Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global

Jeimy J. Cano

Los eventos recientes sobre fuga de información, las noticias de atacantes informáticos doblegando protocolos y tecnologías de seguridad, las fallas de seguridad que se han presentado tanto en el sector público como en el sector privado, son argumentos suficientes para evidenciar que estamos en un nuevo escenario de riesgos y amenazas, donde la información se convierte en un arma estratégica y táctica, que cuestiona la gobernabilidad de una organización o la de una nación. (CANO, J. 2008).

En este contexto, los ejercicios de riesgos y controles propios de las empresas, para establecer y analizar los activos de información críticos, han dejado de ser *"algo que hacen los de seguridad"* para transformarse día con día en una disciplina que adopta la organización, para hacer de su gestión de la información una ventaja clave y competitiva frente a su entorno de negocio. Por tanto, la figura opcional de la seguridad de la información, comienza a desvanecerse y a tomar una relevancia estratégica, ahora en un escenario donde la información, es la *"moneda fundamental"* para generar, proponer y desarrollar posiciones privilegiadas de personas, empresas y naciones.

Cuando elevamos esta reflexión a nivel de Estados y países, encontramos múltiples vistas para comprender los riesgos y amenazas frente a la información y sus impactos, que generan confusión y desconfianza, generalmente aprovechadas por los escépticos, para reparar en comentarios poco constructivos, que tratan de limitar la importancia de estos temas. Sin embargo, los hechos y eventos que se han presentado, mantienen la atención de gobiernos sobre estos peligros, que aunque escondidos en el tejido de las noticias cotidianas, son actores claves de las relaciones internacionales y la capacidad de reacción de un Estado. (McAFEE 2009).

Reconociendo al enemigo digital: Ciberdefensa

Una primera estrategia que adoptan los Estados cuando reconocen *"al nuevo enemigo"* en el contexto de una sociedad de la información y el conocimiento, es reconocer que cuenta con infraestructura de información crítica, requerida para mantener la operación y gobernabilidad de la nación. Siguiendo la directiva presidencial No.13010, firmada por el presidente norteamericano Bill Clinton en 1998 (US CONGRESS 1998), se definen ocho sectores críticos cuyos servicios son vitales para el funcionamiento de la nación, y la incapacidad de operación o destrucción tendría un impacto directo en la defensa o en la seguridad económica de los Estados Unidos. Tales sectores son: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales (mínimas requeridas para atender al público).

Así las cosas, un ataque masivo y coordinado a alguno o varios de estos sectores establece una condición importante y crítica para una nación, pues se pone en juego la estabilidad de lamisma y la confianza de la ciudadanía en su gobierno para enfrentarse a estas amenazas. En este sentido, el concepto de guerra tradicional, se transforma para darle paso a una nueva función del Estado frente a la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos, ante las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.

En consecuencia, se acuña el término de **ciberdefensa** como esa nueva connotación sistémica y sistemática que deben desarrollar los gobiernos, para comprender ahora sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la comprensión de variables como, las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo online; la renovación de la administración de justicia en el entorno digital; y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

En tal sentido, las reflexiones y decisiones sobre la seguridad nacional, tienen una renovada connotación, para atender ahora un enemigo móvil, cambiante y evolucionado, que se mueve tanto en las infraestructuras críticas como fuera de ellas; que sabe lo reactivo de las empresas y gobiernos; y que, a pesar de que pueda ser identificado en sus ataques, es poco creíble probar que existió.

La defensa nacional, como noción acuñada por las fuerzas militares de un país, requiere ser analizada y repensada en el contexto del *"nuevo rostro de la guerra"*, de una confrontación que enfrenta lo mejor de los entrenados en el arte de la inseguridad de la información, con lo mejor de los entrenados para controlar y mantener la paz de una nación. Por tanto, animar una revisión de las estrategias de seguridad nacional ante posibles y factibles escenarios de confrontación tecnológica y de guerra de la información, prepara a los Estados para defender su

gobernabilidad y asegurar su resiliencia en condiciones de falla parcial o total.

A la fechas muchos Estados (generalmente de países desarrollados) han tomado acciones concretas en el reto de la ciberdefensa, encontrando en sus ciudadanos los primeros y más importantes aliados para sus estrategias de protección de la nación en el contexto digital. Dichos Estados comprenden que es, desde el ciudadano y su experiencia en el uso de las tecnologías de información y comunicaciones, donde pueden fortalecer el perímetro extendido de seguridad nacional digital. Conocedores de que es poroso y poco confiable, saben que allí encuentran su mejor carta para hacer realidad su visión de defensa de la nación en un mundo interconectado. (CANO, J. 2008b)

Detallando las prácticas de aseguramiento: ciberseguridad

Para darle vida a esta visión de la defensa nacional digital, se requieren elementos específicos que materialicen ese querer en acciones detalladas, que aplicadas en las tecnologías de información e interiorizadas en los hábitos de los ciudadanos, puedan hacer evidente esa nueva propiedad emergente, denominada seguridad nacional digital, que genera confianza, respeto y confiabilidad en las iniciativas del gobierno ante la realidad de la creciente dinámica informática y de las telecomunicaciones.

Considerando lo anterior, es evidente que los gobiernos no pueden hacer realidad su nueva visión de la defensa, sin una estrategia concreta de prácticas de seguridad de la información, como base fundamental de su visión de seguridad nacional, donde cada uno de los individuos reconozcan en la información un activo fundamental que articula todas las infraestructuras críticas de la nación, y que hace realidad el sueño de una sociedad "informada".

Así las cosas, el concepto de **ciberseguridad**, como realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital, en un conjunto de variables claves, acertadamente definidas por la ITU -International Telecommunication Union-, en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de una realidad digital y de información instantánea.

La ITU, entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional. (ITU 2010)

Cada una de las variables establecidas por la ITU, no buscan otra cosa que comprender los riesgos propios de una sociedad de la información digital y en constante movimiento, que considere los aspectos normativos, las tecnologías de seguridad de la información, la organización de la seguridad de la información necesaria

para operar, la cultura de seguridad de la información y la cooperación entre países, como fuente de la armonización de visión de la ciberseguridad en el planeta.

Reflexiones finales

De acuerdo con lo planteado, cuando hablamos de ciberseguridad, necesariamente debemos considerar las acciones básicas que desarrolla una nación para proteger de manera coherente, sistemática y sistémica los activos de información crítica, distribuidos en toda su infraestructura y cómo ellos impactan la operación del Estado.

De la mano con los conceptos de ciberdefensa y ciberseguridad, se han venido desarrollando reflexiones académicas y de la industria, relacionadas con ciberterrorismo y cibercrimen (CANO, J. 2008), dos amenazas emergentes en una sociedad digital, las cuales han comenzado a inquietar a los ciudadanos, quienes hoy por hoy se sienten expuestos frente a la materialización de las mismas y sus efectos reales sobre la confianza en el Estado y sus instituciones.

Si bien la ciberdefensa como la ciberseguridad, son temas de estudio e investigación actual, tanto en la industria, la academia y el gobierno, es claro que requieren atención inmediata con acciones definidas que permitan comunicar a los potenciales agresores, que estamos preparados para enfrentar el reto de un ataque informático coordinado, para hacer respetar nuestra soberanía nacional digital.

Referencias

[1] ITU (2010) Global cybersecurity agenda. Disponible en: http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf

[2] US CONGRESS (1998) PRESIDENTIAL DECISION DIRECTIVE/NSC-63. Disponible en: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[3] CANO, J. (2008) Cibercrimen y ciberterrorismo. Dos amenazas emergentes. [4]ISACA Information Control and Audit Journal. Vol 6. Disponible en: http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Pages/JOnline-Cibercrimen-y-Ciberterrorismo-Dos-Amenazas-Emergentes.aspx

[4] CANO, J. (2008b) La guerra fría electrónica y la inseguridad de la información. Publicación en Blog. Disponible en: http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450012245&random=4197

[5] McAFEE (2009) Virtual Criminology Report 2009. Virtually Here: The age of cyber warfare. Disponible en: http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf

Jeimy J. Cano. *Ph.D, CFE. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management. Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE por la ACFE y Cobit Foundation Certificate por ISACA.*