ARI

ARI 41/2013

11 de noviembre de 2013

Real Instituto Elcano

La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU

THIBER

Tema[1]

La *National Security Agency* (NSA) de EEUU ha adquirido gran notoriedad tras conocerse sus actividades de espionaje a través del caso Snowden y las escuchas a líderes aliados. Menos conocida es la colaboración público-privada que hace posible esas actividades.

Resumen

La *National Security Agency* (NSA) de EEUU ha adquirido gran notoriedad tras conocerse sus actividades de espionaje a través del caso Snowden y las escuchas a líderes aliados. Pero para que la NSA pueda desarrollar sus funciones precisa de la colaboración privada. La evolución tecnológica al servicio del espionaje en EEUU precisa contar con un amplio entramado de industrias, universidades y redes de apoyo si pretende vigilar a todo lo que pueda afectar a los intereses de seguridad y a todos los que puedan hacerlo. Gracias a esa red de apoyo, la NSA ostenta una amplia superioridad tecnológica con sus competidores y puede condicionar la colaboración con los aliados pero, como se ha visto en el caso Snowden, también corre el riesgo de que se produzcan filtraciones por la red. Este ARI describe la evolución de las actividades de la NSA y el diseño de su red de apoyo industrial y universitaria.

Análisis

Introducción

La **NSA** sigue ocupando titulares en los medios de comunicación desde que se reveló el aparente espionaje masivo realizado sobre las comunicaciones telefónicas y cibernéticas de los países europeos, asiáticos, africanos y americanos a raíz del **caso Snowden**, fundamentado éste en la filtración por parte de **Edward Snowden** de más de 20.000 documentos sensibles o clasificados sustraídos de los servidores de la NSA.

---

1 THIBER (*the cybersecurity think tank*) es una iniciativa englobada en el Instituto de Ciencias Forenses y de la seguridad de la Universidad Autónoma de Madrid. Autores**:** Enrique Fojón Chamorro, ingeniero superior en Informática, enrique.fojon[arroba]inv.uam.es; Guillem Colom Piella, doctor en Seguridad Internacional, guillem.colom[arroba]inv.uam.es; y Adolfo Hernández Lorente, ingeniero superior en Informática, adolfo.hernandez[arroba]inv.uam.es.

La historia reciente de la NSA –o al menos la que se conoce– ha estado marcada por sonados escándalos, fracasos o filtraciones, entre los que destacan la escucha de las comunicaciones de personalidades contrarias a la **Guerra de Vietnam** o promotoras de los derechos civiles en la década de 1960, los incidentes de los buques espía USS Liberty en la costa israelí en la **Guerra de los Seis Días (1967)** y el USS Pueblo en las costas norcoreanas poco antes de iniciarse la ofensiva del Tet (1968), la imposibilidad de localizar a los responsables de los **atentados del 11-S** a pesar de que algunos de ellos residían de forma permanente en EEUU y la mayoría de ellos vivieron en Laurel –a pocos kilómetros de la sede central de la agencia en Fort Meade (Maryland)–, la imposibilidad de proporcionar a George W. Bush evidencias suficientes sobre la existencia o desarrollo de armamento de destrucción masiva en Irak, o la actual filtración realizada por Edward Snowden.

Los orígenes de la NSA se remontan a los primeros años de la Guerra Fría, cuando en 1952 el presidente Harry S. Truman creó una organización de inteligencia criptológica que, integrada en el recién constituido Departamento de Defensa, sustituyera a la efímera Agencia de Seguridad de las Fuerzas Armadas (1949-1952) en materia de monitorización, procesamiento y análisis de comunicaciones telefónicas y electrónicas de terceros países y protección de las redes propias y aliadas. Durante la Guerra Fría, esta agencia no sólo llegó a tener casi 80.000 puestos de trabajo y controlar casi todas las comunicaciones electrónicas procedentes del bloque Oriental, sino que en su seno se creó en la década de 1970 el controvertido programa ECHELON de vigilancia tecnológica, supuestamente capaz de monitorizar las comunicaciones telefónicas, de fax y de tráfico de datos de todo el globo.

Según refleja la Figura 1, la NSA ha desarrollado múltiples programas de espionaje para adaptar sus capacidades a la evolución tecnológica y a los requerimientos estratégicos. En este sentido, fue a raíz de los sucesos del 11-S cuando, amparada en la **Guerra contra el Terror y la nueva legislación antiterrorista**, puso en marcha numerosos programas de vigilancia tecnológica capaces de monitorizar de forma exhaustiva el tráfico de Internet, las cuentas de correo electrónico, los datos multimedia, las comunicaciones telefónicas y la telefonía por Internet, siendo el más famoso de ellos el controvertido PRISM capaz de monitorizar el ciberespacio. Sin embargo, tal y como ha revelado el caso Snowden, las labores de espionaje no sólo se han limitado a al-Qaeda, sus afiliados o a los potenciales adversarios de EEUU, sino que éstas se han generalizado a otros países, organizaciones internacionales y líderes políticos de todo el globo.

Figura 1. Principales programas de vigilancia y espionaje ejecutados por la NSA

PRINCIPALES PROGRAMAS DE INTELIGENCIA DE LA NSA *

AÑO CREACIÓN	AÑO FIN	NOMBRE	FINALIDAD	AREA DE INFLUENCIA	OPERADORES
1945	1975	SHAMROCK	Interceptación masiva de mensajes telegráficos	EE.UU.	NSA
1962	A	ECHELON	Interceptación masiva de comunicaciones electrónicas	Todo el mundo	NSA + UKUSA
1967	1973	Minaret	Interceptación de comunicaciones electrónicas de ciudadanos bajo sospecha	EE.UU.	NSA
1978	I	**Blarney	Recolección de metadatos de llamadas telefónicas	EE.UU.	NSA
1982	A	Main Core	Recolección de información personal y financiera de ciudadanos bajo sospecha	EE.UU.	NSA, CIA, FBI
1990´s	I	Highlander	Interceptación masiva de comunicaciones vía satélite -INMARSAT	Oriente medio	NSA
1990´s	1990´s	Thinthread	Interceptación masiva de datos de internet	EE.UU.	NSA
2000	I	Mainway	Recolección de metadatos de llamadas telefónicas	EE.UU.	NSA
2000	A	Bullrun	Inclusión de vulnerabilidades en hardware y sotware de determinados objetivos	Todo el mundo	NSA
ATENTADOS TERRORISTAS DEL 11 DE SEPTIEMBRE DE 2001					
2001	A	Terrorist Surveillance Program	Intereceptación masiva de datos de sospechosos de actividades terroristas	Todo el mundo	NSA + UKUSA
2002	2007	Trailblazer	Interceptación masiva de datos de internet	EE.UU.	NSA
2002	I	Pinwale	Recolección de correos electrónicos	Todo el mundo	NSA
2002	A	RAGTIME	Interceptación masiva de datos de sospechosos de actividades terroristas en EE.UU	Todo el mundo	NSA
2003	I	FairView	Recolección de metadatos de llamadas telefónicas, correos electrónicos y actividad internet ciudadanos de todo el mundo	Todo el mundo	NSA
2003	I	NIMD	Interceptación masiva de datos multimedia	EE.UU.	NSA
2004	A	Boundless Informant	Recolección de metadatos de llamadas telefónicas	Todo el mundo	NSA
2005	2007	Turbulence	Interceptación masiva de datos de internet	Todo el mundo	NSA
2007	A	PRISM	Recolección de información de los principaes proveedores de servicios	EE.UU.	NSA
2007	A	X-Keyscore	Intereceptación masiva de datos de internet	Todo el mundo	NSA + UKUSA
2007	I	Dropmire	Espionaje de las comunicaciones de embajadas y organizaciones internacionales	EE.UU.	NSA
2009	A	Mastering de Internet	Recolección de metadatos de llamadas telefónicas, correos electrónicos y actividad en internet ciudadanos de todo el mundo	Todo el mundo	UKUSA

* - Su conocimiento es público
** - Programa que fue agrupado bajo FAIRVIEW
A - Sigue activo
I - Se desconoce su estado
UKUSA - Alianza formada por EEUU, Canada, Reino Unido, Nueva Zelanda y Australia

THIBER

Fuente: elaboración de THIBER.

Para poder llevar a cabo esta ingente labor, la NSA –que desde 2009 comparte jefatura con el mando militar del ciberespacio (*US Cyber Command*, USCYBERCOM) que, dependiente del mando estratégico estadounidense, se encarga de realizar operaciones en este nuevo dominio– dispone de una amplia gama de herramientas tecnológicas de última generación que le permiten mantener una superioridad permanente respecto al resto de Estados, tanto aliados como potenciales adversarios. Para ello, en la actualidad la NSA cuenta con una plantilla cercana a los 40.000 empleados, un presupuesto reconocido de 10.800 millones de dólares y cerca de 500 programas –operativos o en fase de desarrollo– destinados a la vigilancia y el espionaje tecnológicos.

La transformación de la NSA

Siendo importante lo anterior, **conviene conocer que tras ese esfuerzo público existe una movilización de recursos y talento privado en apoyo a las tareas de vigilancia de la NSA** que explica su capacidad actual. Desde los sucesos del 11 de septiembre de 2001, la comunidad de inteligencia estadounidense –y en especial la NSA– ha tenido que satisfacer una fuerte demanda de información susceptible de emplearse para la seguridad y defensa del país. Para ello, la NSA ha redefinido y optimizado los procesos que regulan sus relaciones con universidades y empresas con el fin de implementar una "gestión del cambio" ágil, flexible y acorde a sus necesidades operativas, reduciendo así la burocracia interna y mejorando la eficacia de esta agencia que –desde los tiempos del general Ralph Canine como primer director de

la NSA hasta la actualidad, con el general Keith Alexander al mando– ha demostrado una enorme rigidez que ha condicionado su día a día y menoscabado muchas de sus capacidades. No obstante, esta relación también ha aumentado la vulnerabilidad de la NSA a las filtraciones debido a la multiplicación de subcontrataciones público-privadas que se ve obligada a realizar.

Tras el 11-S, el general Michael Hayden, director de la NSA entre 2000 y 2005, persuadió al entorno del presidente George W. Bush sobre la necesidad de llevar a cabo una revolución tecnológica y operativa en el seno de la agencia. Para ello se valió del apoyo del vice-presidente Dick Cheney y del asesor legal de éste, David Addington, que culminó con la firma de una orden presidencial que permitía a la NSA sortear la Ley de Vigilancia de la Inteligencia Extranjera (***Foreign Intelligence Surveillance Act*, FISA**), una norma aprobada por la Administración Carter en 1978 para evitar el empleo de recursos federales en la investigación sin orden judicial a ciudadanos estadounidenses dentro del territorio nacional.

A partir de 2001, la NSA ha ampliado sus instalaciones a lo largo y ancho del país y en la actualidad dispone de cuatro grandes centros de escuchas en EEUU: Oahu, Hawai; Grovetown, Georgia; Sugar Grove, West Virginia; y Yakima en Washington que, según algunas fuentes, podría haberse cerrado a principios de 2013. Además, dispone de dos grandes centros de procesamiento de datos: uno en Buckley, Colorado, y otro recién inaugurado en Camp Williams, Utah, así como de un centro criptológico en San Antonio, Texas. Todas estas instalaciones están conectadas con la sede central en Fort Meade y constituyen lo que la jerga especializada se denomina el "pulpo" (la NSA *surveillance octopus*) que recoge el mapa en la Figura 2.

Figura 2. Principales instalaciones de la NSA en territorio estadounidense

Fuente: elaboración de THIBER.

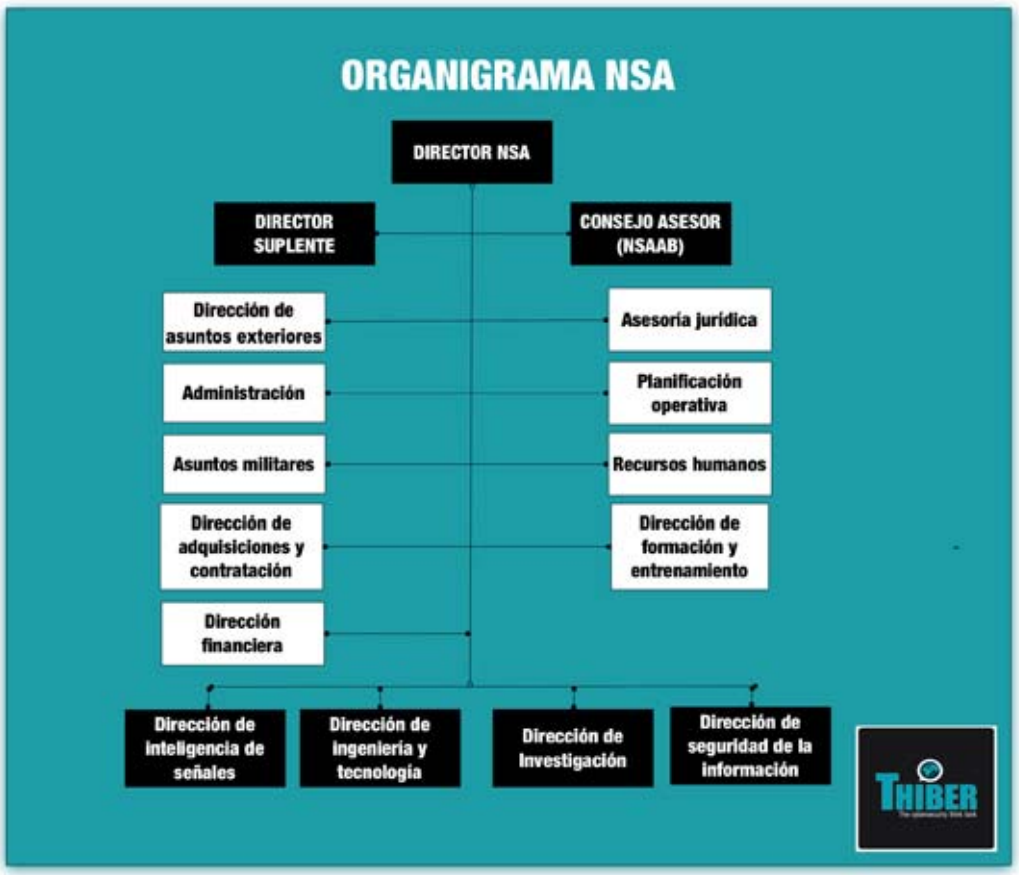
De forma similar al resto de las agencias de inteligencia del país, **la actividad de la NSA no sería posible sin una estrecha relación con la comunidad universitaria y las principales empresas de los sectores de las telecomunicaciones, Internet y defensa del país**. Esta relación a tres bandas no ha permanecido estable en el tiempo sino que ha evolucionado siguiendo las dinámicas vinculadas con el desarrollo tecnológico. Así, mientras la comunidad universitaria acaparó el grueso de los proyectos y presupuesto de la agencia para I+D+i entre las décadas de 1950 a 1970, a finales de los años 70 –coincidiendo con la Revolución de la Información– ésta fue dejando paso a los gigantes de las telecomunicaciones y defensa, que mantuvieron su hegemonía como principales contratistas de la NSA hasta los primeros años del nuevo milenio, cuando la industria de Internet –altamente especializada y cuyo elemento central de su actividad es la gestión de los datos– empezó a participar en los programas de I+D+i de la NSA. No obstante, la relación existente entre ambos actores es menos sólida que con la industria tradicional, puesto que muchas de estas empresas de Internet son de reciente creación y no han nacido en el seno de la comunidad universitaria ni bajo el paraguas de la comunidad de inteligencia o de defensa, por lo que la confianza y la capacidad de control directo o indirecto de la NSA sobre estos contratistas es también menor.

En el ámbito de la NSA, la participación público-privada se articula a través de los siguientes cuatro componentes: el Consejo Asesor (*NSA Advisory Board*), el Parque Tecnológico Nacional (*National Business Park*), la Alianza de Inteligencia y Seguridad Nacional (*Intelligence and National Security Alliance*, INSA) y la comunidad universitaria.

En primer lugar, el Consejo Asesor tiene sus orígenes en el Consejo Científico (*National Security Agency Scientific Advisory Board*, NSASAB) creado en 1953 para asesorar al director de la NSA sobre las líneas de investigación y desarrollo que debía adoptar la agencia para la obtención de capacidades en función de sus necesidades operativas aplicando en todo momento los últimos avances tecnológicos, en especial aquellos relacionados con el cifrado.[2]

2 En la actualidad, el Consejo Asesor del director de la NSA se denomina *NSA Emerging Technologies Panel*, aunque dentro de la propia Agencia se siguen refiriendo a él como *NSA Advisory Board* (NSAAB).

Figura 3. Organigrama de primer nivel de la Agencia Nacional de Seguridad (NSA)



El Consejo, cuya existencia y funciones han permanecido en secreto hasta hace una década, ha contado siempre con científicos e ingenieros de reconocido prestigio, así como directivos de las principales empresas tecnológicas del país. Entre otros, el matemático John von Neumann y el vicepresidente de IBM John McPherson, formaron parte del primer NSASAB. Otros ilustres miembros del órgano asesor fueron Alf L. Andersen, fundador de los laboratorios Bell, y David Aucsmith, jefe de seguridad de Microsoft e Intel. El Consejo asesora sobre todas las actividades de la NSA, desde la priorización de las multimillonarias inversiones a la contratación de personal destinadas a las **cuatro áreas operativas de la agencia: inteligencia de señales, ingeniería, investigación y seguridad de los sistemas de información**.

Los principales contratistas de la NSA, definidas como aquellas empresas que trabajan en programas clasificados como alto secreto, poseen sus oficinas centrales o principales en las inmediaciones de Fort Meade, en un área conocida como el *National Business Park*, un parque empresarial de poco más de 100 hectáreas situado en Annapolis Junction que ha ido creciendo hacia el vecino condado de Howard a medida que han crecido las necesidades de la Agencia. La NSA dispone de un conjunto de programas relacionados con las empresas que van desde la identificación de compañías con tecnología acordes con las necesidades operativas de la Agencia hasta programas de apoyo a la internacionalización de las pymes. A través de estos programas, la NSA ha creado un exhaustivo censo de empresas nacionales con capacidades tecnológicas de

primer nivel y susceptibles de colaborar con la agencia en la prestación de servicios y el desarrollo de proyectos. En la actualidad un total de 260 empresas con acreditación para trabajar en programas clasificados como secretos –un 13% del total de 2.000 empresas que disponen de esa acreditación– tiene oficinas en el Parque. Entre éstas destacan gigantes de la industria de defensa estadounidense como **Booz Allen Hamilton**, **L-3 Communications**, **CSC**, **Northrop Grumman**, **General Dynamics** y **SAIC**. Muchas de estas empresas son contratistas principales de otras agencias de inteligencia estadounidense, del Pentágono o de organismos internacionales como la OTAN, lo que proporciona valor añadido a sus actividades. Además del NBP, la NSA dispone de una docena de parques empresariales similares, entre los que destacan los situados en Dulles-Chantilly (Virginia), Denver-Aurora (Colorado) y Tampa (Florida).

La Alianza ha reemplazado, a partir de noviembre de 2005, a la Asociación de Apoyo a los Asuntos de Seguridad (*Security Affairs Support Association*, SASA) creada en 1979 para facilitar la cooperación, el intercambio de información y el fomento de la innovación dentro la comunidad de inteligencia estadounidense. Desde su sede en Arlington, la **INSA influye en la comunidad de inteligencia distribuyendo fondos y copando puestos de dirección relevantes**. Los miembros de INSA, incluidos todos los contratistas principales de los programas secretos de la NSA, son receptores de casi la totalidad del presupuesto de la comunidad de inteligencia destinado al I+D+i, que se estima en 40.000 millones de dólares durante 2013. Es una pieza clave del sistema nacional de inteligencia estadounidense en la que participan las principales empresas de los sectores de las telecomunicaciones, Internet y defensa del país, así como algunas de las principales universidades nacionales.

El actual director general de INSA es John Negroponte, que a lo largo de su carrera ha ejercido como embajador de EEUU ante las Naciones Unidas (2001-2004), embajador en Irak (2004-2005), primer director de Inteligencia Nacional (2005-2007) y subsecretario de Defensa (2007-2009). Otros ilustres directores generales han sido el actual director de la CIA, John Brennan, los ex-directores de la NSA John Michael McConnell (1992-1996) y Kenneth A. Minihan (1996-1999) y la ex consejera del Departamento de Seguridad Interior entre 2004 y 2007, Frances Townsend. En la actualidad, algunas de las empresas que están representadas en el consejo de gobierno de INSA son BAE Systems, Boeing, BoozAllenHamilton, CSC, HP, IBM, Microsoft, Northrop Grumman, Lockheed Martin, QinetiQ y Raytheon, mientras que son muy pocas las industrias de Internet que tienen representación en este selecto foro.

Finalmente, la **NSA y sus empresas contratistas se nutren mayoritariamente de talentos procedentes de las universidades estadounidenses**, la mayoría de las cuales integradas en la red nacional de centros de excelencia, una organización formal promovida por la NSA y el DHS para fomentar la excelencia formativa en matemática, física, criptografía, computación y ciberseguridad. Además, la NSA realiza procesos de reclutamiento en la totalidad de la comunidad universitaria estadounidense con el objeto de captar aquel talento no identificado a través de los programas de esta red nacional de centros de excelencia.

Del mismo modo, la NSA ha firmado convenios específicos con un conjunto de universidades para el desarrollo de determinados programas relacionados con sus actividades operativas. En 2006, en el seno de la Oficina del Director de Seguridad Nacional nació la Agencia para la Investigación de Proyectos Avanzados de Inteligencia (*Intelligence Advanced Research Projects Agency*, IARPA), una organización con vocación similar a la famosa Agencia para la Investigación de Proyectos Avanzados de Defensa (*Defense Advanced Research Projects Agency*, DARPA) cuya misión es investigar y promover el desarrollo de capacidades susceptibles de ser utilizadas por la comunidad de inteligencia estadounidense. Situada en el M-Square, un parque tecnológico perteneciente a la Universidad de Maryland y situado a escasos 35 kilómetros de la sede de la NSA, la **IARPA desarrolla su actividad alrededor de tres grandes programas: colección inteligente, análisis incisivo y operaciones seguras**. La "colección inteligente" tiene como objeto mejorar la calidad de los datos recolectados por la comunidad de inteligencia; el "análisis incisivo" pretende mejorar el análisis de los datos recolectados en tiempo real; y las "operaciones seguras" tiene como objeto contrarrestar las capacidades que hayan sido desarrolladas por los potenciales adversarios de EEUU para coartar la libertad de movimientos del país en la red. En la actualidad, **IARPA y NSA trabajan en un conjunto de programas que permitan obtener, a partir del *Big Data*, patrones deductivos sobre el comportamiento futuro de individuos o grupos**, algo muy similar al programa recreado hace más de una década por Steven Spielberg en la película *Minority Report*, una metodología de análisis con profundas implicaciones sociales, políticas y, sobre todo, económicas. Como ejemplo de la colaboración, la NSA ha firmado de un convenio con la Universidad de Carolina del Norte por 31 millones de dólares para la creación de un laboratorio que permita optimizar los procesos de inteligencia asociados al *Big Data*.

La colaboración publico-privada de la NSA tras el caso Snowden

Las revelaciones de Edward Snowden han sacado a la luz el intrincado sistema de colaboración público-privada de la NSA descrito anteriormente y fundamentado en una **relación simbiótica entre la agencia, la universidad y la industria**. A pesar del escándalo que se ha producido por la revelación de que empresas como Google, Apple, Facebook y Microsoft habían proporcionado información de sus usuarios a la NSA, de las comparecencias ante comisiones de investigación y de las declaraciones políticas de que se restringirán las acciones de espionaje, parece difícil que EEUU reforme en profundidad un sistema de colaboración público-privada que le ofrece tantos dividendos en materia de inteligencia, tecnología, conocimiento y captación y retención del talento.

No obstante, y teniendo en cuenta que **el modelo de negocio de la industria de Internet se fundamenta en la confianza que le otorga el usuario** (bien sea éste un ciudadano, una empresa o un gobierno), es probable que muchas de estas empresas se vean obligadas a redefinir su colaboración con la NSA, pero es difícil que lo hagan hasta el punto de exponerse a perder los importantes proyectos de I+D+i o los suculentos contratos que obtienen a través de su colaboración con la NSA. Tampoco

pueden exponerse a contrariar a la NSA renunciando a cooperar con ella si no quieren verse abocadas al cierre, tal y como ya ha ocurrido con los proveedores de correo seguros Lavabit y Silent Circle. Una dependencia que se acentúa en el caso de la comunidad universitaria y científica que desarrollan investigación para que la NSA pueda seguir ejecutando operaciones de inteligencia. Tampoco puede confiarse la garantía de la privacidad a los legisladores porque, como la trayectoria de la NSA demuestra, cualquier regulación restrictiva de la colaboración público-privada en materia de inteligencia puede ser puenteada por motivos de seguridad nacional, por lo que sólo cabe esperar que las filtraciones y los escándalos hayan contribuido a **crear una masa crítica de activismo y de desconfianza en la sociedad civil que impongan el autocontrol y la autoregulación en las actividades de inteligencia**.

Conclusiones

El pasado octubre, pocos meses después de que se desatara el caso Snowden, el director de la NSA informaba que la legislación y los programas de espionaje telefónico y de Internet aprobados por George W. Bush tras los sucesos del 11-S y conservados por la Administración Obama tras el fin formal de la Guerra Contra el Terror habían permitido frustrar 54 ataques terroristas alrededor del mundo, 25 de los cuales en Europa, 13 en EEUU, 11 en Asia y cinco en África. Precisamente, estos programas de espionaje masivo aparentemente capaces de monitorizar cualquier comunicación telefónica y de Internet de todo el planeta constituyen la herramienta fundamental de la NSA y se han convertido en uno de los ojos y oídos de EEUU, proporcionando de esta forma el 80% de la inteligencia que emplea el país para apoyar sus decisiones.

El éxito de estos programas de inteligencia criptológica solamente es posible mediante una estrecha colaboración público-privada que, articulada en torno a una relación simbiótica entre el gobierno, la empresa y la universidad, no sólo garantiza la obtención del mejor capital humano, la retención y gestión de este talento o la identificación, financiación y desarrollo de los sistemas tecnológicos más avanzados y acordes con las necesidades reales de cada momento, sino también el acceso gubernamental a los sistemas, capacidades, servicios y flujos de información gestionados por estas empresas, la práctica totalidad de las cuales bajo manos estadounidenses.

Las filtraciones de Edward Snowden y las revelaciones posteriores han obligado a muchos gobiernos a **estimar el valor estratégico del ciberespacio para sus intereses nacionales**. Si hasta ahora consideraban al ciberespacio como un bien común abierto y seguro, ahora han conocido cómo se puede usar para obtener información y ejercer poder. También han dejado al descubierto la **interdependencia asimétrica entre EEUU y sus aliados en materia de inteligencia y el precio que hay que pagar por información que comparten y la inteligencia que reciben**. Si quieren reducirla, deberán tomar ejemplo de la red de colaboración público-privada en EEUU para desarrollar capacidades avanzadas, defensivas u ofensivas, en el ciberespacio. Un entramado de influencias, fondos y programas que ha permitido a EEUU desarrollar una brecha de capacidades tecnológicas con sus aliados y competidores.

Finalmente, las opiniones públicas han conocido su exposición a las tecnologías y la dificultad de sus gobiernos para proteger su privacidad sin una movilización activa. Toda la información –pública o privada– que circula por el ciberespacio tiene un valor de mercado y puede ser usado por terceros en contra de los intereses públicos y privados, por lo que es de esperar que aprendan de la experiencia y se adentren en la **cultura de ciberseguridad** que precisan para moverse en una sociedad global.