Infraestructuras críticas: límites virtuales de las naciones en las relaciones diplomáticas

Martín Salmerón[9]

Siendo el ciberespacio un ambiente que ofrece millones de posibilidades y extiende cada día más su alcance, es interesante realizar un pequeño análisis sobre las interacciones que ocurren dentro del mismo.

Gracias a las Tecnologías de la Información y las comunicaciones (T.I.C.), existen herramientas que permiten la interconexión entre dos personas que físicamente se encuentran a kilómetros de distancia, pero que virtualmente están a un clic de interactuar haciendo uso de la mayoría de sus sentidos.

Ello ha permitido con el correr del tiempo, que las relaciones interpersonales trasciendan el "espacio íntimo individual", y den lugar a relaciones más complejas que, además, promueven la intervención económica y funcional de las mismas; es decir, ya no es necesaria la interacción presencial para realizar transacciones o intercambios, sino que, en el mundo "binario" se resuelven, en diferentes monedas, en cuestión de segundos, y con la existencia de las "cripto monedas", este intercambio se ha simplificado para hacer común un idioma cada vez más utilizado a nivel mundial.

Por otro lado, existen intercambios de metodologías de ejecución de tareas, la transferencia del know-how de muchísimas actividades se trafican por la internet, al punto tal de lograr llegar a convertir en "físico" algo "virtual" con mínima y en un futuro no muy lejano "nula" participación de mano de obra humana.

A medida que el tiempo ha pasado y sigue su vertiginoso avance, definiciones como la "internet de las cosas" pasan a ser más que algo hogareño y se convierten en conceptos complejos que trascienden la manera en que un modem se conecta con algunos dispositivos del hogar, para convertirse en estructuras virtuales de gran envergadura, desde donde comienzan a pender infraestructuras de la información que administran datos en grandes cantidades.

Esta dependencia, en esencia, no tiene otro objetivo más que el de "eficientizar" los procesos deductivos, productivos, educativos, entre otros, y en la mayoría de los casos, poca o ninguna importancia se le da a la "seguridad", ya no solo de la información misma, sino también, de la infraestructura que la sostiene, desde el punto de vista físico y virtual.

Cuando una infraestructura de estas características se encuentra con "información de la población", cuando comienza a administrar datos que son útiles a la "Administración y Gobierno" de un Estado, es que la importancia de las mismas crece potencialmente y, por lo tanto, crece la necesidad de brindar la adecuada seguridad a estas.

9 Licenciado en Sistemas Aéreos e Interespaciales

Son estas estructuras, virtuales y físicas, que al momento de encontrarse administrando información de vital importancia para un Estado u organización gubernamental, pasan a denominarse “infraestructuras críticas del Estado”.

Ahora bien, habiendo aclarado en lo posible algunos conceptos básicos respecto de dichas infraestructuras, podemos hacer la analogía en donde, un Estado, virtualmente organizado en información y procesos, debidamente asegurados estos, comienza a interactuar con otros Estados, organizados de la misma manera.

Allí es cuando vemos que, no solo las infraestructuras críticas de un Estado, aseguradas en un sistema “aislado”, comienzan a tener necesidad de interactuar entre sí sino que, además, ya no solo importa brindar la debida seguridad a esa estructura, sino también a los canales y modos de “interacción”.

Por supuesto que manteniendo los modos “clásicos” de interacción, en donde los representantes de un Estado, ya sea en la figura de sus ministros o del mismo presidente de la Nación, existe la “seguridad” del interactuar cara a cara. Sin embargo, en un futuro existen muchas posibilidades de que esta interacción sea cada vez más “protocolar”, y que las negociaciones y arreglos sean previamente realizadas en entornos virtuales, para ser rematadas de forma presencial con el simple acto de una firma.

Es así como, de un tiempo hasta ahora, nuestros profesionales de “lo internacional” tendrían que prestar atención a estos “métodos” de interactuar con sus pares extranjeros, buscando no solo la mejor manera de comprenderse el uno al otro, sino también dándole importancia a la seguridad de estas estructuras.

Es importante entender que, la información crítica de un Estado, contenida en la infraestructura correspondiente, será un objetivo “codiciado” por quienes deseen atentar contra los intereses de este. Lógicamente entonces, no debe existir ningún canal que conecte a ésta con otras infraestructuras que no le sean funcionales, puesto que, a nivel virtual, todas las estructuras pueden ser vulneradas de alguna u otra manera a lo largo del tiempo.

Sin embargo, existen momentos en donde, en pos de funcionalizar un intercambio, innovar políticamente en el campo de las relaciones, se “saltan” algunos pasos para poder cumplir con los objetivos previstos.

Es en estos momentos donde debe darse prioridad a cumplir con criterios de seguridad debidamente establecidos por profesionales del área de la Ciberseguridad y la Ciberdefensa, aun cuando esto no sea “políticamente visible”, la importancia de la información que se administra en estos casos puede llegar a verse perjudicada y con ello, convertirse en elementos de extorsión a los intereses del Estado por aquellos que, como antes cita el texto, buscan obtener ventajas de cualquier tipo, por el solo hecho de hacerse de dicha información.

En nuestro país, la resolución 580/2011, de la Jefatura de Gabinete de Ministros, creo el PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD.

En dicha resolución, se pone de manifiesto entre otras cosas que:

“El mundo contemporáneo se caracteriza por los profundos cambios originados en el desarrollo y difusión de las tecnologías de la información y la comunicación en la sociedad, las cuales se encuentran sustentadas en gran medida en el ciberespacio”

“La utilización de las comunicaciones virtuales es un recurso que depende de la infraestructura digital, la cual es considerada como infraestructura crítica, entendiéndose ésta como imprescindible para el funcionamiento de los sistemas de información y comunicaciones, de los que a su vez dependen de modo inexorable, tanto el Sector Público Nacional como el sector privado”

“La seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas”

Entre las funciones del Programa Nacional de Infraestructuras críticas se enmarcan algunas de las siguientes tareas entre otras:

“Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Publico Nacional.”

“Promover la concientización con relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica”.

Es por esto que, como profesionales en el ámbito de las Relaciones Internacionales, no están exentos ni alejados de la administración pública nacional porque, al final de cuentas, quienes nos representan ante el concierto de las naciones, sea en el nivel que sea, son usuarios y custodios de información que puede resultar critica a nuestros intereses nacionales, y como tal, deben interiorizarse sobre la forma adecuada de administrar dicha información en pos de acrecentar la seguridad de nuestra nación.

Fuentes

Resolución 580/2011 de la Jefatura del Gabinete de Ministros

Programa Nacional de Infraestructuras Críticas, de Información y Ciberseguridad. www.icic.gob.ar