Escenarios Actuales, año 29, septiembre Nº 2 (2024), pp. 33-38
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Ciberseguridad, desde la óptica de los efectos, la gobernanza y las alianzas, en procura de alcanzar la soberanía digital

Dahir E. Ahmed Guzmán[1]

Resumen

El devenir tecnológico vinculado a la ciberseguridad es vertiginoso, lo que obliga a los Estados a buscar la soberanía digital, debiendo desarrollar una gobernanza específica, tomar decisiones y generar alianzas. Esto sucede muchas veces con una visión eminentemente técnica, sin considerar otros factores que tienen un alto impacto y consecuencias para la sociedad.

Abstract

The technological evolution linked to cybersecurity is dizzying, which forces States to achieve digital sovereignty, having to develop specific governance, make decisions and generate alliances, the above often only with an eminently technical vision, not considering other factors that they have a high impact and consequences for society.

Palabras clave
Ciberseguridad pública
El fecto
Presupuesto fiscal
Rango etario y soberanía digital

Keywords
Public cybersecurity
Effects
Fiscal budget
Age range and digital sovereignty

Introducción

Se abordará esta temática con la intención de reflexionar sobre diferentes aspectos, que están más allá de las capacidades y variables técnicas relacionadas con la ciberseguridad. El desafío que se presenta es analizar y discutir sobre lo que denominaremos "*todo lo demás*", de lo cual no se habla ni discute mucho, pero que tiene un

1 General de Brigada (R), Licenciado y Magíster en Ciencias Militares de la Academia de Guerra del Ejército de Chile, Oficial de Estado Mayor del Ejército y de la Fuerza Aérea de Chile, Profesor de Academia en las asignaturas de Historia Militar, Estrategia e Inteligencia. Posee experiencia profesional en los ámbitos de docencia de nivel superior en Inteligencia, Telecomunicaciones, Fuerzas Especiales, Operaciones de Paz de Naciones Unidas y Diplomacia Militar, graduado del Curso Senior de Seguridad Nacional e Internacional en la Escuela de Gobierno J. F. Kennedy School, Universidad de Harvard, EE.UU. de A. dahirahmedg@gmail.com.

alto impacto en alcanzar el nivel de desarrollo y consolidar los servicios confiables que la ciudadanía demanda respecto de la ciberseguridad en un Estado.

Esta reflexión se orientará a los efectos que busca alcanzar un Estado en el entorno internacional y a la tecnología por asumir, también en la flexibilidad presupuestaria estatal, en el impacto en la academia y en la importancia del rango etario, todas ellas como variables de interés relacionadas, en procura de alcanzar el máximo grado bajo el concepto de la soberanía digital.[2]

Los efectos que busca un Estado

¿Para qué un Estado invierte en ciberseguridad? Sin duda esta es la pregunta directriz de la presente reflexión. La Real Academia Española de la Lengua nos ilustra sobre el concepto de *efecto* como sigue:

- Fin para que se hace algo.
- Finalidad, fin, intención, objetivo, meta, objeto, propósito, motivo, corolario.

Un Estado buscará consolidar competencias como la resiliencia, la independencia, la vanguardia, y la capacidad de defenderse y atacar cibernéticamente, lo que le permitirá generar un grado de disuasión cibernética creíble ante posibles amenazas.

Se requiere lograr y consolidar una comunión que logre generar una relación de apoyo mutuo entre lo público y lo privado, siendo fundamental que actores como el Parlamento, los tribunales de justicia, las universidades, el Ministerio de Relaciones Exteriores y su cuerpo diplomático, los ministerios de Ciencia y Tecnología, de Transporte y Telecomunicaciones, asuman que todos ellos son entes relevantes y que deben estar presentes en esta discusión con una mirada enfocada en los intereses del Estado, al corto, mediano y largo plazo.

En lo relacionado a la resiliencia ante un ambiente cada día más hostil, con ciberataques permanentes e instantáneos, sobre los que algunos se logran defender y otros no, ambas experiencias (públicos y privados), sin duda, entregan valiosas lecciones aprendidas que podrían ser muy bien aprovechadas, permitiendo sumar esfuerzos, generar sinergia, mejorar y reducir los riesgos y amenazas, fortaleciendo con ello la continuidad operacional de los diversos sistemas informáticos.

Surge, entonces, la necesidad de avanzar, aunque sea de manera limitada, en cierta independencia tecnológica, que busque obtener una libertad de acción como Estado. Para progresar en ese propósito, la variable clave es la investigación y desarrollo, donde la academia tiene un rol fundamental en la formación de mejores investigadores, desarrolladores e integradores de tecnología, con el fin de estar a la vanguardia del conocimiento.

Todo lo señalado implica un costo humano y económico que debe ser comprendido, mensurado y asumido por los actores públicos y privados. Sin inversión ni asignación de presupuestos y sin recurso humano calificado no hay viabilidad de mejora.

2 *Soberanía digital* se refiere al control y la capacidad de los países y sus ciudadanos para ejercer su autonomía y toma de decisiones en el ámbito digital. Esto incluye el control sobre los recursos digitales, la infraestructura, los datos, las aplicaciones y los servicios que se utilizan en el país.

En el sistema internacional, todo Estado posee una estatura político estratégica que, mediante la disuasión y otros elementos del poder, contribuye a identificarlo en una posición determinada. Si se generan las condiciones para poseer capacidades de defensa y ataque cybernético, se incrementará su estatura, lo que le permitirá consolidar a su vez las condiciones para generar efectos e influencia, con la intención última de disuadir a diferentes actores y amenazas en este nuevo dominio de batalla como es el ciberespacio.

El naciente y cada día más necesario concepto de *ciberseguridad pública*, que la ciudadanía demandará en forma creciente, junto a una larga lista de otras solicitudes en este ámbito, se suma a un ambiente no físico que podría accionar sobre el normal desarrollo de los Estados y ciudades, afectando a la sociedad en forma transversal.

Los Estados deben poseer una gobernanza robusta enmarcada en una legislación actualizada que regule este ámbito tecnológico. El marco legal y reglamentario que se genere debe ser el adecuado para propiciar las condiciones que permitan robustecer la ciberseguridad. En este sentido, el Parlamento debiese contar con muy buenos asesores, idóneos, imparciales y transparentes en estas temáticas, a objeto de redactar las mejores leyes que la sociedad requiera.

Al mismo tiempo, el Estado debiera crear tribunales dedicados al ciber crimen, con magistrados y fiscales expertos, que entiendan y dominen la temática tecnológica, a objeto de perseguir y sancionar a ciberdelincuentes, en los tiempos razonables que la ciudadanía exige.

La policía también debiese poseer una capacidad humana-técnica adecuada y los conocimientos actualizados, sumado a los recursos suficientes para poder investigar en un ámbito con una demanda de crecimiento constante.

Los voceros de gobierno, en todos los niveles, deben estar preparados para transmitir mensajes a la opinión pública y ciudadanía que den cuenta sobre las amenazas a la ciberseguridad que nos están afectando como sociedad, y debe generar tranquilidad y confianza en las instituciones que lidean con este ambiente no físico.

El entorno internacional y la tecnología a asumir

Un dilema vigente para muchos Estados que no poseen independencia tecnológica, es resolver la disyuntiva sobre cuál tecnología asumir: la proveniente de Oriente u Occidente, siendo válida la interrogante sobre si se podrán utilizar ambas en forma simultánea. La experiencia comparada de convivir con dos ecosistemas digitales señala que esto último es difícil de llevar a la práctica.

Lo anterior nos conduce hacia la encrucijada –cercana o lejana en el tiempo, pero en cada segundo más urgente– sobre la decisión que deberán asumir los Estados, desde una perspectiva realista del mundo, respecto de si están dispuestos a asumir los efectos de las presiones internacionales, que podrían ser de tipo estatal, privadas o una mezcla de ambas, con la particularidad que dichas presiones se orientarán hacia ámbitos no ligados directamente al entorno tecnológico.

Los desafíos más urgentes serán identificar cuáles áreas podrían verse afectadas y tomar acciones remediales con anticipación, que minimicen el impacto negativo. Sin embargo, no todo será desfavorable, también se abrirán oportunidades

para el Estado ante tan importante y trascendental elección.

Bajo estas premisas, sin duda, el quehacer de las Relaciones Exteriores del Estado no serán las mismas, debiendo analizar con quién o quiénes suscribir alianzas de cooperación tecnológica, las que podrían ser vinculantes a la decisión final sobre el origen de la tecnología a escoger. Como una solución a corto plazo, se propone contar en las embajadas con la figura de agregados tecnológicos, que deberán aportar con valiosa, actualizada y oportuna información sobre buenas prácticas, identificación de amenazas y, principalmente, oportunidades para el Estado.

En este sentido, Chile ya ha dado un paso inicial e importante, ya que el 30 de enero del 2023, el Gobierno designó a tres agregados en tecnología a las embajadas de Chile en Alemania, Australia y Estados Unidos de América.[3]

La flexibilidad presupuestaria del Estado

Las actualizaciones de tecnología no tienen fecha ni hora de aviso, llegan de improviso y , por lo general, con una urgencia que condiciona la seguridad operacional de los sistemas informáticos. Dichas actualizaciones muchas veces son de elevado valor, el que lógicamente no fue considerado en el presupuesto formulado con un año de anticipación.

En el mismo tenor, aun en el supuesto de que la organización pública posea holguras presupuestarias, la autorización para hacer cambios de ítems muchas veces es lenta y requiere fundamentar la necesidad y la urgencia del cambio ante el ente estatal que dirige, controla y asigna los presupuestos fiscales, lo que exige tiempos excesivos de análisis para recibir una respuesta, idealmente positiva. Lo anterior no se condice con los tiempos de respuesta que demanda la ciberseguridad para reducir el impacto que los ataques informáticos producen al funcionamiento de los organismos del Estado y también al mundo privado, siendo prioritario proteger la infraestructura crítica del país.

Este panorama, que es transversal en muchos países y en la totalidad de sus organismos públicos, pone en una encrucijada a los jefes de servicio, ya que la flexibilidad de la regla fiscal para la formulación y ejecución del gasto, en lo que se refiere a los presupuestos fiscales, es muy estricta. Esto no facilita una adecuada y oportuna respuesta ante lo que llamaremos *emergencias de ciberseguridad*, lo que vulnera gravemente la ciberseguridad y la continuidad operacional.

La academia

El mundo académico también tiene mucho que aportar en estas temáticas, ya que su opinión es fundamental para que el Estado resuelva sobre el origen de la tecnología por adoptan. Una vez resuelta la decisión, deberá estar en condiciones de enseñar a los futuros profesionales y técnicos que operarán los sistemas informáticos, debiendo adecuar las mallas curriculares, los contenidos asociados y la infraestructura.

3 MINISTERIO DE RELACIONES EXTERIORES DE CHILE. 30 de enero 2023. [En línea]. Disponible en: https://www.minrel.gob.cl/noticias-anteriores/presidente-gabriel-boric-designa-agregadurias-en-tecnologia-inversion

También es importante incrementar la participación en eventos nacionales e internacionales, tales como congresos, foros y seminarios, y en publicaciones y coinvestigaciones, que busquen fortalecer la relación de la academia con los entes públicos y privados, así como fomentar el aumento de especialistas en ciberseguridad, dado que la demanda de sus competencias se incrementa en forma exponencial.

El rango etario

Este punto es transversal a todo lo anterior, puesto que la edad incide en el entendimiento de temas de ciberseguridad.

El desafío de lograr conectar a personas nativas digitales con no nativos digitales es prioritario. Por lo general, la juventud se encontrará a la vanguardia del conocimiento en estas materias, pero los tomadores de decisiones a nivel público y privado, los que votan las leyes, los que administran justicia, los que conducen políticamente a un Estado, no lo son en su mayoría, lo que dificulta la comprensión de los problemas, las urgencias y las oportunidades que la tecnología adecuada a un momento preciso ofrece.

Como una solución a corto plazo se propone crear una nueva carrera profesional, la de "traductores tecnológicos". Estas personas cumpliran la función de facilitar la comunicación entre ambos mundos, los nativos y los no nativos digitales, considerando el cambio vertiginoso de la tecnología, que deja las capacidades y conceptos rápidamente obsoletos, dificultando el entendimiento mutuo entre actores relevantes.

Reflexiones finales

El desafío que la ciberseguridad nos impone es romper el paradigma y lograr transitar del concepto de gasto al de inversión en tecnología, lo que reconoce un grado de madurez sobre la importancia de la tecnología, el rol que cumple y la criticidad de la misma.

Se debe reconocer que la decisión que se tome sobre la tecnología a implementar, sea de Oriente u Occidente, será de largo plazo, considerando a los múltiples actores públicos y privados que deberán asumir el impacto de esta decisión.

Se debe identificar con base en equipos multidisciplinarios, no solo tecnológicos, cuáles serán las áreas afectadas y, de esta forma, generar medidas que mitiguen el impacto. Además, se debe identificar tempranamente las oportunidades a objeto de masificar y multiplicar el impacto positivo que tendrá en la sociedad.

El concepto de *soberanía digital* deber ser incorporado en todos los espacios de reflexión y discusión a nivel nacional, ya que, al ser intangible, se tiende a olvidar su existencia y se minimiza su importancia.

Finalmente, la nueva interrogante que dejó la discusión es: ¿la elección sobre cuál tecnología asumir será solamente tecnológica?, al parecer "todo lo demás" tiene mucho que opinar.

Bibliografía

Diccionario Real Academia Española, definición de efecto, [en línea] [consulta 24-08-2024].

Disponible en: https://www.rae.es/diccionario-estudiante/efecto

FOETRA, Sindicato de las Telecomunicaciones de Argentina. [en línea] [consulta 10-09-2024]. Disponible en: https://www.foetra.org.ar/sitio/soberania-digital-soberania-de-datos/

MINISTERIO DE RELACIONES EXTERIORES DE CHILE. [en línea] [consulta 06-09-2024]. Disponible en: https://www.minrel.gob.cl/noticias-anteriores/presidente-gabriel-boric-designa-agregadurias-en-tecnologia-inversion