es vista como una búsqueda particular de las naciones-Estados para proveerse de defensa, entonces la globalización también propicia tanto retos como oportunidades"[11].

Enfoquémonos en los retos. El 44% de los 9,500 ejecutivos de empresas que contestaron la encuesta sobre el Estado Global de la Seguridad de la Información 2018[12] afirman carecer de información sobre una estrategia de seguridad digital. Por otra parte, durante el primer semestre de 2018 se registraron 5.9 mil millones de ataques de a nivel mundial, es decir un 102% que en el mismo periodo de 2017, lo cual marca una tendencia mundial preocupante. Pero en México esos ataques se incrementaron en un 215% en el mismo periodo[13]. De hecho existen estudios que señalan a México como el "tercer país más vulnerado y con mayor índice de ataques a nivel mundial, únicamente detrás de Estados Unidos y el Reino Unido"[14]. Está claro que México enfrenta una variedad de ciberamenazas que han sido agrupadas en tres categorías, a saber:

10 Cfr. Sean Kay: "Globalization, Power, and Security", Security Dialogue vol. 35, no. 1. March 2004, p. 11.
11 Sean Kay, Op. cit., p. 10.
12 Christopher Castelli, Revitalizing privacy and trust in a data-driven world, Key findings from GSISS 2018 PWC, consultado el 21 de Agosto de 2018, disponible en https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf
13 Omar Ortega, "México, la tercera nación con más ciberataques en el mundo", El Financiero, 30 de julio de 2018, p. 42. Cita al Reporte Semestral de Ciberseguridad de SonicWall. Disponible en: http://www.elfinanciero.com.mx/tech/mexico-la-tercer-nacion-con-mas-ciberataques-en-el-mundo
14 Ibid.

> "...la ciberdelincuencia, especialmente el robo, el fraude y la difusión de pornografía infantil. La segunda es el ciberespionaje de Estados Unidos, Rusia, China e Irán, quienes buscan extraer información política, económica y comercial, sobre todo en materia energética. En tercer lugar está el desafío de de colectivos *hacktivistas* como *Anonymous*, los cuales poseen las capacidades necesarias para irrumpir en los sistemas del Estado e imponer sus agendas"[15]

Igualmente claro es que la sociedad civil requiere mucha mayor información respecto de tales amenazas, a juzgar por su comportamiento cotidiano. Un indicador de esa displicencia es que durante 2017 el sistema financiero mexicano se abstuvo de presentar denuncias de ciberdelitos[16].

El telón de fondo de lo anterior son los principios de política exterior con que el Ejecutivo Federal de México conduce las relaciones y que están señalados en la fracción X del artículo 89 constitucional.

> "Si bien la coherencia interna de estos principios fue una sólida base de acción en la etapa previa a la globalización, estos principios sin duda se convierten en limitaciones concretas a una participación más activa en la seguridad hemisférica, pues estaban fundados en una visión internacional en la que los Estados-naciones eran los actores centrales de las relaciones internacionales. Sin embargo, la configuración internacional ha cambiado de manera acelerada: las nuevas amenazas internacionales salen de la esfera de los Estados, el incremento de los intercambios a través de la telecomunicaciones y los flujos financieros atraviesan las fronteras virtualmente, la delincuencia organizada opera en redes con frecuencia articuladas con los poderes económicos y políticos de diversos

15 Edgar Iván Espinosa, Hacia una estrategia nacional de ciberseguridad en México, Revista de Administración Pública No. 136, Volumen L, Nº 1, (enero-abril 2015), INAP, México, p. 143.

16 Jeanette Leyva, "Bancos no acostumbran denunciar ciber delitos: PGR", El Financiero, 22 de agosto de 2018, p. 11.

países, factores ante los cuales la doctrina de política exterior, no está preparada para responder"[17].

El panorama concreto de la ciberseguridad en México ya ha sido diagnosticado a profundidad por expertos nacionales. Remitimos al lector a ensayos sólidos que describen detalladamente el esfuerzo del gobierno federal en materia de ciberseguridad[18], que plantean un inventario de acciones que deben ser asumidas por gobiernos, empresas y la sociedad civil para 2022[19] o bien que instan al establecimiento de un cibercomando plenamente operativo a partir del concepto de ciberdefensa[20].

De hecho, el Objetivo Sectorial 2 del Programa Sectorial de Defensa Nacional 2013-2018 denominado "Fortalecer el Sistema de Inteligencia Militar", tiene entre sus indicadores el 4 "Impulsar el desarrollo de la cuarta dimensión de operaciones militares denominada "ciberespacio", mediante la creación de un Centro de Operaciones del Ciberespacio". Ello se justifica porque "…se requiere desarrollar las capacidades de defensa y seguridad en la cuarta dimensión de operaciones denominada 'Ciberespacio', mediante la creación de un organismo, con instalaciones, equipo y personal adecuados, con el objeto de proteger y asegurar las Tecnologías de la Información y Comunicaciones de la SEDENA y en su caso, la red de infraestructura crítica nacional."[21] SEDENA debe replantear su postura a este respecto.

3. El ciberconflicto

La coyuntura revelada por los datos estadísticos citados, justifica examinar nociones que son arcanas a la sociedad

17 Raúl Benítez Manaut y Georgina Sánchez: Avances y Límites de la participación de México en la Seguridad Hemisférica en el Siglo XXI en "Cooperación y conflicto en las Américas. Seguridad Hemisférica: Un largo y sinuoso camino"; María Cristina Rosas (coordinadora); UNAM – Centro de Estudios de Defensa Hemisférica; México; 2003; pp. 167 y 168.

18 Enrique Francisco Galindo Ceballos, Op. cit., pp. 181 a 198.

19 Alejandro Pisanty, Algunos rasgos del futuro de las agendas digitales nacionales: el caso de México, Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, pp. 13 a 43.

20 Edgar Iván Espinosa, Op. cit. pp. 115 a 146.

21 Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

y la cultura estratégica mexicanas como ciberdefensa. Ignorar el cúmulo de amenazas de las que México es blanco en el ciberespacio, simplemente no es una opción.

El Estado mexicano entiende por ciberdefensa el "conjunto de acciones, recursos y mecanismos del Estado en materia de Seguridad Nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional"[22]. Este concepto no está definido en documentos oficiales mexicanos, pero si el de infraestructuras críticas de información, es decir, "Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia"[23]

Algunas de ellas son de uso dual y merecerían también protección bajo el concepto de ciberdefensa, piénsese en "… una amplia variedad de sistemas guiados por computadora, como la red del sistema de posicionamiento global satelital (GPS por sus siglas en ingles), e infraestructura de energía, comunicaciones, de agua potable o sanitaria, o bien sistemas de refinamiento petrolero o químico." [24]

La defensa se justifica por la necesidad práctica a cargo del Estado –en este caso México– de prevenir, acotar y responder a los ataques de adversarios o enemigos. Por tanto, su noción simétrica es la de ciberataque, concebido como "acciones deliberadas para alterar, desordenar, engañar, degradar o destruir sistemas o redes de cómputo o la información y/o programas residentes en o que están siendo

22 Gobierno Federal, Glosario del Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

23 ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, en su versión publicada en el DOF, 2 de febrero de 2016.

24 Randall R. Dipert, The Ethics of Cyberwarfare, Journal of Military Ethics, Vol. 9, No. 4, 2010, p. 390. Se refiere a M. Walzer, Just and Unjust War, 4th ed., Basic Books, New York, 2006, pp. 144 a 151.

trasmitidos en esos sistemas o redes"[25] Todo administrador de sistemas y redes, públicas o privadas, es responsable de la defesa pasiva de las mismas. Esa es la premisa del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).

Según Randall R. Dipert "Si los ataques entre entidades políticas están suficientemente 'extendidos' entonces hablamos de ciberguerra"[26]. Según este autor es una cuestión de intensidad y de intensión. Empero, el término "guerra" tradicionalmente denota el uso de fuerza letal contra humanos en el marco de un conflicto armado entre comunidades políticas. La noción popular de ciberguerra se aleja de algunos de estos elementos. Por ello, en el medio estadounidense empieza a generalizarse el uso de "guerra kinética"[27] para implicar el efecto físico de la presión (proyectil, convencional o nuclear) o el fuego (explosión, convencional o nuclear) sobre humanos o estructuras y distinguirla así, de otras formas de agresión que no implican movimiento de fuerzas físicas como la guerra psicológica, la guerra económica, la guerra criptográfica, guerra electrónica, guerra sónica o la ciberguerra[28].

Ciberconflicto parece más adecuado para describir el contexto y las consecuencias de los ciberataques, y no por ello restarles peso a su impacto negativo que puede clasificarse desde la desobediencia civil hasta el terrorismo, lo cual no es menor. El ciberconflicto implica que un agente,

25 William A. Owens Kenneth Dam y Herbert S. Lin (ed.) Technology, Policy, law and Ethics regarding US adquisition and Use of Cyberattack Capabilities, The National Academy Press, Washington DC, 2009 citado en David Danks Y Joseph H. Danks, "The Moral Permissibility of Automated Responses During Cyberwar", Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 25.

26 Randall R. Dipert, The Ethics..., p. 397. Se ha sugerido la siguiente definición de ciberguerra "... el uso de computadoras para entorpecer las actividades de un país enemigo, especialmente el ataque deliberado de sistemas de comunicación" W. H. Boothby, , Oxford University Press, Oxford, 2012 citado en David Ormrod et al., Op. cit., p. 288.

27 Timothy Noah, Birth of a Washington Word, When warfare gets "kinetic", Slate, Noviembre de 2002, consultado el 5 de Agosto de 2018, disponible en: http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html

28 Para un estudio de la ciberguerra desde el Derecho Internacional Público remitimos al lector a María Pilar Llorens. Los desafíos del uso de la fuerza en el ciberespacio, Anuario Mexicano de Derecho Internacional, vol. XVII, enero-diciembre, UNAM, 2017, pp. 785 a 816.

individual o colectivo de forma autónoma o patrocinada, pero siempre voluntaria, explota "la infraestructura de red digital y la información contenida en ella, o impacta en los beneficios proporcionados por los sistemas de información enlazados en red, como parte de una ofensiva ideológica dirigida al gobierno, a la población, o a la industria de la nación".[29]

Lógicamente, el elemento definitorio del ciberconflicto es el instrumento por el que se causa daño, que en el ciberespacio es la ciberarma y que puede generar alteración, desórdenes, engaño, degradación o destrucción de sistemas o información. La dificultad inicia a partir de que no existe consenso internacional sobre lo que implica y denota exactamente ese término.

Una definición provisional define ciberarma como un "código de computadora que es usado, o diseñado para ser usado con el propósito de amenazar o causar daño físico, funcional o mental a estructuras, sistemas o seres vivientes", que incluye además dos dimensiones psicológicas, a saber: a) la intención del perpetrador de amenazar o de causar daño a un blanco, y b) la anticipación con la que el perpetrador anuncia su uso y su daño potencial[30]. Por su naturaleza incorpórea, toda ciberarma cuenta con una arquitectura peculiar que, al día de hoy, integra tres capas de ofensivo, a saber:

1. "Software de reconocimiento o espionaje para determinar la naturaleza o debilidad del sistema, y para impactarlo de forma única (en vez de, digamos, también dañar sistemas de información civiles).
2. "Software de producción de daño que altere de forma dañosa el comportamiento del del enemigo o que produzca otros efectos indeseables, incluyendo posiblemente muertes o daño físico a sistemas. Estas son las bombas lógicas o ciber en sí mismas.

29 G. Szentgali, The NATO policy on cyber defence: the road so far, Academic & Applied Research in Military Science (AARMS), No. 12, 2013, citado en David Ormrod et al., Op. cit., p. 289.

30 Thomas Rid y Peter McBurney, Cyber-Weapons, The RUSI Journal, Febrero de 2012, pp. 7 y 8, consultado el 10 de agosto, disponible en https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354

3. "Software de evaluación de daños que determinen la efectividad del de producción de daño."[31]

Pero no toda ciberarma es letal en el sentido literal de la palabra. Puede ser repelida antes de que produzca daño al ser "filtrada" por el sistemablanco o bien, ser removida y puesta en cuarentena al tiempo que el daño puede ser acotado reiniciando el sistema atacado con los datos existentes antes del ataque, acciones que pueden tomar desde microsegundos hasta semanas. Entonces, "Desde el punto de vista del uso ofensivo de la ciberarma, esto las hace armas de cuya efectividad disminuye rápidamente"[32] Por tanto podrían clasificarse en ciberarmas de grado civil y de grado militar. Para este último caso, existen tres categorías de blancos, a saber:

> "Primero, las ciberarmas pueden impactar e inhabilitar a las principales cadenas de comando, específicamente a las de comando y control; de comunicación y de recolección de información, así como a las de comunicación de órdenes precisas para maniobrar, defender, o atacar. Los datos de comando y control, podrían ser bloqueados alterados, o podría insertarse falsos informes u órdenes. La mayoría de las organizaciones militares modernas han endurecido sus canales de comunicación (tales como embeber, poner escudos o proteger de otras formas los cables eléctricos y ópticos), instalando esquemas de encripción elaborados, y sistemas redundantes.
> Segundo, las armas o los sistemas de armas pueden resultar inoperantes por un tiempo o incluso saboteados físicamente por mensajes falsos o intrusiones en los sistemas de información que los controlan; en caso extremo, podrían ser dirigidos por un enemigo para atacar un blanco falso.
> Finalmente, las ciberarmas pueden impactar la infraestructura de uso conjunto, esto es, sistemas y estructuras tanto para uso civil como militar, o incluso blancos civiles con la finalidad de desmoralizar, debilitar, o confundir al ejército enemigo y al liderazgo civil."[33]

31 Randall R. Dipert, The Ethics..., p. 391.
32 Ibid.
33 Randall R. Dipert, The Ethics..., pp. 389 y 390.

Pero este esfuerzo, aún incipiente, de definición y clasificación puede llevar a la falsa conclusión de que hay una comprensión cabal de las ciberarmas. Muy por el contrario, "los mecanismos mediante los cuales las ciberarmas mueven y afectan a las computadoras no son bien comprendidas, y uno puede imaginarse efectos ubicuos incluso peores a los de las armas químicas, que no son deseados pero que, sin embargo, afectan a áreas relativamente limitadas"[34] Esto es un dato cardinal para la esfera ética del ciberconflicto, ya que abre espacios de incertidumbre enormes.

Dos características que definen al ciberconflicto deben tenerse presentes: a) la ciberseguridad es cara en tanto que la acción ofensiva es comparativamente barata, lo que pone en desventaja a Estados y empresas frente a los perpetradores que van desde el individuo hasta los Estados patrocinadores de ciberataques y, b) los efectos laterales no deseados pueden ser más letales que el propio ciberataque y ser adecuadamente anticipados es particularmente difícil.[35]

Considerando lo anterior, generar inteligencia es aún más complicado. Empero, hacerlo es la respuesta racional de Estados y grandes empresas para acotar la incertidumbre que siembra el ciberconflicto. Ello llevará a una revolución dentro del mundo de la inteligencia porque las misiones se centrarán particularmente sobre: a) la configuración de la red de cómputo del adversario, b) la planeación del ciberataque, y c) el autor del ciberataque. La ubicación de los sistemas afectados es mucho menos importante[36]. Ello implica que la respuesta a esa clase específica de amenazas no se circunscribe al ciberespacio. Por el contrario, tiene un contexto social, un sustrato organizacional, un impacto económico y soporte en alguna red personal.

Otro género de dificultades surgen con las diferentes posturas estratégicas que puedan adoptar los blancos. La defensa o protección pasiva de la propia infraestructura e información, de los sistemas y su operatividad no parecen

34 Edward T. Barrett, Warfare in a New Domain: The Ethics of Military Cyber-Operations, Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 10.
35 Cfr. Randall R. Dipert, The Ethics..., p. 385.
36 Cfr. David Ormrod et al., op. cit., p. 289.

plantear mayores desafíos legales. Pero la postura de defensa activa, es decir las ciberoperaciones ofensivas, aún es debatida legalmente.

El argumento estrictamente legal es que el Derecho Internacional Público estipula que los civiles y los objetos civiles no deben ser 'objeto de ataque', porque un ataque kinético se define como el uso de fuerza que causa muerte, lesiones, daños, y destrucción. Sin embargo, un arma no letal deja de lado el uso de la fuerza como en el caso de sistemas de denegación activa (*active denial system* –ADS– por sus siglas en inglés) por tanto es lícito y ético usarlo contra perpetradores civiles[37].

Sin embargo, detrás de esta justificación están las suposiciones no comprobadas de que las ciberarmas no fallan y de que pueden contenerse las repercusiones de los cibertaques. Por supuesto, estos aspectos tienen sin cuidado a los perpetradores pero son necesaria materia de deliberación en las esferas militares y gubernamentales ya que los sistemas o los datos de civiles inocentes, pudiesen ser destruidos o inhabilitados por una respuesta activa. Ante una catástrofe informática desatada por una medida activa que sea percibida como injusta por el público, el Estado responsable podría ver mermada su base de apoyo público "sin importar cuan valioso sea al objetivo político"[38]

La posibilidad de que un ciberataque tenga repercusiones físicas similares a las de un ataque kinético, aún son escasas, pero no improbables. Por tanto, el "uso de la fuerza" en defensa propia, previsto en el artículo 51 de la Carta de las Naciones Unidas parece un fundamento endeble para normar la realidad que implica el cúmulo de ciberataques en las modalidades y niveles actuales, es decir, por ahora la justificación de estricto derecho de una defensa activa por parte de un Estado parece inoperante. Ello abre la posibilidad de explorar una justificación de orden ético partiendo de un abordaje alejado del normativismo.

37 Cfr. Edward T. Barrett, Op. cit., p. 11.

38 Charles J. Dunlap Jr., Some Reflections on the Intersection of Law and Ethics in Cyber War, Air & Space Power Journal, January-February 2013, pp. 27 y 28.

5. Ética consecuencialista[39]

El utilitarismo no está exento de detractores que con variado éxito, refutan sus posiciones más conocidas como el hedonismo. Sin embargo, desde Jeremy Bentham (1748-1832) o John Stuart Mill (1806-1873), el utilitarismo ha evolucionado dando origen, entre otras, a la ética consecuencialista que debe ser juzgada por sus méritos propios, y no en el marco del utilitarismo.

Ahora bien, hay posturas consecuentalistas que arrojan saldos absurdos, que no se revisan aquí en obvio de espacio y tiempo. Por ello, este ensayo se guía por el consecuencialismo evaluativo que establece que la calificación ética de una decisión debe basarse únicamente en el valor de las consecuencias realmente provocadas, sin considerar las características no evaluables de las consecuencias. Este enfoque ético distingue entre 'agente' que es el ser humano que realiza una acción y por tanto que toma una decisión, y el 'observador' que es todo aquel que reconoce una acción o decisión ajena, participe o no de sus consecuencias.

Para la mayoría de los consecuencialistas el valor de una consecuencia se identifica con la 'utilidad total' del acto o decisión, es decir su efecto benéfico. Sus teorías intentan expresar las condiciones necesarias y suficientes para que un acto sea considerado ético. Ello exime al 'agente' de calcular las diferentes utilidades derivadas de su acto, entre otras razones porque muy probablemente cometerán serios errores de cálculo que los llevarían a realizar actos que acotarían la utilidad. En cambio el agente debe seguir sus intuiciones éticas, ya que ellas lo conducirán a realizar actos o a tomar decisiones que maximicen la utilidad, al menos en circunstancias parecidas.

Los opositores a esta posición, de forma muy esquemática, han argumentado lo siguiente:

a) Si la utilidad total es el criterio de la corrección ética, entonces parecería que nadie podría establecer

39 El presente apartado sigue las líneas generales de Sinnott-Armstrong, Walter, "Consequentialism", (Winter 2015 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2015/entries/consequentialism/>.

lo qué es ético lo que desembocaría en un escepticismo general. Los consecuencialistas afirman que hay poderosas razones para creer que ciertos actos reducen la utilidad (terrorismo por ejemplo), aun en el caso de que no se haya evaluado cada consecuencia de un acto como ese, pero reconocen que existen severos límites al conocimiento de lo que puede ser éticamente correcto.

b) Hay que evaluar las consecuencias probables, previsibles o intencionadas en lugar de las reales. Las teorías que se enfocan en las consecuencias reales u objetivamente probables con frecuencia se describen como consecuencialismo objetivo, mientras que las que se centran en las consecuencias intencionales o previstas se agrupan bajo la denominación de consecuencialismo subjetivo.

Mediante el uso de la noción legal de causa próxima podrían acercarse ambas posiciones. Si los consecuencialistas definen consecuencias en términos de lo que es causado, entonces la noción de causalidad que se use para definir las consecuencias afecta directamente la clase y cantidad de eventos futuros que se asuman como consecuencias.

Cuando los actos voluntarios y las coincidencias intervienen en cierta cadena causal, entonces los resultados no son vistos como causados por los actos más allá de las condiciones necesarias que forman parte de la cadena causal. Ahora, si se asume que un acto debe ser una causa próxima de una consecuencia, un consecuencialistas argumenta que la corrección ética del acto está determinada únicamente por tal consecuencia próxima. Esta posición, que podría llamarse consecuencialismo próximo, hace más fácil para los agentes y para los observadores justificar los juicios éticos de los actos porque obvia la necesidad de predecir consecuencias no próximas en el tiempo o en la geografía.

Por otra parte, algunos consecuencialistas argumentan que un acto es éticamente incorrecto sí y sólo sí las consecuencias del acto incluyen un valor total menor desde la perspectiva del agente. Un movimiento clave aquí es adoptar la perspectiva del agente al juzgar el acto realizado, con ello se pretende capturar las intuiciones éticas de sentido común. Se aplicarán estas nociones más adelante.

Habiendo dicho eso, reflexionemos. Un ciberataque implica daño. El ciberdaño conlleva degradación del funcionamiento de un sistema (una persona, una máquina, un programa o una economía) o un artefacto (vehículo de conducción autónoma, marcapasos cardiaco inserto en una persona, por ejemplo) "causado intencionalmente por un agente, vía una red informática…"[40] para "crear efectos emergentes sobre sistemas interconectados de naturaleza física, social o de comportamiento"[41]

Para un país como el nuestro con el nivel de ciberataques registrados, es imperativo resguardar la integridad de sistemas y artefactos que benefician a los individuos mexicanos por medios pasivos, pero también es legítimo complementar nuestra ciberdefensa con medios activos, porque la promoción de la seguridad nacional implica la salvaguarda de la población, el territorio y el ejercicio de la soberanía en cualquier circunstancia.

6. Dilemas éticos del ciberconflicto

El problema de la atribución

Por la propia naturaleza del ciberespacio y de los ciberataques, la identificación de los perpetradores es una tarea compleja ya que con frecuencia, únicamente se cuenta con evidencia circunstancial. Dos incógnitas con repercusiones éticas plantea un ciberataque: a) atribuir el ciberdaño causado, y b) evaluar las consecuencias de responderlo activamente.

Sin duda, para justificar éticamente el adoptar una respuesta (R) en contra de una parte (P) se requiere determinar con alto grado de probabilidad que (P) es responsable de un intento real (H) del daño (D) y que éste implica violación a la soberanía y que causó intencionalmente degradación tangible a algún recurso nacional, sea de propiedad pública o privada, donde el monto de la justificación que es éticamente requerida depende en parte de la naturaleza tanto de R como de H, entre otros factores, como proporcionalidad, inmediatez

40 Randall R. Dipert, Op. cit., 397.
41 David Ormrod et al., Op. cit., p. 282.

y acotamiento de R exclusivamente a P [42]. Responder activamente, más concretamente, coordinar un contra ataque en el ciberespacio, implica iniciar un ciberconflicto[43] con todo lo que ello implica en el plano técnico, político, jurídico y ético.

Dipert opina que "Parece haber muy pocos casos históricos en los cuales un Estado haya sido atacado pero tenga muy poca información respecto de quién lo atacó". Las fuentes son fácilmente falsificables como "protocolos de internet (IP) o de los poco confiables de proveedores de internet (ISP)" [44]

Además, hay muchas técnicas informáticas y herramientas para ocultar la identidad propia en el ciberespacio "distribuyendo el ataque a través de múltiples sistemas o agentes, o disfrazando al responsable de algún H" [45] lo que tiene el potencial de involucrar a personas, sistemas e información inocente en un ataque. Parece poco probable que la definición de la identidad del perpetrador pueda lograrse por medios estrictamente técnicos.

Una solución ética y posible vendrá por lo que se ha llamado "métodos de atribución" que denota al conjunto de todas las "formas de inteligencia (electrónica y humana), junto con la información electrónica e información sobre las capacidades y los medios de producción del *malware*, y sobre la intención hostil [H]. Por tanto es mucho más probable, incluso si sigue siendo más incierto de lo que nos gustaría, identificar positivamente al agente hostil"[46] Pero existen tres dimensiones que hacen de esta tarea un reto formidable: a) distinción, b) la extensión, y c) tiempo.

a) Distinción: Sin lugar a duda hay Estados que utilizan los ciberataques como una herramienta de proyección del poder nacional, con lo cual una defensa activa es más fácil de justificar[47].

42 Cfr. David Danks Y Joseph H. Danks, Op. cit., p. 20.
43 David Ormrod et al., Op. cit., p. 289.
44 Randall R. Dipert, "Other-than..., p. 38.
45 David Danks Y Joseph H. Danks, Op. cit., p. 20.
46 Randall R. Dipert, "Other-than..., p. 38.
47 Una nación ciberhostil es "aquella que ha exhibido un patrón de ciber ataques o ciber espionaje extenso" Randall R. Dipert, "Other-than..., p. 48. Idealmente podría separarse estas dos formas de hostilidad.

Pero también muchos civiles con conocimientos especializados están motivados o patrocinados para atacar con ciberarmas. ¿Su condición de civiles los exime de responsabilidad? Éste es un asunto de complejo encuadre legal, si se atienden a las reglas ordinarias de la jurisdicción, al hecho de que no hubo intrusión al territorio o al espacio aéreo nacionales por personas (soldados) u objetos (aviones, tanques) y al hecho de que no existe consenso sobre lo que podría significar un "estado de ciberguerra".

Pero existen criterios que con autoridad pueden guiar la reflexión en este punto. Por ejemplo, interferir electrónicamente una red militar de computadoras o trasmitir inteligencia táctica de un blanco útil para un ataque específico, entre otros muchos ejemplos, implica para el Comité Internacional de la Cruz Roja que los civiles que así actúan "asumen una función de combate continua, en oposición a únicamente participar en hostilidades de forma espontánea, esporádica y desorganizada"[48]

b) Extensión: Por definición, el ciberespacio se estructura en un conjunto de redes donde los nodos son computadores de diferente capacidad, de propiedad pública o privada, y ubicadas prácticamente en cualquier punto del planeta. Como parte de las maniobras para ocultar su identidad los perpetradores usan esas redes para "distribuir el ataque". Un Estado que se defienda activamente de ese ataque podría causar daño intencional a propiedad pública o privada en puntos de la red geográficamente lejanos y de personas u organizaciones inocentes.

En un ciberataque, los recursos de una tercera nación frecuentemente están involucrados, sin ser atacante o atacado, ya que son los puntos de 'articulación' de ataque. "Empero, un análisis minucioso de las circunstancias de esos ciberrecursos de la tercera nación probablemente muestren que esas naciones han sido negligentes

48 Committee of the Red Cross, "Direct Participation in Hostilities: Questions and Answers", consultado el 10 de Agosto de 2018, disponible en: http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm

en 'supervisar' sus ISP's [proveedores de servicio de internet] y sus sistemas de usuarios, especialmente cuando esos medios de ciberataque son bien conocidos, como lo son ahora; de forma que ahora son usados para atacar a una tercera nación."[49]

Un Estado está obligado a proteger a sus ciudadanos, pero también a los ciudadanos de otras naciones, de las amenazas que se originan en su territorio. Hay quien opina que si no pueden hacerlo por falta de pericia o recursos deben acudir a la cooperación técnica internacional, pero si la rechaza "…pierde su derecho a la no intervención…"[50]

Pero esto ya ocurre a las espaldas de los gobiernos. La tecnología opera precisamente sobre la seguridad que otorga contar con datos distribuidos y consolidados alrededor del mundo.

c) Tiempo: Los ciberconflictos (ataque–defensa–contraataque) se resuelven "en segundos o incluso más rápido."[51] En todo caso, más allá de la reacción humana, lo que sugiere el uso combinado de "respuestas automatizadas" y de otra naturaleza, como generación de inteligencia mediante fuentes humanas, por ejemplo.

El punto es que el uso responsable y ético de respuestas automatizadas debería sustentarse en "políticas de la forma 'Si el evento E sucede en el contexto C, entonces ejecuta la respuesta R' (donde E, C y R pueden ser, todas, altamente complejas), donde R se ejecuta cada vez que los gatillos –combinaciones específicas de Es y Cs– ocurren son la necesidad, o quizás incluso la posibilidad, de ninguna intervención humana"[52]

Caracterizar el dilema ético conformado por las circunstancias anteriores clarificará las opciones a mano para México. Un fraseo posible es el siguiente:

Daño 1: La ciberdefensa integrada por medidas pasivas practicada por México hasta ahora lo coloca como el tercer país con mayor incidencia de

49 Randall R. Dipert, "Other-than..., p. 39.
50 Edward T. Barrett, Op. cit., p. 9.
51 David Danks Y Joseph H. Danks, Op. cit., p. 18.
52 David Danks Y Joseph H. Danks, Op. cit., p. 18.

ciberataques a nivel mundial lo que impacta negativamente a las personas, los negocios, y la infraestructura nacionales.

Daño 2: Una ciberdefensa integrada por medidas tanto pasivas como activas puede provocar "daños colaterales" domésticos y en el extranjero a personas o empresas inocentes, pero puede revertir la tendencia a la alza de la incidencia de cibertaques en México.

El problema de las consecuencias

Ante una ciberdefensa con medidas activas deben evaluarse las "reacciones en cadena". Al implementar tales medidas debe asumirse que el perpetrador opera con sus propias medidas de protección a su sistema de cómputo en anticipación a las medidas activas más obvias en inmediatas.

> "Si sus medidas son todas puramente defensivas, entonces el reto de la reacción en cadena no parecerá ser una barrera sustancial, ya que las acciones 'internas' del adversario no pareciera que fueran a desatar una respuesta ulterior para los defensores. Por supuesto, el mismo recurso que permite a los adversarios proteger sus propios sistemas también hace muy probable que algunas de esas contra respuestas automatizadas sean de naturaleza ofensiva. Los defensores incluso podrían tener conocimiento positivo... de que el adversario tiene instaladas ciber contra respuestas, y por tanto los defensores raramente sabrán algo más que 'es altamente posible una reacción en cadena'"[53]

Conviene complementar este cálculo de orden tecnológico con ponderaciones económicas, sociales y políticas. Pero implementar medidas activas automáticas siempre acarrea el peligro de caer en el "sesgo de auto proyección futura". Este consiste en que la decisión de establecer un sistema de respuestas automatizadas debe tomarse con base en predicciones condicionales, del tipo 'únicamente si se llega al hito de daño A se activan las contra medidas de clase A' "lo que demanda predecir las propias preferencias,

53 Ibid., pp. 25 y 26.

creencias y deseos futuros"[54] Ello añade una complejidad seria en un entorno en donde el orden mundial está cambiando de ejes[55] y donde los 'daños colaterales' pueden ser tan cercanos como el Hospital más próximo si es que computadoras ubicadas ahí están siendo parte de un ciberataque, sin que sus legítimos usuarios lo sepan.

El dilema ético que plantea el cálculo podría definirse de la siguiente manera:

Daño 1: La ciberdefensa integrada por medidas pasivas que practica México raramente provoca reacciones en cadena con lo cual, se evitan daños colaterales y si se provocasen, éstos se contendrían en las fronteras nacionales.

Daño 2: Una ciberdefensa integrada por medidas tanto pasivas como activas muy probablemente provoque reacciones en cadena y "daños colaterales" domésticos y en el extranjero.

7. Opciones éticas ante un ciberconflicto

Entonces ¿qué opción acota más el daño?, ¿la acumulación de ciberataques, que individualmente podrían no ser significativamente lesivos, motivan una medida activa de defensa?, si el daño causado a las activos nacionales no es físico como en la mayoría de los ciberataques actuales ¿la pérdida temporal de la funcionalidad de computadoras o sistemas, motiva una respuesta activa?, la autodefensa activa y anticipatoria ¿podría ser invocada en casos de espionaje o bombas lógicas cuando se calcula en desastrosos los daños potenciales? Las respuestas a estas preguntas son complejas. Empero existen opciones que pueden integrarse en un esquema de atención activo.

Primera. Cooperación internacional[56] en sus dos vertientes, preventiva para desarrollar infraestructura y

54 Ibid., p. 23.

55 Ya se vislumbra un orden asiático "Con la evolución de la tecnología moderna, las mayores potencias de Asia se han armado con arsenales militares muchísimo más destructivos que los que poseía el Estado europeo decimonónico más poderoso, con los consiguientes riesgos de error de cálculo" Henry Kissinger, Orden Mundial, 1ª. Reimp. Debate, 2017, p. 217.

56 Cfr. Charles J. Dunlap Jr., Op. cit., p. 27.

capacidades de ciberdefensa pasiva y activa para auxiliar diligentemente en la contención de un ataque en curso, de sus consecuencias, y en la ubicación geográfica de los nodos de las redes utilizadas para tal fin. Debe reconocerse que no están dadas las condiciones materiales para que la cooperación se cristalice en un acuerdo de control o prohibición del uso de ciberarmas, partiendo del hecho de que "Cualquier computadora es potencialmente una ciberarma y cualquiera con un conocimiento avanzado de sistemas de información es un potencial cibercombatiente."[57] Esta clase de entendimientos podrían fijar el grado de daño colateral que resulta tolerable en la eventualidad de que una de las partes se vea obligada a responder con un contrataque simple o automatizado, así como la naturaleza y extensión de las compensaciones que podrían exigirse para reparar el daño colateral.

Segunda. Ciberdefensa pasiva en los ámbitos públicos y privados guiados por una política pública que sea actualizada de forma frecuente. Ello se expresaría en forma de una mayor eficiencia en "la disuasión basada en negación en futuros intentos podría ser la única respuesta legítima"[58] Impulsar esa política con todos los instrumentos gubernamentales, desde la persuasión (comunicación social) hasta la coerción (supervisión y multa, pérdida de la concesión, etc.)

Tercera. Inteligencia especializada generada de forma autónoma o dentro de un esquema de cooperación bilateral, caso por caso, con la finalidad de entender la lógica y motivación del perpetrador, sus capacidades reales, su grado de cuidado en la preparación del ciberataque, de intentar reconstruir la red utilizada y ubicar físicamente el origen del ataque pasado como preparación de ataques futuros y en última instancia, su identidad.[59] Un buen lugar para empezar son los centros de desarrollo de *software* ya que,

> "Los conflictos futuros muy probablemente dependan fuertemente del para obtener una ventaja en rapidez

57 Randall R. Dipert, The Ethics..., p. 385.
58 Edward T. Barrett, Warfare in a New Domain: The Ethics of Military Cyber-Operations, Journal of Military Ethics, Vol. 12, No. 1, 2013, p. 8.
59 Cfr. Ibid.

> y capacidad de ingestar grandes cantidades de datos para reducir el umbral de detección e identificar vulnerabilidades del adversario"[60]

Cuarta. Tecnología de autenticación avanzada cuyas mejoras incluyan biometrías y encripción para construir redes más confiables. Así lo reconoció el Grupo de los 20 (G20) en la declaración "Forjar un Mundo Interconectado" producto de su reunión sostenida en Hamburgo, Alemania, entre el 7 y el 8 de julio de 2017. Los veinte mandatarios argumentaron:

> "Confiar en las tecnologías digitales requiere una efectiva protección del consumidor, los derechos de propiedad intelectual, la transparencia, y la seguridad en el uso de TIC's. Apoyamos el libre flujo de información al tiempo de respetar los marcos legales atinentes a la privacidad, la protección de datos y los derechos de propiedad intelectual… Estamos comprometidos en ayudar a otorgar seguridad al entorno de las TIC's cuyos beneficios gozan todos los sectores y reafirmamos la importancia de atender colectivamente los temas del uso seguro de TIC's." [61]

Estas declaraciones políticas deberán respaldarse con presupuestos y entendimientos bilaterales. Mientras tanto, el *US National Intelligence Council* pronostica

> "requerirá establecer límites y estándares claros sobre la propiedad de datos, la privacidad y protección de datos, flujos transfronterizos de datos y ciberseguridad que podrían convertirse en puntos importantes de conflictos de políticas públicas domésticas e internacionales"[62]

La fuerza de los hechos y la intensidad de los ciberataques terminarán por mover la voluntad de las élites políticas y económicas, pero quizá no en la arena multilateral sino bilateral. Es muy alta la posibilidad de que los sistemas operativos más usados del mundo contengan "puertas

60 David Ormrod et al., Op. cit., p. 283.
61 Consultado el 29 de Agosto de 2018, disponible en http://www.consilium.europa.eu/media/23955/g20-hamburg-leaders_-communiqué.pdf
62 Christopher Castelli, Op. cit.

traseras" útiles para que el gobierno de EEUU o las mismas empresas desarrolladoras tengan acceso a que cualquier aplicación corra dicho sistema operativo. Ello motivó que Microsoft y el gobierno de la República Popular de China firmaran en 2003 un acuerdo que garantiza a éste último acceso al código fuente de Windows. Ello ya había sucedido con la OTAN, de Rusia, y del Reino Unido. Linux, con su sistema operativo de 'fuente abierta' quiere que miles de programadores alrededor del mundo aprovechen su acceso al código fuente y sugieran mejoras para acotar las vulnerabilidades que detecten. La motivación de Microsoft parecería más de orden político-comercial ya que,

> "En programas tan grandes como esos, es sin embargo intrínsecamente difícil entender el propósito o la debilidad explotable de cada línea o sección de código"[63]

China ya solicitó a las compañías que operan en su territorio "que mantengan los datos y aplicaciones de software dentro de las fronteras geográficas donde opera el negocio" para mantener control sobre los flujos transfronterizos de datos. Ello probablemente reducirá la eficiencia de las redes y tendrá algún efecto en la economía global. "La balcanización del internet cambiará la forma en que las compañías hacen negocios."[64] Esta cuasi regulación ad hoc tendrá también un impacto en contexto estratégico ya que podría constituirse internet para poderosos, para potencias emergentes y para pobres, lo que modificará la incidencia de ciberataques, registrada hasta ahora.

Quinta. Defensa activa dentro de un marco ético desde un abordaje consecuencialista, considerando al menos las tres dimensiones mencionadas líneas arriba: distinción, extensión y tiempo. Para lograr este último punto es necesario planeación de las respuestas, que en esencia son ciberataques automatizados.[65]

63 Randall R. Dipert, The Ethics..., p. 387.
64 Christopher Castelli, Op. cit.
65 David Danks Y Joseph H. Danks, Op.cit., p. 19.

El argumento básico para justificar éticamente una medida activa[66] de ciberdefensa es que el perpetrador ataque algún elemento de la infraestructura crítica nacional, precisamente por la extensión del daño que implicaría para esa sociedad la merma, inhabilitación o destrucción de algún componente de esa infraestructura. Pero ello implica otro dilema ético. Desafortunadamente ello implica que necesariamente,

> "Quedará una gran mayoría de sistemas y computadoras sin proteger, debido al costo. Y a través de estas computadoras y sistemas de información menos protegidos, como los orientados a finanzas, secretarías de Estado, y operaciones de contratación, probablemente podría fluir suficiente información para permitir a un enemigo sofisticado ensamblar las piezas e inferir información más sensible"[67]

Otro ingrediente de este cálculo estratégico es la "probabilidad de éxito" lo cual se facilita si se cuenta con inteligencia de algún tipo, sobre los métodos de ataque o los perpetradores frecuentes, aun si su identidad verdadera se ignora. Todos caen en patrones que a la larga dejan una 'firma' y terminan por ser predecibles.

Con todo ello se deberá imaginar y definir diferentes escenarios de ciberataque, en un ejercicio de prospectiva a nivel profesional y sofisticado. En cada uno de ellos se deberán fijar diferentes hitos de daño de manera que se programe la liberación de una clase de respuestas automáticas específicas cada vez que se llegue a un hito de daño o merma. Ello mantendrá proporcionalidad entre ataque y respuesta acotar el daño colateral causado e, idealmente, anunciarlo a otras naciones con las que se mantengan relaciones de cooperación bilateral en este campo. Por cierto, este último párrafo contiene los elementos esenciales de la misión de un Cibercomando, como el que reclama México.

66 Es decir, 'acciones deliberadas para alterar, desordenar, engañar, degradar o destruir sistemas o redes de cómputo o la información y/o programas residentes en o que están siendo trasmitidos en esos sistemas o redes' David Danks Y Joseph H. Danks, Op. cit., p. 25

67 Randall R. Dipert, "Other-than..., p. 45.

Conclusiones

Habiendo argumentado lo anterior, se arriba a los siguientes puntos:

a) Está éticamente justificado avanzar hacia una ciberdefensa integrada por medidas pasivas y activas.
b) Hacer de la ciberdefensa activa la misión institucional del Centro de Operaciones del Ciberespacio ya previsto. Apoyarlo con recursos humanos, financieros y materiales suficientes para hacerlo plenamente operativo en un lustro o menos.
c) Asumir como sociedad y como Estado que la ciberdefensa activa implica el desarrollo y uso de ciberarmas y que implica reinterpretar los alcances de los principios de política exterior consagrados en la fracción X del artículo 89 de la Constitución Política de los Estados Unidos Mexicanos.
d) Los protocolos de uso de las ciberarmas deben considerar al menos, los siguientes elementos inspirados en la ética consecuencialista:
   - La medida activa es una opción únicamente si se ataca algún componente de la infraestructura crítica nacional,
   - Para ser efectiva la medida activa puede ser automática, pero su uso será reactivo, nunca proactivo,
   - La medida activa automática es una opción siempre que su uso cause un 'daño colateral' menor al que provocaría el ciberataque,
   - El Estado mexicano debe asumir que toda medida activa provocará 'daño colateral' doméstico o en el extranjero que debe compensarse,
   - El uso de la medida activa debe ser graduado respecto de hitos de daño, definidos como parte integral de escenarios de riesgo concebidos con antelación,
e) La ciberdefensa que practique Mexico debe ser pública en sus líneas generales y debe poner énfasis en las medidas pasivas ya en uso y otras como:
   - Explorar esquemas de cooperación bilateral con países aliados,
   - Generar inteligencia especializada,
   - Invertir en tecnología de autenticación avanzada propia, lo que tendría un impacto favorable

al incluir a la sociedad civil en este esfuerzo nacional.

BIBLIOGRAFÍA

Adda, Jacques, *La Globalización de la Economía*, Editorial Sequitur, Madrid, 1999.

Bailey, Christopher E., "The Intelligence Comunity ethos: a closely regulated profession", International Journal of Intelligence Ethics, v. 3, n. 2, Autumn–Winter, 2012, p. 54. Disponible en: http://journals.fcla.edu/ijie/article/view/83453.

Barrett, Edward T., "Warfare in a New Domain: The Ethics of Military Cyber-Operations", Journal of Military Ethics, Vol. 12, No. 1, 2013.

Benítez Manaut, Raúl y Georgina Sánchez, "Avances y Límites de la participación de México en la Seguridad Hemisférica en el Siglo XXI" en *Cooperación y conflicto en las Américas. Seguridad Hemisférica: Un largo y sinuoso camino*; María Cristina Rosas (coordinadora); UNAM – Centro de Estudios de Defensa Hemisférica; México; 2003.

Castelli, Christopher, Revitalizing privacy and trust in a data-driven world, Key findings from GSISS 2018 PWC, consultado el 21 de Agosto de 2018, disponible en https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

David Danks Y Joseph H. Danks, "The Moral Permissibility of Automated Responses During Cyberwar", Journal of Military Ethics, Vol. 12, No. 1, 2013.

Dipert, Randall R. "Other-than-Internet (OIT) Cyberwarefare: Challenges for Ethics, Law, and Policy", Journal of Military Ethics, Vol. 12, No. 1, 2013.

_____, "The Ethics of Cyberwarfare", Journal of Military Ethics, Vol. 9, No. 4, 2010, p. 390. Se refiere a M. Walzer, Just and Unjust War, 4th ed., Basic Books, New York, 2006.

Dunlap Jr., Charles J., "Some Reflections on the Intersection of Law and Ethics in Cyber War", Air & Space Power Journal, January-February 2013.

Espinosa, Edgar Iván, "Hacia una estrategia nacional de ciberseguridad en México", Revista de Administración

Pública No. 136, Volumen L, Nº 1, (enero-abril 2015), INAP, México.

Galindo Ceballos, Enrique Francisco, "La seguridad cibernética en el nuevo entorno operativo", Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México, p. 186

Kay, Sean, "Globalization, Power, and Security", Security Dialogue vol. 35, no. 1. march 2004, p. 11.

Kissinger, Henry, *Orden Mundial*, 1ª. Reimp. Debate, 2017, p. 217.

Leyva, Jeanette, "Bancos no acostumbran denunciar ciber delitos: PGR", El Financiero, 22 de agosto de 2018, p. 11.

Llorens. María Pilar, Los desafíos del uso de la fuerza en el ciberespacio, Anuario Mexicano de Derecho Internacional, vol. XVII, enero-diciembre, UNAM, 2017.

Noah, Timothy, Birth of a Washington Word, When warfare gets "kinetic", Slate, Noviembre de 2002, consultado el 5 de Agosto de 2018, disponible en:
http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html

Ormrod, David y Benjamin Turnbull, "The Cyber conceptual framework for developing a military doctrine", Defence Studies, 2016 Vol. 16, No. 3, Routledg.

Ortega, Omar, "México, la tercera nación con más ciberataques en el mundo", El Financiero, 30 de julio de 2018, p. 42. Cita al Reporte Semestral de Ciberseguridad de SonicWall. Disponible en: http://www.elfinanciero.com.mx/tech/mexico-la-tercer-nacion-con-mas-ciberataques-en-el-mundo

Pisanty, Alejandro, "Algunos rasgos del futuro de las agendas digitales nacionales: el caso de México", Revista de Administración Pública No. 140, Volumen LI, Nº 2, (mayo-agosto 2016), INAP, México.

Sinnott-Armstrong, Walter, "Consequentialism", T*he Stanford Encyclopedia of Philosophy* (Winter 2015 Edition), Edward N. Zalta (ed.), URL:
<https://plato.stanford.edu/archives/win2015/entries/consequentialism/>.

Thomas Rid y Peter McBurney, Cyber-Weapons, The RUSI Journal, Febrero de 2012, pp. 7 y 8, consultado el 10 de agosto, disponible en https://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354

Documentos oficiales

Programa Sectorial de Defensa Nacional 2013-2018, DOF. 13 de diciembre de 2013.

Programa Sectorial de Marina 2013-2018, DOF. 16 de diciembre de 2013.

Código de Ética de los servidores públicos del Gobierno Federal, las Reglas de Integridad para el ejercicio de la función pública, DOF del 20 de agosto de 2015, consultado el 10 de agosto de 2018, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5404568&fecha=20/08/2015

Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, en su versión publicada en el DOF, 2 de febrero de 2016.

Committee of the Red Cross, "Direct Participation in Hostilities: Questions and Answers", consultado el 10 de Agosto de 2018, disponible en: http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm