LA CIBERSEGURIDAD: UN DESAFÍO ESTRATÉGICO, TAREA DE TODOS

Discurso del Director Ejecutivo de CEDESTRA, Vicealmirante (R.) José Luis Fernández Morales, en el marco de seminario desarrollado en conjunto con DUOC UC, sede Valparaíso.

Distinguidas autoridades institucionales y académicas, estimados integrantes de DUOC UC, de la Armada de Chile, invitados especiales y público interesado en la Ciberseguridad, muchas gracias por acompañarnos en el desarrollo de este seminario.

El flujo de la información ha acompañado a la humanidad desde sus orígenes. Primero en los círculos íntimos, luego en los espacios públicos de las polis griegas y, más tarde, en los grandes imperios de la antigüedad.

La historia nos demuestra que la comunicación siempre ha sido vital para el progreso humano, y hoy, en plena era digital y bajo el impacto acelerado de la inteligencia artificial, su influencia es más decisiva que nunca.

Dimensionar este momento histórico no es sencillo. Quizás la forma más clara de comprenderlo sea observar los hitos que nos han traído hasta aquí: pasamos de soportes físicos como cartas, libros y diarios, a un escenario dominado por la comunicación digital, en el que por primera vez -como nos advierte Noah Harari- agentes no humanos producen, interpretan e incluso seleccionan la información que consumimos en nuestras redes sociales.

En este tránsito, la información dejó de residir exclusivamente en medios físicos o en nuestros computadores para alojarse en las llamadas nubes digitales. Espacios que ofrecen enormes ventajas, pero que también abren nuevas vulnerabilidades. Hablamos no solo de redes sociales o archivos institucionales, sino también de los datos que permiten el funcionamiento de la infraestructura crítica de un país: desde sistemas eléctricos y de agua potable, hasta puertos y aeropuertos.

> *"…Mención especial merecen los cables submarinos, sin los cuales la World Wide Web, tal como la conocemos y usamos, simplemente, no existiría…"*

Mención especial merecen los cables submarinos, sin los cuales la World Wide Web, tal como la conocemos y usamos, simplemente, no existiría.

Las redes de información, sin embargo, no solo han facilitado la cooperación, sino también la

confrontación. La historia de los conflictos lo demuestra, y hoy somos testigos de un mundo más tensionado, con disputas geopolíticas que evocan la lógica de una nueva Guerra Fría. Un escenario que amenaza con fragmentar la globalización, situando la tecnología en el centro de la competencia entre potencias.

En la guerra de agresión de Rusia a Ucrania, por ejemplo, hemos visto cómo los drones aéreos y marítimos han transformado la forma de combatir, y cómo los ciberataques y la desinformación se convirtieron en armas decisivas. Desde el año 2022, las ofensivas digitales han golpeado redes energéticas, sistemas de comunicación e instituciones gubernamentales, acompañadas de campañas masivas de propaganda. Frente a la agresión digital rusa, Kiev movilizó su "Ejército Tecnológico", una milicia de voluntarios que lanza ataques disruptivos, recopila inteligencia y combate la desinformación mediante el Centro para la Lucha contra la Desinformación. A su vez, las alianzas con la OTAN, la Unión Europea y empresas como Microsoft y Google han fortalecido la detección de amenazas y la resiliencia de las infraestructuras críticas.

En este terreno, la línea entre la paz y el conflicto es difusa: un solo actor entrenado, armado apenas con un computador, puede desestabilizar a una organización completa.

De allí que la ciberseguridad sea hoy un imperativo estratégico. La *realpolitik* -aquella basada en criterios pragmáticos al margen de ideologías- ha regresado, pero con un agravante: muchas veces la amenaza es anónima, imposible de atribuir con certeza, lo que abre un espacio asimétrico a favor del agresor.

Conviene subrayar -con énfasis- que la ciberseguridad no es un asunto reservado únicamente a escenarios bélicos ni a la confrontación entre potencias. Su impacto es cotidiano y directo: está presente en la protección de nuestras cuentas bancarias y de nuestros datos personales, en la continuidad de los servicios básicos que usamos a diario, en la confianza de las transacciones digitales de las empresas, e incluso, en la credibilidad de nuestras instituciones democráticas. Cada ataque informático, cada filtración de datos o campaña de desinformación, erosiona la confianza social y puede generar consecuencias tan graves como las de una agresión militar. Por eso, la ciberseguridad debe entenderse como un bien público, inseparable del desarrollo económico, de la seguridad ciudadana y de la vida democrática de un país.

Para Chile, resguardar la soberanía digital -esto es, la capacidad de actuar y decidir autónomamente en el espacio digital- exige un rol activo del Estado, pero también la participación de toda la sociedad. Empresas, academia y ciudadanía deben sumar esfuerzos para enfrentar una tarea que es nacional.

Nuestra Política Nacional de Ciberseguridad 2023–2028 reconoce déficits claros: baja resiliencia de las organizaciones, insuficiente cultura digital, escasez de especialistas, limitada sofisticación de la demanda y aumento del ciberdelito. Sin embargo, también hemos avanzado: Chile ocupa hoy el lugar 19 en el *National Cyber Security Index*, liderando en América Latina. Hemos fortalecido la acción de los Equipos de Respuesta a Incidentes de Seguridad Informática públicos y privados, y en esta jornada, hemos escuchado a destacados especialistas exponer sobre la importancia de la ciberseguridad y los desafíos que plantea la inteligencia artificial en este ámbito.

No podría no referirme a la ciberseguridad en el ámbito marítimo. La Organización Marítima Internacional ha dado pasos relevantes al

establecer directrices sobre la gestión de riesgos cibernéticos, integrándolos al Código Internacional de Gestión de la Seguridad. Esto significa que, al igual que la seguridad operacional de los buques, la ciberseguridad debe ser gestionada de manera sistemática y verificable. La razón es evidente: los sistemas de navegación, la gestión de carga y las operaciones portuarias están hoy casi completamente digitalizados, y un ataque puede paralizar rutas comerciales enteras o afectar la seguridad de la vida humana en el mar. Basta recordar el ataque global de 2017 contra la naviera Maersk, que detuvo terminales portuarios en distintos continentes y generó pérdidas globales millonarias. Por ello, asegurar un transporte marítimo seguro, protegido y resiliente frente a amenazas cibernéticas no es solo una preocupación técnica, sino un asunto estratégico de alcance mundial.

Todo esto nos lleva a una conclusión clara: enfrentar los grandes desafíos de la ciberseguridad exige planificación estratégica en todos los niveles. Desde las empresas hasta la academia, desde los Estados hasta los organismos internacionales. Requiere, además, desarrollar capacidades concretas, y -como lo ha intentado este seminario- despertar vocaciones que fortalezcan nuestro capital humano.

En definitiva, la ciberseguridad ya no es solo un asunto técnico: es un componente central de nuestra seguridad nacional y de nuestra soberanía. Y su resguardo, como hemos podido reflexionar juntos durante esta jornada, es una tarea colectiva, ineludible y urgente.

Al finalizar este seminario: Ciberseguridad, desafío estratégico, tarea de todos, me hago un deber agradecer a los distinguidos expositores que hoy nos han ilustrado con sus claras e interesantes ponencias. Vaya para cada uno de ellos nuestros sinceros agradecimientos.

Y, finalmente, agradecer a las diferentes personas que lo han hecho posible. La ardua labor de planificación, organización y coordinación desplegada por integrantes del DUOC UC Sede Valparaíso y el Centro de Estudios Estratégicos de la Armada para dar vida a este seminario, han puesto de manifiesto que la cooperación institucional, en materias tan sensibles como la ciberseguridad, es un hecho cuando existe voluntad y unidad de objetivo.

Muchas gracias.