ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

19/2013 03 abril de 2013

María José Caro Bejarano

AVANZANDO HACIA UNA CIBER-ESTABILIDAD INTERNACIONAL

AVANZANDO HACIA UNA CIBER-ESTABILIDAD INTERNACIONAL

Resumen:

La preocupación de las naciones por el papel que pueda jugar los ciberataques en la escalada de una confrontación hacia un conflicto en el sentido tradicional es el objeto de este documento. Se recoge la propuesta del Consejo Atlántico de elaborar una estrategia de ciber-estabilidad internacional apoyada en tres factores, que sea el impulso para avanzar en el consenso de normas internacionales de comportamiento en el ciberespacio y en la consecución de acuerdos con países aliados y socios, pero también con potenciales adversarios.

Abstract:

The nations concern about the role cyber-attacks could play in a confrontation escalating into a conflict in the traditional sense is the subject of this document. It presents the Atlantic Council proposal to develop a strategy for international cyber-stability based on three factors to advance the consensus on international norms of behavior in cyberspace and creating agreements with close allies and partners, but also with potential adversaries.

Palabras clave:

Ciber-estabilidad, conflicto, ciberataque, resistencia, cooperación, transparencia

Keywords:

Cyber stability, conflict, cyber attack, resiliency, cooperation, transparency

INTRODUCCIÓN

Las vulnerabilidades cibernéticas conocidas plantean cuestiones relativas a la seguridad nacional en este mundo globalizado en el que somos mucho más dependientes de las tecnologías de la información y las comunicaciones, las llamadas TIC.

Las llamadas infraestructuras críticas y empresas e industrias con tecnologías punteras son todas ellas dependientes de estas nuevas redes y sistemas y por ello son vulnerables ante ciberataques.

El tema tiene cierta complejidad, ya que el entorno cibernético se diseñó para facilitar una comunicación fiable y rápida, pero el hardware y el software en que se apoya no se desarrolló teniendo en cuenta la seguridad. Además, las redes e infraestructuras que subyacen a este tipo de comunicaciones, son poco conocidos y en muchos aspectos interdependientes. Los proveedores de servicios de Internet no pueden funcionar sin electricidad, sin embargo, la red eléctrica depende de la información que intercambia por Internet. Estos recursos cibernéticos, por lo general están en manos del sector privado, sin embargo, la protección contra un determinado ataque puede depender de una acción gubernamental.

La dificultad aumenta porque las capacidades cibernéticas ofensivas están siendo desarrolladas por muchas naciones y siendo buscadas por organizaciones terroristas. Las consecuencias de un ciberataque importante están comenzando a ser analizadas por varios países desarrollados. No está aún claro el papel que jugará el aspecto cibernético en la guerra convencional. Se desconoce el peso progresivo que el factor cibernético pueda tener en una confrontación o conflicto que pudiera escalar hacia un intercambio más amplio geográficamente o en su poder destructivo.

Algunos informes apuntan hacia la forma de alcanzar una ciber-estabilidad internacional[1], poniendo el énfasis en el papel fundamental de la resistencia, la cooperación y la transparencia para crear esa estabilidad. En concreto, se proponen iniciativas específicas de tipo tecnológico, regulatorio y diplomática. También propone normas mundiales cibernéticas críticas para esa ciber-estabilidad. Se sugiere que incluso los potenciales adversarios del Estado-nación pueden encontrar áreas de cooperación en este aspecto.

[1] Véase Achieving International Cyber Stability, Franklin D. Kramer, The Atlantic Council of the United States. September 2012.

CAMINANDO HACIA LA CIBER-ESTABILIDAD

Como se ha mencionado anteriormente el aspecto más preocupante de la ciberseguridad es la posible capacidad de las tecnologías de la información y las comunicaciones para generar o escalar un conflicto geopolítico en hostilidades abiertas o no contenidas a través de ataques a redes operativas. El debilitamiento de capacidades críticas tales como las capacidades militares o la red de suministro eléctrico sería altamente desestabilizador y potencialmente podría escalar a más, generando una progresiva necesidad de avanzar una confrontación hacia un conflicto o intensificar un conflicto contenido hacia un ámbito más amplio.

La ciber-estabilidad internacional puede, sin embargo, lograrse mediante tres vías: la resiliencia, la cooperación y la transparencia. Para conseguir estos objetivos habría que plasmarlos en una triple estrategia con acciones para reducir las vulnerabilidades orientadas a las principales redes operativas; actividades de colaboración con países aliados y socios; y una interacción transparente para la creación de normas, la prestación de la asistencia, y el diálogo con los demás, incluyendo adversarios potenciales, para reducir el riesgo.

El valor de esta ciber-estabilidad sería triple. En primer lugar, al reducir las vulnerabilidades se reduce el riesgo de ataque por un adversario, ya que tal ataque tendrá menos capacidad de lograr sus objetivos. Igualmente, en la medida que un ataque no se materializa el daño se reducirá.

En segundo lugar, al generar la cooperación, aumenta la posibilidad de éxito de la defensa. Por otra parte, también crea un entorno geopolítico internacional que puede dar forma a las actitudes y así reducir, aún más, la probabilidad de un ataque.

En tercer lugar, al aumentar la transparencia, se pueden crear normas internacionales de comportamiento, tanto con respecto a posibles socios como a adversarios potenciales. Para el primer grupo, se ofrece la posibilidad de información y asistencia. Para el grupo de adversarios potenciales se puede crear un aprendizaje compartido que posiblemente conduzca a dos conclusiones: primero, que puede ser de utilidad encontrar áreas de colaboración, a pesar de que no haya un acuerdo universal, y en segundo lugar, que puede haber buenas razones para limitar el uso cibernético para evitar la generación involuntaria de un conflicto y/o escalada.

En el establecimiento de la ciber-estabilidad, es necesario establecer las prioridades ya que el deseo de proteger todo por igual no es realizable de forma práctica, ya sea desde

el punto de vista de los recursos o desde el punto de vista político.

No todas las infraestructuras son igual de críticas o esenciales, a la hora de sustentar la seguridad o la economía. Por ello y de manera clara, los organismos nacionales militares y de seguridad deben ser capaces de operar conjuntamente ante una confrontación. Del mismo modo, en un país no hay actividades que puedan realizarse sin energía eléctrica. Las telecomunicaciones y los sistemas financieros son igualmente cruciales. Centrándose en estas cuatro infraestructuras claves habría que generar y priorizar los recursos disponibles y las soluciones a medida.
Para lograr la *resistencia* se requerirá un enfoque centrado en la ciberseguridad con 1) actualizaciones de hardware y software integradas en 2) una arquitectura eficaz combinada con 3) las obligaciones de los ISP (proveedores de servicios internet) quienes 4) trabajarán con el gobierno en relación con la respuesta a los ataques y 5) será informado, para una mayor comprensión de las operaciones del sistema atacado, mediante el uso de ejercicios y modelización.

El primer paso en la obtención de la *resistencia* es realizar un esfuerzo de desarrollo importante para la mejora de las capacidades hardware y software.

El segundo paso será el desarrollo y la integración de los componentes en una arquitectura operacional. Tal arquitectura se centrará en lo que el ejército llama "misión de seguridad", es decir, la capacidad para realizar la tarea requerida, sin mantener el mismo nivel alto de rendimiento que estaría disponible si los sistemas estuvieran siendo atacados.

El tercer elemento de *resistencia* involucra un mejor sistema de visibilidad y un mayor conocimiento del sistema mediante las capacidades de los proveedores de servicios de Internet. Aunque los ISP tienen que comprometerse, no se les debe pedir que traten con funciones inherentemente gubernamentales – como la protección de infraestructuras críticas - sin la debida intervención del gobierno. Por consiguiente, debería darse un acuerdo combinado gobierno/ISP que requiere que los proveedores de servicios de Internet asesoren al gobierno en caso de infecciones u otras amenazas a la fiabilidad y entonces será el gobierno quien tome o autorice al ISP a tomar medidas para ayudar a eliminar esa amenaza.

La *cooperación* eficaz requiere un enfoque con cuatro partes: el establecimiento de 1) un pequeño grupo cooperativo de naciones afines, incluyendo el establecimiento de un Consejo de Ciber-Estabilidad, 2) la utilización de las normas acordadas, 3) trabajar juntos sobre las actividades operacionales, y 4), incluyendo a las entidades clave del sector privado, en este esfuerzo.

En el primer paso, los Estados Unidos ya han comenzado una estrecha interacción con el Reino Unido, como lo ha hecho con otros países como Canadá y Australia. Esta cooperación debería ser ampliarse para incluir a otros aliados clave que tienen importantes capacidades cibernéticas. Este es el caso de Francia, Alemania, Japón y la República de Corea.

En segundo lugar, deberían establecerse normas comunes sobre infraestructuras críticas entre este grupo de países afines. Debería crearse un Consejo de Ciber-Estabilidad, siguiendo las líneas de la Junta de Estabilidad Financiera establecida por las naciones para cuestiones financieras derivadas de los acuerdos de Basilea.

En tercer lugar, será necesario crear un enfoque operacional coordinado. Un elemento clave será la creación de una red de decisores que tome las decisiones estratégicas, incluyendo al sector privado, identificados con anticipación para hacer frente a ataques a una infraestructura crítica.

Un enfoque viable para la *transparencia* tendrá también tres partes: 1) la elaboración y promulgación de normas para los que trabajen con los países de ideas afines; 2) asistencia a los países que deseen ser socios eficaces para mejorar la capacidad de resistencia y recuperación, y 3) la interacción transparente que implique diálogo con los demás, incluyendo a los adversarios potenciales, para reducir los riesgos.

CONCLUSION

Para las naciones asociadas a la propuesta de un Consejo de Ciber-Estabilidad surgen tres normas:
1) Los gobiernos deberían promover el establecimiento de arquitecturas resistentes en cada una de las cuatro infraestructuras críticas claves: militar, eléctrica, telecomunicaciones y finanzas.
2) Los gobiernos deberían cooperar en la creación de un Consejo de Ciber-Estabilidad internacional que se encargue del establecimiento de normas y capacidades operativas.
3) Los gobiernos deberían alcanzar compromisos con ISP y otras entidades de infraestructuras críticas y de tecnología de la información para crear arquitecturas de ciberseguridad internacionales con capacidad de resistencia y recuperación, en relación con la operación del propuesto Consejo de Ciber-Estabilidad.

También será de gran valor ampliar las capacidades de ciberseguridad a otras naciones que estén dispuestas a participar de manera efectiva en la creación de la ciber-estabilidad. Los Estados Unidos, en su nueva estrategia de defensa, busca asociarse específicamente con, y/o tutorizar a otras naciones para aumentar sus capacidades en los dominios comunes como es el ciberespacio.

Por último, la colaboración con países de interés cibernético, como China y Rusia, puede ser posible en áreas particulares. Lo primero sería la reducción de la capacidad de terroristas y otros terceras partes para lanzar un ataque contra cualquiera de estos países. Lo segundo sería generar un entendimiento común de los temas relacionados con el papel potencial del aspecto cibernético en la generación y la escalada de conflictos.

Mª José Caro Bejarano
Analista del IEEE