UNA AGENDA DE CIBERSEGURIDAD PARA LA SOCIEDAD CIVIL: ¿QUÉ HAY EN JUEGO?

Alex Comninos

INTRODUCCIÓN

La seguridad de las redes digitales y de la información que circula por dichas redes es cada vez más importante para los gobiernos, el sector privado y la sociedad civil. El ciberdelito es cada vez más sofisticado.[1] Los Estados se acusan entre sí de hackear incidentes.[2] Las organizaciones de la sociedad civil, los Estados, las corporaciones y los usuarios y usuarias de internet se ven expuestos y se vuelven víctimas de virus y malware, violación de datos, violación de la privacidad en línea y vigilancia. Los gobiernos y las corporaciones espían a los netizens (ciudadanos de la red) y las personas que se dedican a defender los derechos humanos son especialmente víctimas de tal vigilancia. El "hacktivismo" está surgiendo como forma de protesta a menudo en defensa de los derechos humanos, pero también es posible que infrinjan derechos o disparen respuestas gubernamentales que infringen esos derechos.[3] Quienes defienden los derechos humanos de las mujeres, importantes interesadas e interesados en la ciberseguridad, deben enfrentar vigilancia, vulnerabilidades de la seguridad de la información y problemas que

1. RSA 2012 Cybercrime Trends Report: The Current State of Cybercrime and What to Expect in 2012, http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf.
2. US and China accuse each other of cyber warfare, RT (Russia Today) 19 February 2019, http://rt.com/usa/cyber-china-war-unit-604/
3. James Ball "By criminalising online dissent we put democracy in peril", The Guardian 1 August 2011, guardian.co.uk/commentisfree/2011/aug/01/onlinedissent-democracy-hacking; Cory Doctorow, Pirate Bay to Anonymous: DDoS is censorship, cut it out, BoingBoing 1 May 2012, http://boingboing.net/2012/05/11/pirate-bay-to-anonymous-ddos.html, Jay Leiderman, Justice for the PayPal WikiLeaks protesters: why DDoS is free speech, The Guardian, 22 enero 2013, http://www.guardian.co.uk/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech

Alex Comninos esta candidato de doctorado, Universidad Justus-Liebig, Giessen.

APC ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

pueden atentar contra su vida. A la vez, ese grupo puede usar las TIC para denunciar y defenderse contra los abusos de derechos humanos, por lo que dichas TIC deben ser seguras.[4]

Los gobiernos utilizan la seguridad nacional como justificación para censurar, controlar o vigilar el uso de internet, y a veces para cortar la comunicación. Algunos ejércitos están creando ciberunidades y han empezado a surgir carreras armamentistas en el ciberespacio,[5] junto con el crecimiento de un "complejo ciberindustrial". El sector privado está cada vez más involucrado en el control de internet. A través de mecanismos de responsabilidad de intermediarios, las empresas de telecomunicaciones, los proveedores de servicios de internet (ISP) y otros actores del sector privado controlan hoy activamente internet."[6]

Los gobiernos, los militares, las agencias de inteligencia y el sector privado lideran el debate y la creación de políticas de ciberseguridad, pero la sociedad civil debe participar en ello en pie de igualdad. Robert Deibert ha dicho que la sociedad civil "se reconoce cada vez como un actor importante en la gobernanza del ciberespacio" y que es necesario desarrollar una estrategia de ciberseguridad "que resuelva los peligros reales que abundan en gobiernos y corporaciones, que enfrente en forma directa las inquietudes nacionales sin dejar de proteger y preservar la apertura de las redes de información y comunicación."[7]

Este trabajo introduce algunas cuestiones conceptuales importantes en relación a la ciberseguridad, analiza algunos de los principales peligros y brinda sugerencias en cuanto a la postura que debería adoptar la sociedad civil.

EL CONCEPTO DE CIBERSEGURIDAD

Definición

La ciberseguridad se refiere a la seguridad de la información digital almacenada en redes electrónicas, al igual que la seguridad de las redes que almacenan y transmiten información. Sin embargo, no existe demasiado consenso en cuanto a su definición exacta. *Ciberseguridad* se usa a veces en forma intercambiable con *seguridad de la información* – "protección de la información y los sistemas de información para evitar el acceso, uso, revelación, modificación, o destrucción no autorizados con el fin de mantener su confidencialidad, integridad y disponibilidad."[8] La seguridad de la información y la ciberseguridad se refieren, en general, a lo mismo. Sin embargo, seguridad de la información es lo que usan las organizaciones y los y las profesionales de TI, mientras que ciberseguridad es lo que se utiliza más en debates políticos, o cuando se habla de cuestiones de seguridad de la información como parte de la seguridad nacional.

La Unión Internacional de Telecomunicaciones (UIT) define ciberseguridad como:

> "la recopilación de herramientas, políticas, conceptos de seguridad, salvaguardas, lineamientos, posturas sobre manejo de riesgos, acciones, capacitación, buenas prácticas, garantías y tecnologías que se pueden usar para proteger el ciberambiente y la organización y los recursos del/a usuario/a[9] ... La ciberseguridad apunta a garantizar el logro y mantenimiento de la seguridad de la propiedad de la organización y los recursos del/a usuario/a contra los peligros de seguridad relevantes en el ciberambiente. Los objetivos generales de

4. Danna Ingleton, Let's stop our fear of tech leading to misuse of security legislation, en Crossing borders : cyberspace and national security, GenderIT, 25 de octubre 2012, http://www.genderit.org/node/3684.
5. Ron Deibert, Towards a cyber security strategy for civil society, en Alan Finlay (ed.) *Global Information Society Watch 2011: Internet rights and democratization*, APC & HIVOS, http://www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society
6. Ibid.
7. Ibid.
8. Integridad "significa proteger contra la modificación o destrucción impropia de información, e incluye la garantía de no repudio y autenticidad de la información"; confidencialidad "significa preservar las restricciones autorizadas en relación al acceso y la revelación, incluyendo medios para proteger la privacidad personal y la información propietaria" y disponibilidad "quiere decir garantizar un acceso en tiempo y forma, además de confiable , a la información y a usarla". Richard Kissel, *Glossary of Key Information Security Terms*, Instituto Nacional de Ciencia y Tecnología, Departamento de Comercio de Estados Unidos, febrero 2011, p 93. http://books.google.com/books?id=k5H3NsBXIsMC
9. "Los recursos de la organización y los/as usuarios/as incluyen: dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información trasmitida y/o almacenada en el ciberambiente."

seguridad incluyen: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio [y] confidencialidad."[10]

ASUNTOS A CONSIDERAR

Esta definición es algo más amplia que la de seguridad de la información. Además de proteger solamente los sistemas de información, también protege "el ciberambiente" (expresión bastante vaga) y "los recursos de los/as usuarios/as". Se refiere no solo a *asegurar los sistemas de información*, sino también al *uso de los sistemas de información para asegurar los recursos*.

Entonces, *cuán amplio debería ser el concepto de ciberseguridad? Qué problemas habría que incorporar, y cuáles no?* Un informe de la OECD[11] informa a los Estados que la ciberseguridad "ha llegado a significar un enorme espectro de cosas.Y esto lleva no sólo a la instauración de poderes que son demasiado amplios en su alcance y aplicación, sino que también existe el riesgo de instaurar un consenso ilusorio."12 El hecho de incluir demasiados temas podría hacer que el concepto perdiera coherencia. Cuánto más amplio sea el concepto de ciberseguridad, más temas se incluyen en la agenda de los ejércitos y las agencias de inteligencia de los Estados. Hay muchos asuntos que, si bien dependen del uso seguro de las tecnologías de la información y la comunicación (TIC) y de internet, no se abordan mejor desde la seguridad nacional, ni desde el marco de la seguridad de la información, el Estado o la visión militar. No siempre es útil analizar algo como tema de ciberseguridad, aunque obviamente tenga dimensiones de seguridad de la información.

Asegurar

Cuando se habla de algunas cosas como cuestiones de seguridad, se les da un tono de urgencia e importancia. Hablar de algo como un problema de seguridad suele implicar que se trata de una amenaza para el modo de vida de la sociedad, y justificar la adopción de medidas extraordinarias o de emergencia para frenar el peligro. Cuando los asuntos se transforman, en el discurso, en cuestiones de seguridad nacional, hablamos de "asegurar". Asegurar implica "designar un peligro existencial que requiere una acción de emergencia, o medidas especiales, y que un público significativo acepte esa delegación específica."[12] Cuando se aseguran con éxito, se convierten en asuntos de seguridad nacional y cambia la manera de tratarlos "más allá de las reglas de juego establecidas". El problema se enmarca "ya sea como un tipo especial de política o como algo que va más allá de la política".[13] Para tener éxito al asegurar algo, hay que contar con tres componentes: presentar el tema como un peligro o una amenaza, acción urgente para enfrentar el peligro y efectos sobre las relaciones con los actores cambiando el modo en que normalmente se trata dicho tema.[14]

Asegurar el ciberespacio es un factor importante que incide sobre el ecosistema global de comunicaciones. Los problemas relativos a la seguridad de la información, internet, la gobernanza de internet y otras áreas se aseguran y se transforman en cuestiones de seguridad nacional cuando se miran a través del lente de la ciberseguridad. Esto incide en forma negativa sobre las estructuras existentes de gobernanza y los mecanismos de toma de decisiones sobre esos temas. Cuando se asegura un asunto, no necesariamente mejora o aumenta el rol y la voz de la sociedad civil como actor en la gobernanza de esa área. Cuando se apela a acciones extraordinarias o de emergencia, hay que garantizar que dichas medidas no tengan consecuencias negativas sobre la apertura y la seguridad de internet, y que no afecten negativamente los derechos humanos.

Una perspectiva histórica: ampliar y profundizar el concepto de seguridad

La historia del concepto de seguridad contiene algunas lecciones que se pueden aplicar a la ciberseguridad. Durante las tres últimas décadas, el concepto de seguridad se ha ampliado, al igual que la agenda de seguridad estatal, para incluir muchos sectores y problemas. En el contexto de *détente* (distención) y con el fin de la Guerra fría, empezaron los debates académicos y políticos entre los "ampliadores", que argumentaban a favor de ampliar la definición y la agenda de seguridad más allá de la seguridad de los Estados y los temas estratégicos de la guerra fría, y los "reductores", que proponían mantener una definición y una agenda reducidas de seguridad, centrándose en cuestiones

10. Unión Internacional de Telecomunicaciones, Sector de Normalización de las Telecomunicaciones, Revisión de la ciberseguridad, Recomendación ITU-T X.1205 (04/2008), http://www.itu.int/ITU-T/recommendations/rec.aspx?id=9136 Adoptada por Resolución 181 de la UIT, Guadalajara, 2010 (http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf)

11. Organización para la cooperación económica y el desarrollo.

12. Barry Buzan, Ole Waever, & Jaap de Wilde, 1998. *Security: a new framework for analysis*. Lynne Rienner: Boulder, Colorado, p. 27.

13. Ibid, p. 24.

14. Ibid.

militares y de seguridad nacional. Desde el final de la guerra fría, los gobiernos, los ejércitos, la academia y la sociedad civil han participado en la ampliación del concepto de seguridad para incluir otros sectores que no se relacionaban tradicionalmente con la seguridad del Estado, por ejemplo, seguridad cultural, económica, ambiental, climática y alimentaria. A la vez, el concepto se ha "profundizado" a fin de incluir a los humanos como objeto central de la seguridad, en lugar de los Estados o los ejércitos.

El concepto de seguridad post guerra fría es "muy amplio... aún contiene el problema de ser muy amplio", es "aún más abstracto que antes" y todavía "está en manos del Estado", de modo que se puede usar contra las personas.[15] Ahora, con una definición más amplia de seguridad, los gobiernos tienen más excusas para desarrollar el aparato coercitivo del Estado, o para implementar medidas extraordinarias – como la vigilancia y regulación de cada vez más asuntos. Muchos temas con los que debería lidiar la sociedad civil se trasladaron a las agendas de seguridad nacional de los Estados, dándole a éstos más poder para intervenir.

El concepto de ciberseguridad también está ahora en proceso de profundización y ampliación. Antes, la ciberseguridad y la seguridad de la información eran conceptos técnicos, que se conversaban sobre todo entre especialistas, profesionales de TI, corporaciones, Estados, ejércitos y agencias de inteligencia y seguridad. Los conceptos ahora son cada vez más importantes para todos nosotros y nosotras y se han ampliado para incluir más cosas que las que antes inquietaban a la comunidad técnica, el sector comercial y el Estado. Esto ofrece más oportunidades de intervención para nuevos actores. Pero, junto con este proceso, se está ampliando la agenda de la ciberseguridad. Este hecho puede llevar a que otras áreas problemáticas, como la gobernanza de internet, la gobernanza global, la gobernanza nacional, la legislación y la regulación pasen a la agenda de ciberseguridad y, por esta vía, a las agendas de seguridad nacional de los Estados. El resultado final puede ser que estos temas salgan de las estructuras actuales de gobernanza, con enfoques multisectoriales. En consecuencia, la sociedad civil podría quedar al margen de la discusión. Como sociedad civil, debemos asegurarnos de poder conducir la ampliación del concepto de ciberseguridad sin ser marginados.

Cuando se habla de ciberseguridad, lo que está en juego es la voz y el poder de la sociedad civil como actor interesado.

Este trabajo no pretende brindar un análisis completo de todos los peligros relevantes de ciberseguridad. El objetivo del mismo es más bien alentar una reflexión crítica sobre ciberseguridad y plantear algunas cuestiones a fin de ayudar a la sociedad civil a desarrollar estrategias de ciberseguridad. A continuación se tratan algunos temas importantes en relación a la ciberseguridad, para luego formular recomendaciones.

Tecnodiscurso y propagación del miedo

La ciberseguridad puede ser bastante compleja para los netizens sin conocimiento técnico. Esto puede llevar a muchas personas, incluyendo a los medios, los y las responsables de la formulación de políticas y actores del gobierno, el sector comercial y la sociedad civil a tomar los informes al pie de la letra. Es fácil mal interpretar, malentender, representar e informar mal sobre los asuntos de ciberseguridad. Dado el relativo anonimato de internet, resulta difícil atribuir responsabilidades o causalidades en caso de ciberataques o ciberincidentes. En este ambiente, los debates políticos multiplican denuncias sin fundamento a toda velocidad.

Muchos relatos equívocos sobre incidentes de ciberseguridad se repiten una y otra vez, aunque suelen carecer de fundamentos más profundas que la mera especulación. El presidente de Estados Unidos Barack Obama, por ejemplo, dijo: "Sabemos que unos ciberintrusos violaron nuestra red de energía eléctrica y que en otros países los ciberataques han sumergido a ciudades enteras en la oscuridad"[16] – pero no mencionó qué países eran. Los medios de prensa estadounidenses se apropiaron de esa historia, en el conocido programa de televisión *60 Minutes*, aunque su discurso fue que "varias fuentes de inteligencia muy importantes confirmaron que hubo una serie de ciberataques en Brasil" en 2005 y 2007.[17] Estas declaraciones se siguen repitiendo en los medios sin ningún fundamento. Un cable de Wikileaks y una declaración del regulador de electricidad de Brasil indican que los apagones no fueron

15. Ver "A Conversation with Annette Seegers" y se puede consultar una explicación más larga en Annette Seegers, "The New Security in a Democratic South Africa", presentación en The Robert Strauss Center for International Security and Law", 1 de noviembre 2010, http://blip.tv/robert-strauss-center/the-new-security-in-democratic-south-africa-4362239. En base a este trabajo, Seegers, Annette (2010) 'The new security in democratic South Africa: a cautionary tale', Conflict, Security & Development, 10: 2, 263 — 285.

16. Cyberwar: Sabotaging the System, CBS News, 15 de junio 2010, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml see the 60 Minutes segment at https://www.youtube.com/watch?v=IPHHd8YW9EA (parte 1) y https://www.youtube.com/watch?v=dU2XPFoyAR8 (parte 2).

17. Ibid.

resultado de ciberataques, sino que fueron causados por "polución en la cadena de aislantes causada por depósitos de hollín".[18]

Militarización del ciberespacio y carrera ciberarmamentista

La ciberseguridad aparece cada vez más en la agenda de seguridad de los Estados. En todo el mundo, los Estados han empezado a establecer "cibercomandos" o ciberunidades dentro de sus ejércitos. El Ciber Comando de Estados Unidos tiene "capacidad operativa" desde mayo de 2010. El "cibercomando" se están volviendo una idea atractiva para otros países. La Secretaría de defensa de Reino Unido propuso integrar un ciber comando que dependa del Ministerio de Defensa. El Ministerio de Defensa de India piensa establecer una "Autoridad de ciber control y comando". China creó un "Ejército azul" para defender al Ejército de liberación popular de los ataques a sus redes.[19] Irán también tiene planes de armar un cibercomando para las fuerzas armadas de los países.[20] Se utilizan ciberunidades para frenar el disenso en línea. En marzo de 2011, en una reunión del partido de gobierno de Sudán, se anunció que los "ciber jihadistas" iban a "aplastar" a los disidentes que se manifestaran en línea pidiendo un cambio de gobierno.[21] También se despliegan ciberunidades en conflictos. En Siria, por ejemplo, quienes apoyan al gobierno crearon el "Ejército electrónico de Siria" que se usa para vigilar activistas y a los miembros del Ejército libre de Siria.[22] "Otros adoptan medios menos convencionales, como brindar apoyo tácito a grupos propatrióticos para realizar ciberataques ofensivos en defensa del Estado, como parece el caso en Irán, Siria, Rusia, Birmania y China."[23],

Los Estados asignan cada vez más recursos a la seguridad de la información, así como a la guerra de la información. En 2011, cuando Estados Unidos enfrentaba una crisis presupuestal, el Pentágono solicitó 3.200 millones de dólares para asignarlos a la ciberseguridad —cifra semejante al gasto militar total de ese año en Marruecos o Argentina.[24] Es probable que aumentar el gasto militar para ciberconflictos sea un desperdicio de recursos, que no necesariamente resuelve los problemas de ciberseguridad.

Internet está cada vez más militarizada. Los virus, que antes eran instrumento de ciberdelincuentes y de algún bromista profesional, son desarrollados ahora activamente por los militares y las agencias de inteligencia. El virus Stuxnet, responsable de sabotear los centrifugadores involucrados en el programa de enriquecimiento de uranio de Irán, fue probablemente el primer malware diseñado específicamente para infectar equipos industriales que se propagó en forma masiva. Stuxnet fue probablemente diseñado y propagado con apoyo de las agencias estatales de inteligencia y seguridad (se supone que de Estados Unidos e Israel).[25] Cofer Black, ex-Director del Centro Antiterrorismo de la CIA (y director de una subsidiaria del mayor contratista privado de seguridad del Departamento de Estado de Estados Unidos) anunció durante Black Hat 2011, una conferencia sobre seguridad de la información, que Stuxnet marcó el "Rubicón de nuestro futuro."[26] Ya sea que esto represente un momento histórico o no (o la admisión implícita de la participación de una agencia estadounidense en Stuxnet), lo que muestra es que el complejo de la industria militar aceptó tácitamente el malware como herramienta a ser usada por los Estados en futuros conflictos de información.

Desde que apareció Stuxnet hubo denuncias de la aparición de otro virus, llamado Flame, que se propagó por varios países de Medio Oriente y Africa del norte utilizando el código de Stuxnet. Además de ese nuevo virus, el código fuente de Stuxnet se consigue ahora en internet, lo que habilita a una multitud de actores a adaptar el código a sus propósitos.

El Ministerio de Defensa de Japón encargó a Fujitsu el desarrollo de "virus defensivos" por 2,3 millones de dólares que sean "capaces de identificar la fuente de

18. Marcello Soares, Brazilian Blackout Traced to Sooty Insulators, Not Hackers, *Wired Magazine*, 11 de noviembre 2009, http://www.wired.com/threatlevel/2009/11/brazil_blackout/. Brian Krebs, Cable: No Cyber Attack in Brazilian '09 Blackout, Krebs on Security, 3 de diciembre 2010, http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout/

19. Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", Peace Magazine 27(4), octubre 2011, http://peacemagazine.org/archive/v27n4p16.htm

20. Iran to launch first cyber command, Press TV, 15 de junio 2011, http://presstv.com/detail/184774.html

21. Sudan's NCP says its "cyber-Jihadists" ready to "crush" online oppositionists, Sudan Tribune, 22 de marzo 2011, http://www.sudantribune.com/Sudan-s-NCP-says-its-cyber,38372

22. "What is the Syrian Electronic Army?", Mashable, 12 de agosto 2012, http://mashable.com/2012/08/10/syrian-electronic-army/

23. Deibert, op. cit.

24. Alex Comninos, "Anonymous: Information Conflict and New Challenges to Peace Practitioners", op. cit.

25. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", Wired, 11 de julio 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/

26. Tabassum Zakaria, "Former CIA official sees terrorism-cyber parallels", Reuters, 3 de agosto 2011, http://www.reuters.com/article/2011/08/03/us-usa-security-cyber-idUSTRE7727AJ20110803; and Glenn Chapman, "Cold War gives way to Code War: CIA veteran", Agencia France Press, 4 de agosto 2011, http://www.google.com/hostednews/afp/article/ALeqM5h-_86Ftav0uDHvMYDzydPgVWjNzQ?docId=CNG.0dcc70d787af82f2b283aeb2af9d940e.e01

un ciberataque con gran precisión, luego replicarse de computador en computador, limpiando virus a través de la red". Sin embargo, según un experto en seguridad, el virus "podría tener consecuencias imprevistas, como ser difícil de controlar". Un "buen" virus "fuera de control" podría propagarse al azar o de forma inesperada, y sería difícil de frenar.[27] El virus, fuera de Japón, podría también violar la soberanía de otros países, extendiendo posiblemente el conflicto.

El complejo industrial de la ciberseguridad

> *"En los consejos de gobierno, debemos cuidarnos de adquirir influencias sin garantía, ya sean buscadas o no, del complejo industrial militar. La posibilidad de que se produzca una desastrosa escalada de poder fuera de lugar existe y persistirá.*
>
> *Jamás deberíamos permitir que el peso de esa combinación ponga en peligro nuestras libertados o procesos democráticos. No debemos dar nada por sentado. Sólo una alerta y una ciudadanía informada pueden promover el engranaje adecuado de la enorme maquinaria industrial y militar con nuestros métodos y metas pacíficas, para que puedan prosperar juntas la seguridad y la libertad."*
>
> - DWIGHT D. EISENHOWER, Presidente de Estados Unidos de América, discurso de despedida ante el Congreso Nacional, 1961[28]

Otra amenaza importante en relación a la ciberseguridad es el surgimiento de un complejo ciberindustrial. Los ejércitos modernos desarrollaron redes comerciales con proveedores de equipos de defensa y contratistas de servicios de defesa. El personal de las empresas de defensa suelen ser ex funcionarios de gobierno y existe una "puerta giratoria" entre ambos. Ambos tienen un interés particular en el aumento de los presupuestos de defensa y, para justificar esos presupuestos, tienen que presentarle peligros a la ciudadanía, a los parlamentos y a los gobiernos. El complejo industrial militar siempre busca nuevas amenazas para justificar nuevos gastos y el surgimiento de "ciberpeligros" brinda esa oportunidad. El complejo ciberindustrial no solo está desarrollando ciberarmas ofensivas y defensivas, sino que también está desarrollando cada vez más equipos de vigilancia. Tanto que ha surgido una nueva industra que "hace desaparecer secretamente los datos y los guarda para siempre en servidores finales con capacidad para almacenar muchos petabytes (millones de gigabytes) de información". Esta nueva industria "ofrece nuevas herramientas para buscar datos y reconstruir nuestro pasado, e incluso nuestros movimientos en tiempo real a través de los teléfonos móviles, de forma que bien podrían volver y perseguirnos".[29]

CIBERSEGURIDAD Y CENSURA

La ciberseguridad se puede usar para introducir y legitimar modos de censura y normalizarla. En Rusia, por ejemplo, un "Registro único" de sitios web prohibidos tiene por objetivo darle al gobierno la posibilidad de cerrar cualquier sitio web que se considere peligroso para los niños y niñas, lo que incluye pornografía infantil, información sobre drogas e información de cómo cometer un suicidio. El registro "podría llevar a censurar al azar sitios web y la libertad de expresión"[30] y "fomentar el bloqueo de todo tipo de discurso político en línea". Además "gracias a la propagación de las nuevas tecnologías de monitoreo de internet, el Registro podría convertirse en un arma para espiar a millones de rusos y rusas."[31]

El rol de las agencias de inteligencia

En lo que se trata de ciberseguridad, surge un conflicto de intereses fundamental. Las agencias de inteligencia pueden preferir asegurar sus propias infraestructuras,

27. Gerry Smith, Fujitsu Cyberweapon Developed In Japan: 'Good' Virus Created For Cyber Defense, Huff Post Tech 04 enero 2012, http://www.huffingtonpost.com/2012/01/04/fujitsu-cyberweapon-japan_n_1183462.html. Ver también Graham Cluley, Why Japan's search-and-destroy cyber weapon could be a very bad idea, Naked Security, 12 de enero 2012, http://nakedsecurity.sophos.com/2012/01/03/japan-cyber-weapon-bad/

28. Texto en: http://coursesa.matrix.msu.edu/~hst306/documents/indust.html, video en: http://www.youtube.com/watch?v=8y06NSBBRtY

29. Pratap Chatterjee, The new cyber-industrial complex spying on us, The Guardian, 2 de diciembre de 2011, http://www.guardian.co.uk/commentisfree/cifamerica/2011/dec/02/cyber-industrial-complex-spying

30. Bryan Bishop, Internet censorship bill passes upper house of Russian Parliament, The Verge, 18 de julio 2012, http://www.theverge.com/2012/7/18/3168011/internet-censorship-bill-passes-upper-house-russian-parliament.

31. Andrei Soldatov & Irina Borogan, The Kremlin's New Internet Surveillance Plan Goes Live Today, *Wired*, 1 de noviembre 2012. http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

pero si desean vigilar a otros/as, no necesariamente quieren que tengan infraestructuras seguras de información. Los canales seguros y privados de comunicación ofrecen muchas menos oportunidades de reunión y vigilancia de inteligencia que las infraestructuras inseguras. Esto significa que debemos ser escépticos cuando las agencias de inteligencia se involucran en ciberseguridad y es necesario garantizar que sus operaciones estén sujetas a supervisión civil y parlamentaria. La sociedad civil y los/as legisladores/as tienen que proteger especialmente este asunto.

Ciberseguridad y vigilancia

El objetivo de la ciberseguridad debería ser proteger a los netizens de la vigilancia. Sin embargo, las iniciativas de ciberseguridad pueden darle más poder a las empresas y los gobiernos para espiar a los usuarios y usuarias. Por ejemplo, la Ley de ciberseguridad propuesta en 2012 en Estados Unidos pretendía "otorgar nuevas potestades a las empresas para espiar a los usuarios/as, compartir información con el gobierno y pedir amplia inmunidad legal para sus acciones."[32] La segunda enmienda de la Ley de Intercambio y Protección de Ciberinteligencia que ahora está siendo considerada por la Cámara de Representantes de Estados Unidos prevé una excepción de "ciberseguridad" que anula las leyes existentes de privacidad. En nombre de la ciberseguridad, las empresas recibirían inmunidad total por compartir información con las agencias del gobierno, incluso la comunicación privada de usuarios y usuarias. Las corporaciones tendrían potestad completa para reunir y compartir "información de ciberseguridad", incluyendo información personal, y la única limitación sería que la información se reúna con "objetivos de ciberseguridad."[33]

La amenaza de las redes sociales

El crecimiento del complejo ciberindustrial, junto con el crecimiento de nuestra presencia en línea en las redes sociales y los medios sociales ha llevado a un importante aumento de la capacidad de vigilancia por parte de las agencias de inteligencia. Por ejemplo, en 2009, la Agencia Central de Inteligencia de Estados Unidos invirtió en una empresa que se especializa en monitoreo de medios sociales. La empresa, llamada Visible, "navela por alrededor de medio millón de sitios de la web 2.0 por día, escarbando por más de un millón de envíos y conversaciones que ocurren en blogs, foros en línea, Flickr, YouTube, Twitter y Amazon".[34]

Las redes sociales pueden dejar a la sociedad civil expuesta a vigilancia, además de habilitar la manipulación. Las empresas de ciberseguridad desarrollaron software que crean personas falsas en las redes sociales con fines de vigilancia, así como para manipular conversaciones en línea y parecerse a movimientos de base, práctica conocida como "astroturfing". Por ejemplo, en 2010, la Fuerza Aérea de Estados Unidos hizo un llamado a propuestas para el desarrollo de software de astroturfing – o programa de "manejo de personas" – que permitiría controlar a personas falsas en plataformas de medios sociales.[35]

El software de astroturfing se puede usar tanto para vigilar, como para difundir propaganda, que se presenta como si procediera genuinamente de la sociedad civil. Esto representa un grave peligro para la seguridad de la información (la seguridad de la información en este contexto consiste en proteger la "confidencialidad, la integridad y la disponibilidad" de la información y la comunicación). El periodista George Monbiot comentó que "[el] software de este tipo tiene potencial para destruir internet como foro para el debate constructivo. Hace que la democracia en línea sea una farsa."[36]

32. Mark M. Jaycox, The Cybersecurity Act was a surveillance bill in disguise, *The Guardian*, 2 de agosto 2012.

33. Mark M. Jaycox, CISPA, the Privacy-Invading Cybersecurity Spying Bill, is Back in Congress, Electronic Frontier Foundation, 13 de febrero 2013, https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cybersecurity-spying-bill-back-congress.

34. Noah Schachtman, U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets, *Wired Magazine*, 19 de octubre de 2009, http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/

35. John Hudson, The Embarrassing Revelations of Cyber Security Firm HBGary Federal, The Atlantic Wire, 24 de febrero 2011, http://www.theatlanticwire.com/technology/2011/02/the-embarrassing-revelations-of-cyber-security-firm-hbgary-federal/20977; Happy Rockefeller, The HB Gary Email That Should Concern Us All, The Daily Kos, 16 de febrero 2011. http://www.dailykos.com/story/2011/02/16/945768/-UPDATED-The-HB-Gary-Email-That-Should-Concern-Us-All, El llamado original a propuestas de "Software de manejo de personas" (número de solicitud: RTB220610, 22 de junio de 2010) fue para un "Servicio de manejo de persona en línea. 50 licencias de usuario/a, 10 personas por usuario/a." El "software admitirá 10 personas por usuario/a, completo con contexto, historia, detalles de apoyo y ciberpresencias que sean técnica, cultural y geográficamente coherentes. Las aplicaciones individuales habilitarán a un/a operador/a a ejercer cierto número de personas diferentes en línea desde la misma estación de trabajo y sin temor a ser descubierto/a por adversarios/as sofisticados/as. Tiene que parecer que las personas se originan en casi cualquier parte del mundo y que pueden interactura a través de servicios en línea y plataformas de medios sociales convencionales. El servicio incluye un ambiente de aplicación amigable para el/la usuario/a a fin de maximizar la conciencia de situación del/a usuario/a exhibiendo información local en tiempo real." Publicado por primera vez en FedBizOpps.gov, archivado en: http://www.seankerrigan.com/docs/PersonaManagementSoftware.pdf

36. Ibid.

Seguridad de software: *día-cero* y *día-para-siempre*

Los artículos sobre ciberseguridad suelen ser bastante atractivos (o aterradores). Pero el verdadero desafío que enfrenta la ciberseguridad no tiene que ver con el terrorismo internacional, el espionaje promovido por los Estados, o los hackers en esteroides. El problema radica en el código fuente del software que usamos todos los días, ya sea del sistema operativo que se usa, las aplicaciones de nuestros dispositivos informáticos, o los navegadores web y los add-ons que los hacen funcionar (por ejemplo, Flash y Java), y el software utilizado para construir los sitios web que pueblan internet. El verdadero problema de ciberseguridad radica en la *seguridad de software*. En general se entiende que internet (el protocolo TCP/IP) y la web no fueron diseñados para ser seguros. Originalmente, internet era una red académica de pares confiables. El problema de la confianza y la seguridad no tenía importancia en ese momento y no se tuvo en cuenta. Si bien ha habido avances en cuanto a asegurar las infraestructuras (el desarrollo de Extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSEC)[37] y el protocolo HTTPS[38] por ejemplo), en general se acepta que no se puede volver a diseñar internet para la seguridad y que ese nuevo diseño plantearía desafíos para su interoperatividad. Por encima de la capa de las infraestructuras abiertas de internet existe la capa de aplicación. Se trata de las aplicaciones que existen a nivel local en nuestras máquinas, en el software que facilita el acceso a la web y los servicios de internet, como los navegadores de la web, los mensajes instantáneos y los clientes de VoIP (como Skype, por ejemplo), además del software que guía los servicios en línea y los sitios web donde almacenamos nuestros datos. Es en esta capa donde se puede diseñar e instalar seguridad, y allí es donde existe la mayor inseguridad. También es en esta capa donde se pueden implementar con mayor facilidad soluciones que garanticen la seguridad de la información.

La pericia en la solución de los errores de seguridad en el código va en aumento, pero no sigue el ritmo de incremento de errores. En comparación con lo que sucedía hace 15 años, todos los sistemas operativos populares y contemporáneos de los computadores de mesa (Windows, Linux y Mac) ofrecen actualizaciones automáticas de seguridad para los "bichos" de seguridad que luego son "emparchados" por las actualizaciones. Si bien se encuentran más errores en el código, más virus que antes, somos cada vez más eficientes para encontrarlos. A la vez, producimos cada vez más códigos (informáticos y aplicaciones en línea), así que el número neto de bichos/errores y, por ende, las vulnerabilidades de seguridad de nuestro código van en aumento, lo que produce más errores de software que antes.[39]

Un error de seguridad (también conocido como vulnerabilidad) es, esencialmente, un fragmento de código de software que no tiene en cuenta la seguridad y que, por ende, puede ser explotado por las personas para obtener acceso a datos a los que no deberían acceder en circunstancias normales. Cuando se descubre un bicho/error, un hacker malicioso puede hacer un exploit a fin de poner en peligro una serie de datos o el acceso a un computador. El malware – virus y caballos troyanos – es una serie de exploits que se aprovechan de esos errores. Existen dos tipos importantes de errores de software que son muy relevantes para la ciberseguridad y ocuparse de ellos puede ser la manera más eficiente de asegurar el ciberespacio: son los de cero-día (*zero-day*) y los de día-para-siempre (*forever-day*).

Los bichos/vulnerabilidades de cero-día que se descubrieron eran desconocidos para los desarrolladores originales de software. Los proveedores originales de software no pueden arreglar el software porque quizá no conocen su existencia, o porque no han tenido tiempo para hacerlo. Tuvieron "cero días" para resolver el error. Un ataque de cero-día es cuando se aprovecha la vulnerabilidad de cero día. Son especialmente peligrosos porque la mayoría de las personas, más allá de los/as investigadores/as en seguridad, o de aquellos/as que tienen malas intenciones, conocen la vulnerabilidad y no se pueden proteger de esos ataques. Los ataques más graves de ciberseguridad proceden de bichos de cero-día y exploits de cero-día. Lo correcto cuando se encuentra un cero-día es notificar al desarrollador original del software, para que encuentre una solución al error o, en otra etapa, hay que informar a los usuarios/as del software afectado, así como también habría que avisar a otros actores interesados y al público en general. "Al igual que la mayoría de las tecnologías, los exploits tienen un uso dual. Se pueden usar como parte de los esfuerzos de investigación para

37. DNSSEC es un conjunto de especificaciones de la Fuerza de tareas de ingeniería de internet que agregan extensiones al servicio de DNS, que agrega la autenticación del origen de los datos y la integridad de los datos del Sistema de Nombres de Dominio. Sin embargo, no brinda confidencialidad. (Ver Arends, et al., Request For Comment 4033, DNS Security Introduction and Requirements, marzo de 2005. Fuerza de tareas de ingeniería de internet, http://tools.ietf.org/html/rfc4033; Ver también RFCs 4034 y 4035, además de http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions para acceder a una buena explicación.

38. El Protocolo seguro de transferencia de hipertexto (HTTPS) le adiciona seguridad al Protocolo de transferencia de hipertexto (HTTP) agregando una encriptación bidireccional entre el/la usuario/a y el sitio web (http://en.wikipedia.org/wiki/HTTP_Secure).

39. Gary McGraw, Cyber War, Cyber Peace, Stones, and Glass Houses, charla en el Institute for Security, Technology, and Society (ISTS), Dartmouth College, 26 de abril 2012, http://www.ists.dartmouth.edu/events/abstract-mcgraw.html, http://www.youtube.com/watch?v=LCULzMa7iqs

ayudar a fortalecer los computadores contra intrusiones. Pero también se pueden utilizar como armas y desplegarse agresivamente para todo, desde espionaje gubernamental y corporativo, hasta fraude liso y llano".[40] Un artículo publicado recientemente en *Forbes* destaca el creciente mercado gris y desregulado de cero-días. "Algunas empresas legítimas operan en una zona gris legal dentro del mercado de cero-días, vendiéndole exploits a los gobiernos y las agencias que vigilan el cumplimiento de la ley del mundo entero... Pero como la venta no está regulada, crece la inquietud porque algunas empresas del mercado gris proveen a gobiernos extranjeros no muy legítimos que podrían usar los exploits como parte de una serie de ataques maliciosos dirigidos contra otros países u opositores. También existe un mercado negro anárquico … donde los exploits se venden a una variedad de actores con fines a menudo delictivos" y "se teme que el floreciente negocio de encontrar y vender exploits esté creciendo y escapando al control, lo que lleva a que se exijan nuevas leyes para regular ese tipo de comercio turbio."[41] Es importante considerar la regulación en lo que se refiere al cero-día. Hay que alentar a las empresas de software a encontrar y resolver los cero-días en su propio software, e incentivar a los investigadores/as en seguridad a encontrar también los cero-días y notificar a las empresas, al igual que a otros actores interesados.[42]

Un problema grave para la ciberseguridad del/a usuario/a promedio, así como para las infraestructuras principales que se conectan a internet, son los "días-para-siempre", "días-infinitos" o "i-días". Se trata de "errores de programación que nunca se arreglan o demoran mucho en arreglarse —incluso cuando la empresa que desarrolló el software los reconoce". Estos errores pueden afectar a usuarios/as cotidianos de la red y también a las infraestructuras nucleares, como sistemas de control industrial, que se usan a menudo para controlar infraestructuras tales como redes eléctricas. Los sistemas de control industrial requieren grandes inversiones en equipos que se supone que duren años. A diferencia del ciclo comercial del desarrollo de software, los operadores de los sistemas de control industrial suelen carecer de fondos para actualizar sus sistemas regularmente. Hay vulnerabilidades bien documentadas ("días para siempre") en los controladores de Siemens que hicieron que el virus Stuxnet infectara los reactores nucleares Natanz en Irán. Estos controladores también operan una vasta gama de maquinaria para diferentes aplicaciones en el mundo entero "que se usa en instalaciones nucleares y otras infraestructuras claves, así como en plantas de fábricas comerciales que hacen de todo, desde productos farmacéuticos, hasta automóviles".[43]

UN ENFOQUE DESDE LA SOCIEDAD CIVIL

Cómo debería ser la agenda y la estrategia de ciberseguridad de la sociedad civil?

La sociedad civil no es una entidad homogénea, sino que se compone de una variedad de culturas, responde a un amplio abanico de asuntos e incluye un vasto muestrario de opiniones divergentes en cuanto a cómo resolver diferentes problemas. En algunas áreas convergen los intereses de la sociedad civil global, mientras en otras existe una gran divergencia. Sin embargo, la sociedad civil se ve enfrentada a desafíos de ciberseguridad que son comunes a todos los grupos.

Si bien la sociedad civil en general tiene interés en que internet sea un espacio abierto, que promueva la libertad de expresión y de acceso a la información, la seguridad de la comunicación también es de su interés. La confianza en la seguridad y la privacidad de las infraestructuras de comunicación permite llevar adelante sus asuntos sin inquietarse por robo de dinero o de información, o por vigilancia electrónica.

A veces, las medidas para garantizar la seguridad, la apertura y la privacidad pueden ser contradictorias entre sí. Es esencial que las iniciativas de ciberseguridad protejan la posibilidad de usar internet para ejercer los derechos de libertad de expresión y de asociación. El objetivo de la seguridad de las redes tampoco debería exponer a los individuos a una vigilancia indebida e ilegal, y debe respetar su derecho a la privacidad. La sociedad civil debe tener una postura respecto de la ciberseguridad que sea equilibrada en relación a todos esos derechos diferentes.

40. Ryan Gallagher, Cyberwar's gray market, Slate 16 de enero 2013, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html Ver también, Andy Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees), Forbes, 21 de marzo 2012, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

41. Ryan Gallagher, Cyberwar's gray market, op. cit.

42. Hay una propuesta de dicha regulación que se destaca en Sandro Gaycken & Felix FX Lindner, Zero-Day Governance: an (inexpensive) solution to the cybersecurity problem, Trabajo presentado en Cyber Dialogue 2012: What is stewardship in cyberspace?, marzo 2012, http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf

43. Kim Zetter, Serious security holes found in Siemens control systems targeted by Stuxnet, Ars Technica 4 de agosto 2011, http://arstechnica.com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/

Una perspectiva de la ciberseguridad como parte de los derechos humanos debería incluir en la agenda no sólo la seguridad de los Estados y los gobiernos, sino también la seguridad de las redes comerciales, las redes de la sociedad civil y las organizaciones. La seguridad de los usuarios y usuarias individuales (netizens) también debe ser fundamental.

La sociedad civil debe decidir cuidadosamente si incorporar estos problemas en las agendas de ciberseguridad nacional, y saber si así se resuelven mejor o no tales cuestiones. También tiene que analizar los costos y beneficios del hecho de asegurar algunas cosas. Ese tipo de cosas garantiza la importancia del estatuto de la seguridad nacional? Se resuelven mejor en un marco de seguridad nacional o de seguridad de la información? Se encuentran actualmente en otras estructuras de gobierno? Existen mecanismos o iniciativas que no sean en internet y que ya se estén ocupando de esos problemas? La sociedad civil tiene que pensar muy bien cuándo habría que establecer normas de seguridad y cuándo no. El aumento de la seguridad aumenta o margina el papel ya existente de la sociedad civil? Algunas cuestiones pueden requerir seguridad, otras quizá haya que conversarlas e incorporarlas a la agenda de ciberseguridad pero no necesariamente asegurarlas, y otras aún es posible que haya que desasegurarlas.

Es necesario ahondar en el diálogo multisectorial sobre estrategias nacionales de ciberseguridad. La sociedad civil debe participar activamente y exigir una participación multisectorial en la formulación de políticas y acuerdos nacionales, regionales e internacionales de ciberseguridad. La sociedad civil, las comunidades académica y técnica, los usuarios y usuarias de internet y los creadores y creadoras de contenidos (netizens), el sector privado, el sector empresarial, los ejércitos y las agencias de inteligencia, todos deben estar presentes en el diálogo. El diálogo multisectorial sobre ciberseguridad se debe promover desde los foros multisectoriales existentes, como el FGI.

Es necesario ocuparse de la gobernanza de la ciberseguridad de una manera que no implique suplantar otros problemas de la gobernanza de internet. Los mecanismos existentes para la elaboración de políticas de gobernanza de internet a nivel nacional e internacional no deberían sustituirse por nuevos sistemas de elaboración de políticas enfocados exclusivamente en la ciberseguridad.

Las políticas de ciberseguridad deberían profundizar la seguridad de los defensores y defensoras de los derechos de las mujeres y garantizar que las estrategias de seguridad nacional frenan la violencia hacia las mujeres, tanto en línea como en la realidad.[44] Los defensores y defensoras de los derechos de las mujeres también necesitan capacitación en herramientas tecnológicas que sirvan para proteger su seguridad operativa y física – como herramientas de encriptación y anonimato.

Por último, la sociedad civil debe exigir que el diálogo sobre ciberseguridad se base en hechos probados. Dado el problema de atribución en ciberseguridad, resulta fácil tomar decisiones políticas sobre hechos incorrectos. Hay que exigirle a los y las responsables de la elaboración de políticas que sus denuncias de incidentes y amenazas a la ciberseguridad se basen en pruebas.

44. Ver también Danna Ingleton, "Let's stop our fear of tech leading to misuse of security legislation" GenderIT, 25 de octubre 2012, http://www.genderit.org

APC ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

UNA AGENDA DE CIBERSEGURIDAD PARA LA SOCIEDAD CIVIL QUÉ HAY EN JUEGO?

APC es una red internacional de organizaciones de la sociedad civil fundada en 1990 que empodera y asiste a gente que trabaja por la paz, los derechos humanos, el desarrollo y la protección del medio ambiente, a través del uso estratégico de las tecnologías de información y comunicación (TIC).

APC trabaja para construir un mundo en donde todas las personas tengan un acceso fácil, equitativo y accesible al potencial creativo de las tecnologías de información y comunicación para mejorar sus vidas y crear sociedades más igualitarias y democráticas.

www.apc.org info@apc.org

Encomendado por la Asociación para el Progreso de las Comunicaciones (APC)

Realizado con apoyo de la Agencia Sueca de Cooperación Internacional para el Desarrollo (Sida).

¡CONECTA TUS DERECHOS!

UNA AGENDA DE CIBERSEGURIDAD
PARA LA SOCIEDAD CIVIL. QUÉ HAY EN JUEGO?

Abril 2013

APC-201304-CIPP-R-ES-DIGITAL-184

ISBN: 978-92-95096-93-6

Diseño gráfico: MONOCROMO