Revista de Administración Pública

INAP

Introducción

El presente número de la Revista de Administración Pública es producto de una invitación del Dr. Carlos Reta Martínez, Presidente del INAP, quien ha tenido la visión de observar que la Ciberseguridad es un tema emergente con múltiples ángulos relevantes para la Administración Pública, Siguiendo su gentil invitación a coordinar esta edición, tanto el Instituto como este autor hicimos amplia convocatoria a autores y temas, con el resultado que hoy ponemos en manos de los lectores.

La ciberseguridad, como se discute en los artículos aquí contenidos, es un tema emergente, sujeto a vaivenes de atención, nomenclatura y enfoques, y que a través de ellps va estableciendo algunos paradigmas, al menos en la escala de una década, a la vez que se renueva constantemente. Tema multidisciplinario por excelencia, nuestra fortuna en esta convocatoria nos ha atraído autores expertos –no hablo acerca de mí– y dotados de una profunda visión ética y pragmática a la vez. Las vidas profesionales de nuestras autoras y autores se han enriquecido con sus actividades tanto académicas como profesionales, con intercambios de ideas vigorosos y actuaciones públicas en cargos de decisión sujetos a fuertes presiones. Su reflexión nutrida por la multidisciplina nos deja un panorama amplio y variado. Sin duda habrá otras perspectivas y experiencias que tomar en cuenta, que exceden la capacidad de este volumen, y serán bienvenidas hacia el futuro, pero no me cabe duda de que les debemos ya una visión panorámica de gran riqueza.

La convocatoria, como lo reflejan los artículos aquí contenidos, solicitó a los autores escribir sobre ciberseguridad en tanto ciberseguridad nacional. En el trabajo de coordinación y en la revisión editorial se contempló la diversidad de definiciones existentes para ciberseguridad y los conceptos relacionados, atendiendo a la perspectiva de los autores, pidiendo siempre observar el objetivo a tratar: la ciberseguridad nacional. Las esferas de la seguridad informática –personal, pública– se intersectan con la seguridad nacional y así han sido contempladas.

Jimena Moreno, Mercedes Albornoz y Solange Maqueo nos ofrecen una revisión comparada de la cuestión de ciberseguridad en los países de América Latina, sobre todo desde el punto de vista de la legislación y la práctica legal, complementada con observaciones sobre la práctica gubernamental. Esta visión comparativa de una realidad rápidamente cambiante será de utilidad para quienes estudian y responden a iniciativas de ley y proyectos de regulación, tanto como para quienes deben buscar los marcos legales para la acción en el ámbito operativo.

Mario Vignettes estudia la esfera ética del ciberconflicto. A partir de una revisión de los marcos relevantes en el pensamiento ético, permite alimentar el análisis y la toma de decisiones en diversas posiciones, como la preventiva, la defensiva y la ofensiva, en el conflicto en el ciberespacio. Conviene recordar que el conflicto en el ciberespacio no se restringe exclusivamente a este ámbito virtual; los actores del ciberconflicto son seres humanos y sus organizaciones, y las consecuencias del ciberconflicto se traducen, al menos potencialmente, en daños o defensa a las personas y sus activos físicos. El texto de Vignettes deberá ser estudiado por años como un marco para el pensamiento, la planeación y la acción en este campo.

María José Rodríguez extrae de su profundo conocimiento y experiencia un análisis sólido de la intersección entre ciberseguridad, a nivel nacional, e inteligencia. A partir del reconocimiento de la inteligencia como una necesidad vital de los Estados y un recorrido por los desafíos del ciberespacio a la seguridad nacional, revisa documentos y estrategias en la intersección de ciberseguridad nacional e inteligencia en varios países, incluyendo la Estrategia Nacional de Ciberseguridad de México. Concluye con un

planteamiento que debe ser tomado en cuenta por el Estado mexicano hacia el futuro.

Anahiby Becerril revisa también los ámbitos de intersección de ciberseguridad y seguridad nacional, a partir de una llamada de atención sobre la vitalidad y actualidad de los riesgos originados en el ciberespacio. De forma sistemática recorre los tipos de armas y ataques cibernéticos y ubica como especial foco de atención la guerra informacional. Una revisión del estado del arte de algunas defensas, entre ellas las basadas en técnicas de Inteligencia artificial, lleva a un llamado –en el que coinciden casi todas las contribuciones de esta colección– a que el Estado mexicano propicie la investigación en ciencia y tecnología conducentes a mejores capacidades de defensa del interés nacional.

Rafael Espinosa y Guillermo Morales revisan la situación de seguridad de la información en las instituciones de educación superior en México. Estas instituciones han sido y seguirán siendo nodales para la seguridad informática en todos sus niveles; fueron las primeras en contar con recursos computacionales y de red abiertos al mundo y por ello las primeras en recibir ataques informáticos, y en formar organizaciones y recursos humanos competentes para enfrentarlos exitosamente. El desarrollo de capacidades, que va más allá de las competencias técnicas de los individuos y debe llevar a un ecosistema robusto de ciberseguridad, pasa inexorablemente por las universidades. Futuras estrategias de ciberseguridad harán bien –y más: deberán– acercarse nuevamente a estas fecundas raíces.

Salvador Camacho nos abre a perspectivas recientes en el uso del sistema de nombres de dominio de Internet (DNS) como vehículo y objetivo de ataques lesivos a la ciberseguridad nacional, y a técnicas –entre ellas algunas basadas en tecnologías *Blockchain*– para dar seguridad al DNS sin interferir en el activo comercio y uso de los nombres de dominio. El artículo orienta al impacto en seguridad nacional a futuro para México y –él también– llama a fortalecer el desarrollo tecnológico y el de capacidades.

Salvador Venegas toma uno de los temas de mayor visión a futuro en ciberseguridad: la computación cuántica. Esta disciplina, que ve días de febril desarrollo ahora y hacia el futuro, puede permitir formas inéditas e insospechadas de

protección de la información mediante criptografía cuántica y, del otro lado de la moneda, puede proveer a los atacantes de una capacidad de descifrado de esquemas criptográficos que puede derrotar a cualquier defensa no cuántica. Si bien la computación cuántica enfrenta todavía desafíos formidables –es posible lograr coherencia con números muy pequeños de *qubits*– el desarrollo de su ciencia y de la tecnología en tanto software y simulaciones de dispositivos es rico y prometedor. Como otras disciplinas basadas en software, enfrenta barreras de entrada mucho menores que la producción de dispositivos y debe ser abordada de manera decisiva. Su dependencia de una formación matemática sólida y actual exige la formación de personal y laboratorios que, si se inician a tiempo y en la escala adecuada, y con apoyo suficiente, ágil y oportuno, puede proveer una envolvente avanzada a la estrategia nacional en materia de ciberseguridad, tanto al sector público como al privado, y a su colaboración. Hacerlo tendrá un costo relativamente bajo y sobre todo muy inferior al de no hacerlo.

Carlos Estrada Nava presenta y justifica la necesidad de establecer un atlas de riesgos de ciberseguridad para México, como una tarea de gran escala a la vez que urgente. Para ello provee taxonomías útiles e información actualizada del entorno geopolítico de la ciberseguridad, y un inventario de los grandes pasos hacia una estrategia de ciberseguridad que se han presentado en el país, así como de iniciativas recientes propuestas en el ámbito legislativo. Sin duda habrá controversias sobre algunos de los conceptos expresados por el autor, como en todos los demás artículos, las cuales serán bienvenidas para dar madurez al debate público informado en esta crucial materia.

Fátima Cambronero aborda un tema crucial para la ciberseguridad nacional: absorber eficazmente las lecciones aprendidas en más de veinte años de evolución y práctica de la gobernanza de Internet mediante mecanismos, acuerdos e instituciones multisectoriales o "multistakeholder", que no están maniatadas por las restricciones del esquema multilateral o intergubernamental propio de las relaciones internacionales (y lo complementan con agilidad, relevancia, y participación de los actores relevantes en formas eficaces). Formula convincentemente la tesis de que las decisiones

y acciones de carácter estratégico en ciberseguridad, en particular la nacional, sólo podrán alcanzar la eficacia y la capacidad de respuesta que el entorno cambiante exige si son multisectoriales y estructuradas en forma que pueda producir los resultados deseados.

Finalmente, en el artículo de quien suscribe esta introducción, Alejandro Pisanty, se discuten aspectos problemáticos de la definición de ciberseguridad y de su intersección con la seguridad nacional. El énfasis en entender las conexiones con el delito cibernético y la actividad de actores subnacionales y no nacionales conduce a una discusión de los regímenes aplicables, multilateral, multistakeholder, y un híbrido o régimen ecléctico vigente en la actualidad al que se propone reconocer en su naturaleza específica. El artículo termina con un análisis de los juegos que las potencias juegan para apalancar su acción entre regímenes y llama al Estado mexicano a hacer conciencia de éstos y operar en función de ese conocimiento en beneficio del interés nacional.

Agradezco al INAP y en particular al Dr. Carlos Reta Martínez la invitación, a la que ha sido una gratísima tarea de coordinar el presente número de la RAP. Que me fuera planteado el reto de contribuir de esta manera a la magna tarea del INAP ha sido singularmente honroso. También han sido invaluables las discusiones con algunos de los autores y autoras. La Facultad de Química de la UNAM, mi alma mater y lugar-ancla, a través de su Departamento de Física y Química Teórica, otorgó incondicionalmente su apoyo a la realización de este proyecto; llegue a él mi agradecimiento a través de nuestro Jefe de Departamento el Dr. Jesús Hernández Trujillo. Un agradecimiento a los revisores de los artículos, contribución insustituible. A cada una y uno de las autoras y autores mi reconocimiento y agradecimiento por la calidad profesional y humana, la dedicación, la paciencia y el brillante resultado de sus trabajos.

Alejandro Pisanty
Director del Número 148 de la RAP