Centro Andino de Estudios Estratégicos

CENAE

Acerca de la soberanía del Ecuador en el ciberespacio

Mario Ramos

Septiembre 2014

Acerca de la soberanía del Ecuador en el ciberespacio

Si no fuera por las revelaciones de Snowden, plantear la hipótesis de que nuestra soberanía y seguridad en el ciberespacio es muy débil, sería automáticamente descalificada y tildada como una paranoia más de la teoría de la conspiración.

Si cualquiera de las fuerzas aéreas de nuestros vecinos invadiera nuestro espacio aéreo, no cabe duda que sería motivo de escándalo y dependiendo de la gravedad del hecho, incluso se convocaría a organismos internacionales para dejar sentado el respectivo reclamo.

Pero al parecer hay una soberanía que está siendo violada sistemáticamente, sin que el gran público e incluso los organismos de seguridad y defensa, tengan clara conciencia o respuesta a esa situación. La amenaza a la seguridad interna y externa a través del medio tecnológico, no es aun cabalmente asimilada en toda su magnitud por los ciudadanos y por los responsables de establecer las respectivas políticas, regulaciones y estrategias para cuidar la privacidad de las personas y la información, servicios e infraestructura sensible del Estado.

Como veremos en los siguientes párrafos, el problema es excesivamente complejo. Ahora es posible que un país sea vulnerado por un enemigo o por la ciberdelincuencia en sus redes e infraestructuras informáticas desde cualquier parte del planeta.

Además, la tecnología presente está convirtiendo en pieza de museo, nuestra comprensión de lo que puede ser una guerra. En la actualidad, varios ejércitos han conformado unidades de *ciberguerreros* y están preparándose para el campo de batalla del futuro. De hecho, ya se ha empleado *ciberarmamento*[1] en varios conflictos, por ejemplo en la guerra de Irak miles de oficiales iraquíes recibieron mensajes en sus correos electrónicos, en lo que fue una efectiva operación psicológica. Pero esto ya es prehistoria, se intuye que pueden existir *ciberarmas* muy refinadas que esperan el escenario y el momento oportuno para ser utilizadas.

En estos tiempos es muy factible conocer el tipo de armamento convencional que posee un país, pero es muy difícil saber qué tipo de instrumentos y habilidades existen y se están desarrollado para la ciberguerra. La inteligencia electrónica no es la principal preocupación para determinados países que la emplean desde hace décadas y han aprendido a defenderse de aquella, sino conocer cómo está preparando el campo de batalla un enemigo potencial para desatar una ataque cibernético tan veloz que no haya posibilidad de defensa.

Cuando hablamos de *preparación del campo de batalla*, lo hacemos en el sentido convencional, es decir, la clásica función que tienen los ingenieros militares, pero no en las perspectivas que puede tener en su repertorio un *ciberguerrero*. Una unidad militar especializada en ciberguerra en '*tiempos de paz*' pueden estar colocando *puertas traseras* y *bombas lógicas* en miles de blancos sin que nadie lo pueda notar, y mantenerlos ahí como *células dormidas* esperando a ser actividades cuando la necesidad lo amerite. Todo un sistema de mando y control y comunicación puede ser desactivado por un ataque cibernético, y ésta es solo una de las múltiples posibilidades[2] que tiene a su alcance una *fuerza especial*

[1] Por ejemplo, se acusa a Israel de haber saboteado la planta de enriquecimiento de uranio de Natanz, Irán, usando el gusano Stuxnet.

[2] Se puede conseguir que un sistema de armas funcione mal, neutralizarlo o bloquearlo. Igual cosa puede suceder con la red de suministro eléctrico y por ende paralizar todo lo que funciona con electricidad. Los aviones son ahora sistemas informáticos que vuelan, si estos fallan simplemente dejan de volar. Enviar órdenes falsas a fuerzas armadas enemigas. Provocar caos en los sistemas de movilidad. Inundar de propaganda a los

cibernética. La cuestión se complica si esas capacidades caen en manos del crimen organizado, imaginemos qué sucedería si logran vulnerar el sistema financiero de un Estado.

Actuar sin hacer ruido no es ninguna novedad, la Agencia Nacional de Seguridad de los EE.UU. (NSA por sus siglas en inglés), de acuerdo a las revelaciones de Snowden, durante décadas fue (y lo sigue siendo) la herramienta con la cual sin alterar datos o causar daños, se infiltró en la infraestructura de Internet de casi todo el globo y convirtió al ciberespacio en un potente método para adquirir todo el conocimiento necesario.

Cuando los hackers han conseguido robar propiedad intelectual o información clave de empresas u organismos estatales, muchas veces los afectados ni siquiera se enteran que han sido víctimas de una sustracción, porque es posible penetrar una red y asumir el rol de administrador autorizado sin activar alarmas, toda infiltración se puede oscurecer - borrar.

Ingredientes que permiten la ciber inseguridad

Entre los factores que facilitan la ciberguerra y el cibercrimen están los fallos en *softwares* y *hardwares*. Todos los dispositivos que se conectan a Internet son fabricados por múltiples empresas, por lo que se pierde el control sobre lo que realmente contienen, otro tanto sucede con la elaboración de los programas informáticos, en su creación intervienen varias personas y compañías. Los "errores" de programación permiten a los hackers penetrar los softwares y crear formas de engañar los sistemas.

"En 2009, un nuevo tipo o variante de malware ingresó en el ciberespacio cada 2,2 segundos por término medio". (…) "El caso más famoso, y uno que sirve para ilustrar un fenómeno más amplio, ocurrió cuando alguien en Microsoft vertió un simulador de vuelo entero dentro del programa Excel 97. Microsoft sólo lo descubrió cuando la gente empezó a agradecerle a la compañía haberlo hecho. Los programadores pueden hacer algo así por diversión, por ánimo de lucro, o por estar al servicio de la competencia o un servicio de inteligencia extranjero; pero cualquiera que sea el motivo, la cuestión es que es casi tarea imposible garantizar que programas tan grandes estén limpios de esas pocas líneas de código que se necesitan para permitir un acceso no autorizado a través de una <puerta trasera>." (Clarke y Knake, 2011:128-130,131).

Lo que se puede hacer con un error en los millones de líneas de código, se puede hacer con millones de circuitos integrados, chips, routers, servidores, etc.

Esta es la razón por la que la industria de armamentos de Rusia ha anunciado que ellos fabricarán todos sus componentes. De igual manera, China está vetando la adquisición de productos informáticos extranjeros y solo tolera los de procedencia nacional. Cuando más dependiente está una fuerza armada o un Estado de programas informáticos y otras tecnologías que tienen que ver con Internet, se vuelve más vulnerable. Cada día se generaliza la opinión de los expertos en el sentido de que los códigos del sistema operativo de grandes empresas como Microsoft o Cisco, entre otras, contienen puertas traseras o vulnerabilidades de seguridad. Por otro lado, servicios de inteligencia han tomado medidas radicales, simplemente han decidido *desconectarse* y volver a la máquina de escribir o utilizar técnicas criptográficas vigorosas que deben estar cambiando y evolucionando en espacios cortos de tiempo, lo que es un inconveniente por los costos que genera.

---

medios de comunicación. Ataque concertado al sistema informático de un sector de la economía. Robo de la identidad a través de infiltrarse en el Registro Civil, etc.

Crear nuestras propias redes informáticas para aplicaciones relacionadas a seguridad y defensa, es algo inevitable si tomamos en serio la amenaza que hay que afrontar. Se tiene que avanzar en separar la infraestructura crítica de la Internet pública o abierta.

Ecuador está a la vanguardia en determinados servicios ciudadanos como la entrega del pasaporte y el documento de identidad, entre otros, y busca cada día mejorar y agilitar los trámites públicos. Esto ha sido posible gracias a la gran inversión que el gobierno de la Revolución Ciudadana ha realizado en tecnología, mucha de la cual tiene que ver con Internet y universalización de acceso a las redes.

Esto implica que, cada día la economía se conecta más y depende de la Internet, por lo que el gobierno debe establecer políticas, regulaciones y estrategias de avanzada para gradualmente lograr niveles óptimos de seguridad y defensa en el ciberespacio.

Muchos sugieren cambiar la 'cultura' del Windows, por sistemas de código abierto como el Linux, sin embargo, la solución va más allá que simplemente definir una tendencia tecnológica, ya que en realidad los dos tipos de sistemas tienen vulnerabilidades y *puertas traseras*. Es difícil conseguir seguridad absoluta, pero si es posible incrementar sustancialmente los niveles de inmunidad. La alternativa que permitiría disminuir el riesgo es desarrollar nuestras propias soluciones casa adentro, especialmente las destinadas a proteger aspectos e infraestructuras sensibles. Este es un paso inevitable a adoptar si queremos estar menos expuestos a los ataques cibernéticos, esto en un principio puede ser costoso, pero los beneficios en el largo plazo serán incalculables.

Snowden reveló que las grandes transnacionales proveedoras de redes o servicios de Internet, tienen tratos con la Agencia de Seguridad Nacional de los EE.UU. Sería una suprema irresponsabilidad no ir construyendo nuestra independencia en esa materia. El uso de software comercial por el código fuente que se considera propiedad intelectual, es uno de los orígenes de todas las amenazas a la seguridad de los países.

Desafíos para la soberanía en el ciberespacio

Los sistemas de información están conectados a algún tipo de red IP, la cultura del 'todo conectado' adquiere progresiva complejidad y esto los vuelve más vulnerables, además sus aplicaciones tienen muy diversas variables, lo que imposibilita controlar todas sus funciones.

Se tiene que avanzar en una nueva arquitectura de Internet que contemple todos los desarrollos que en materia de seguridad se requiere en la actualidad. El Internet nació en el siglo pasado con un diseño que no estaba pensado para todos los usos que ahora se aplican en los sistemas TIC, como en el gobierno, educación y comercio electrónico, todas las capacidades que tienen ahora los celulares, los servicios públicos, gestión de infraestructuras de manera remota, Internet de las Cosas (una casa domotizada proporciona suficiente información sobre los hábitos, psicología, relaciones de sus ocupantes), los ciudadanos desconocen que los populares dispositivos inteligentes tienen la aptitud de espiar con imagen y sonido a sus usuarios, así que si usted tiene su televisor conectado a Internet, ya puede imaginar los riesgos.

"El aumento en la conectividad de cualquier tipo de dispositivo está provocando cada vez más incidentes de seguridad, a cambio de una serie de ventajas a corto plazo. Es necesario implementar políticas más restrictivas de conectividad a la red, realizando un análisis crítico de los problemas de seguridad que se originan a largo plazo y buscando alternativas a las estrategias de gestión remota. En cuanto a la interoperabilidad de sistemas,

hay una corriente de opinión entre los especialistas del sector industrial que opina que parte de los problemas de seguridad podrían evitarse volviendo a utilizar sistemas y protocolos dedicados." (Salvador Carrasco, 2014:6).

En materia de ciberseguridad no se puede ser ingenuo, para conseguir soberanía sobre el patrimonio tecnológico de un Estado es inevitable desarrollar un conocimiento e industria propios, sobre todo en la infraestructura de comunicaciones relacionadas a los aspectos sensibles de un país.

"Utilizar tecnología desarrollada por terceros países supone exponerse a que puedan existir agujeros introducidos de forma deliberada, debilidades que podrían ser explotadas en caso de conflicto o introducidas en las actualizaciones periódicas. En el mejor de los casos, supone utilizar unas técnicas que están un paso por detrás de las empleadas por el país proveedor." (Salvador Carrasco, 2014:10).

Por todo lo expuesto hasta el momento, creemos que no es exagerado señalar que en algunos ámbitos carecemos de soberanía en el ciberespacio, especialmente en cuanto a resguardar datos de los ciudadanos como su número de identidad o cuentas bancarias. En este marco, Sally Burch expone claramente lo que la concentración monopólica en el área de la tecnología digital e Internet implica:

"EEUU, que mediante su control de la infraestructura y con sus corporaciones transnacionales domina claramente el mundo Internet, tiene muy clara su prioridad de mantener un régimen global de libre comercio en este ámbito (o sea, un mercado desregulado, salvo en materia de propiedad intelectual) para garantizar las ambiciones globales de sus corporaciones y hegemonizar el futuro digital del planeta. Esta potencia asigna una gran prioridad a mantener su supremacía tecnológica y a favorecer la expansión de sus empresas (que ya se cuentan entre las más poderosas de la economía estadounidense). También dedican ingentes inversiones para desarrollar enormes bancos de datos a partir de los flujos mundiales de información, que constituyen en sí mismos una fuente de conocimiento y de poder; a expandir aún más su capacidad de vigilancia y espionaje global; y a desarrollar ciber-armas y capacidad ofensiva como un aspecto central de su política de "ciberdefensa"."[3]

Si bien hay anuncios prometedores, como los realizados por la UNASUR en el sentido de que es necesario construir un anillo de fibra óptica suramericano para conectar a la región sin depender de los EE.UU, Ecuador y los países con auténtica vocación de independencia en materia tecnológica no pueden caminar al ritmo de los Estados que tienen posturas geopolíticas ambiguas. Lo que no niega que se debe hacer todos los esfuerzos para elaborar una política y estrategia común en ciberseguridad y ciberdefensa.

Las nuevas tendencias de las TICs

El servicio de *nube* exhibe una imagen de amenaza para la mayoría de potenciales usuarios, ya que parten de supuestos como: los datos pueden ser controlados por el proveedor del mencionado servicio, filtración de información confidencial e incluso la pérdida total o parcial de los datos, un espía no tendría que infiltrarse en innumerables computadores, solo hacerlo en pocos objetivos-*nubes* o proveedores. Sin embargo, esto puede ocurrir cuando no se toman las medidas necesarias de control como: encriptación de datos en la fuente y transición, nubes privadas externalizadas, asilamiento de información, encriptación transparente, entre otras tecnologías.

[3] URL del artículo: http://www.alainet.org/active/76641

Es decir, las intenciones del FBI "de controlar en tiempo real aplicaciones en la Nube como Gmail o Dropbox. (…) programas de control [que] también se han destapado en Reino Unido, la India y otros países". (Salvador Carrasco, 2014:12). Son posibles porque se trata de nubes públicas gratuitas, no privadas.

Todo se complica gracias a las asombrosas prestaciones que tienen en el momento actual los celulares, que facilitan la vida pero han convertido a sus portadores en seres absolutamente vulnerables en su privacidad y seguridad, y en instrumento para la ciberguerra:

"Durante la guerra de Irak, un ataque relámpago con morteros destruyó cuatro helicópteros Apache recién llegados a una base norteamericana. La precisión del bombardeo fue posible porque los soldados tenían la costumbre de tomar fotos, usando sus teléfonos móviles, de la llegada de cada nueva flota y, por supuesto, subir dichas fotos a Internet. Las imágenes incluían metadatos, en particular datos GPS, que permitían localizar con total exactitud la posición de las aeronaves." (Salvador Carrasco, 2014:13).

No es exageración señalar que el usuario de una tablet, smartphone o celular está sujeto, si alguien tiene interés en él, a ser localizado en todo momento, seguir sus desplazamientos, escuchar lo que dice e incluso atacarlo usando técnicas avanzadas de seguimiento y revelación de datos.

Otra novedad actual es el Big Data, que consiste en sacar provecho a las grandes cantidades de datos que reposan en las instituciones, correlacionando con diferentes tipos de información, para generar nuevo conocimiento, como tendencias de mercado, gustos y preferencias, entre otros. En otras palabras, procesar información a escalas desconocidas e involucrar a un número diverso de elementos. Esto es posible porque el célebre pero inexistente 'libre mercado' se está superponiendo a la confidencialidad de los datos de sus clientes.

Pero dejemos que *in extenso* los especialistas nos den sus opiniones al respecto:

"Vivimos entre trillones de datos, una enormidad silenciosa en formato alfanumérico. Desde las geolocalizaciones en GPS hasta la más insignificante transacción comercial mediante tarjeta de crédito o débito en la tienda de la esquina deja una huella digital que es procesada inmediatamente por el sistema capitalista a través de las empresas o bien por instancias gubernamentales.

La estadística es la primera disciplina científica actual. Todo se reduce a establecer correlaciones útiles o señeras entre señales dispares que emanan de la comparación, muchas veces arbitraria, entre grandes conjuntos de big data. Las correlaciones nos dicen qué está pasando pero nunca se preguntan ni arrojan luz ni ofrecen resultados satisfactorios sobre los antecedentes o causas de un hecho determinado.

Lo más alarmante, no obstante, es que ofrecemos nuestra intimidad de modo gratuito, sin recabar en que estamos regalando nuestro ser a cambio de nada. Sobrevivimos en una constante alienación de nuestra esencia humana. Nos dejamos manipular en nombre de una quimera llamada libertad capitalista.

La información que se vierte a diario conforma las tendencias de uso genérico y el marco de referencia a seguir por las multitudes. El procesamiento de los big data mide la adhesión o conformidad más o menos reticente de la gente a los ítems inoculados por los mass media."[4]

De otra forma, Salvador Carrasco nos dice en esencia lo mismo:

[4] URL del artículo: http://www.rebelion.org/noticias/2014/8/188780.pdf

"El impacto económico del Big Data es enorme. De hecho, ya se está empleando en el marketing y la prospección comercial de forma general (planificación de campañas publicitarias, localización de centros comerciales, distribución de productos) y para el *targeting* y *scoring* individualizado en función del perfil de cada cliente, un perfil muy detallado.

La información que tienen esas corporaciones sobre individuos específicos o sobre segmentos de población es lo suficientemente buena como para emplearla más allá que en inteligencia económica. Estas empresas se han convertido en grandes corporaciones en el sector de las tecnologías y la influencia que podrían ejercer por sí mismas, o empujados por los gobiernos de sus países de origen o los grupos de interés que los soportan, es enorme. Su existencia compromete el propósito original de las iniciativas como Open Data, el libre acceso a las bases de datos en manos de las administraciones públicas, o de las leyes de transparencia. Los grandes grupos del sector de la información son los que tendrán más recursos para la explotación y el cruce de esta información procedente de la Administración." (Salvador Carrasco, 2014:16).

Habría que aclarar que en Ecuador, la política de datos abiertos no compromete la seguridad nacional, ni la privacidad de los ciudadanos. El *Open Data* en Ecuador está normado y solo se puede publicar lo que la norma faculta. (Ley Orgánica de Transparencia y Acceso a la Información Pública).

¿Qué hacer?

La iniciativa del gobierno de la Revolución Ciudadana de permitir que los estudiantes usen sus celulares u otros aparatos móviles en las clases es correcta y debe enfocarse de manera especial en educar a los usuarios en el sentido de que tomen control sobre la tecnología y no dependan en exceso de ella. Es importante inculcar a las nuevas generaciones, lo innecesario de publicar los aspectos personales y cotidianos de sus vidas en las redes sociales, por ejemplo.

Frente a los riesgos conocidos y sobre todo, por los que aún desconocemos, es imprescindible si queremos avanzar en el proyecto del voto electrónico y preservar nuestra democracia y la transparencia de la voluntad popular en los procesos electorales, fijarse como condición ineludible, avanzar de manera rápida en mayores niveles en cuanto a soberanía tecnológica. El *Gran Hermano* goza de una imaginación desestabilizadora inagotable, por lo que existe la posibilidad teórica de que si un proceso electoral depende de redes de comunicación que no controlamos se tuerzan sus resultados.

En nuestro artículo del 18 de junio del 2013 titulado: *"Es necesaria una Revolución Militar Integral en Nuestra América"*, escribimos lo siguiente:

"Por otro lado, frente a la cada vez creciente amenaza de ataques cibernéticos, el Ministerio de Defensa (…) [debe] pensar en crear un Mando de Defensa Cibernética para protección de infraestructuras y servicios púbicos críticos. Este tipo de proyectos toman tiempo implementarlos, por eso, se debe empezar ya. La expansión de la tecnología digital genera vulnerabilidades y riesgos." (Ramos, 2013:7)

Nos alegra el anuncio de que efectivamente se creará un Comando Operacional de Ciberdefensa. Desconocemos los detalles de su diseño, pero suponemos se crearan unidades operativas compuestas por profesionales en la materia y que su reclutamiento se hará de manera similar a como se procede con los especialistas (así se los denomina a los médicos, abogados, etc., que ingresan a las FF.AA y como reconocimiento a su nivel académico se les otorga el grado de teniente), que luego de realizar el respectivo curso de militarización,

consideramos deben pertenecer al Arma de Inteligencia, que tendrá que desarrollar subespecialidades en el campo.

Si algún organismo de seguridad ecuatoriano cometió la ingenuidad de adquirir hardware y software de encriptación e inteligencia de los EE.UU o de algunos de sus aliados, en especial de la OTAN, debe desecharlo.

Pero limitarnos a pensar en desarrollar nuestra ciberdefensa es insuficiente, hoy las TICs son parte sistémica de la sociedad actual y la economía no puede funcionar sin redes de comunicación, por lo que es necesario avanzar en una estructura tecnológica que nos garantice seguridad integral. El gran reto es lograr verdadera soberanía en materia de TICs, entendida ésta no como autocracia técnica ya que las vinculaciones son inevitables, sino como el desarrollo de políticas, regulaciones y estrategias lo suficientemente robustas que permitan el control sobre los aspectos más sensibles del funcionamiento de nuestro Estado, democracia y protección de los ciudadanos, teniendo muy claro la ruta a seguir cuando se trata de proteger los intereses nacionales en materia de independencia tecnológica en el largo plazo.

En política exterior, como ya lo han señalado varios ciberactivistas, se debe persistir hasta que se logre obtener una normativa que permita llevar a la justicia a los Estados que practican la vigilancia masiva, aunque conseguir esto, desde nuestro punto de vista, es poco realista. Por otro lado, toda iniciativa que provenga de los EE.UU o sus aliados debe ser calificada de sospechosa.

En fin, en este campo hay mucho por hacer para lograr soberanía y seguridad nacional en el ciberespacio, el tema no se agota en lo expuesto, lo fundamental es tomar conciencia sobre lo que se tiene que hacer para conseguirlo.

Mario Ramos
Director
Centro Andino de Estudios Estratégicos
14/septiembre /2014

Bibliografía:

- CLARKE, Richard A. - KNAKE, Robert K.; *Guerra en la red – Los nuevos campos de batalla*, editorial Ariel, Barcelona, 2011, pp. 367

Documentos:

- Centro Andino de Estudios Estratégicos; *Es necesaria una Revolución Militar Integral en Nuestra América*, Mario Ramos, 18 de junio del 2013, pp. 20

- Instituto Español de Estudios Estratégicos; documento marco: *Los problemas estructurales en el planteamiento de la ciberseguridad*, Luis de Salvador Carrasco, 09/2014, pp. 29

Del Internet:

- BURCH, Sally; *Retos de la era digital para América Latina y el Caribe*, 29 de agosto de 2014, www.alainet.org.

- GINES, Armando; *Big data, la vigilancia perfecta*, 23 de agosto de 2014, www.rebelion.org.