INFORME DE DEFENSA NACIONAL, recaído en el proyecto de ley, en primer trámite constitucional, que instituye el mes de noviembre como el Mes Nacional de la Infraestructura Crítica y su Resiliencia.

BOLETÍN Nº 14.732-02.

Objetivo(s) / Constancias / Normas de Quórum Especial / Consulta Excma. Corte Suprema / Asistencia / Antecedentes de Hecho / Aspectos Centrales del Debate / Discusión en General y en Particular / Votación en General y en Particular / Texto / Acordado / Resumen Ejecutivo.

HONORABLE SENADO:

La Comisión de Defensa Nacional tiene el honor de informar la proposición de ley individualizada en el rubro, iniciada en moción del Senador señor Kenneth Pugh Olavarría, de las Senadoras señoras Carmen Gloria Aravena Acuña y Ximena Rincón González y de los Senadores señores Pedro Araya Guerrero y Álvaro Elizalde Soto.

De acuerdo a lo dispuesto en el artículo 127 del Reglamento de la Corporación, por tratarse de una iniciativa de artículo único, la Comisión la discutió en general y en particular, y resolvió, unánimemente, proponer a la Sala que sea considerada del mismo modo. Asimismo, cabe consignar que este proyecto resultó aprobado en general y en particular por unanimidad (5x0).

\- - -

OBJETIVO DEL PROYECTO

Instituir noviembre de cada año como el Mes Nacional de la Infraestructura Crítica y su Resiliencia, para generar el conocimiento sobre la necesidad de fortalecer sus capacidades y seguridad.

\- - -

CONSTANCIAS

- Normas de quórum especial: No tiene.

- Consulta a la Excma. Corte Suprema: No hubo.

\- - -

ASISTENCIA

- Representantes del Ejecutivo e invitados: no hubo.

- Otros: no hubo.

- - -

ANTECEDENTES DE HECHO

Moción de los Honorables Senadores señor Kenneth Pugh, señoras Carmen Gloria Aravena y Ximena Rincón y señores Pedro Araya y Álvaro Elizalde.

Los autores de la moción que da origen a esta proposición de ley recuerdan que la Política de Ciberdefensa de Chile, publicada en de marzo de 2018, define a las Infraestructuras Críticas de la Información (ICI) como “las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado.”.

Connotan que las referidas infraestructuras han cobrado especial importancia a partir del creciente uso de las tecnologías de la información, del desarrollo de la digitalización y frente al aumento de fenómenos meteorológicos extremos. Aseguran que lo anterior implica un desafío para la seguridad de los países, en orden a resguardarlas para el mantenimiento de prestaciones sociales básicas o esenciales, que se encuentran expuestas a vulneraciones que pueden producir graves afectaciones a la seguridad, la salud o la convivencia social de la población.

Agregan que la Política Nacional de Ciberseguridad, de abril de 2017, por su lado, considera dentro de los objetivos a alcanzar para el año 2022, contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos, incorporando para ello la protección de dichas infraestructuras, la identificación y jerarquización de las mismas, la existencia de equipos de respuesta a incidentes de ciberseguridad, la implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes, como también la evaluación de sus riesgos y la gestión de acuerdo a estándares que contemplen la confidencialidad, integridad y disponibilidad de la ICI, junto con la prevención, manejo y recuperación de ciberataques y otros

incidentes de seguridad informática, y planes de contingencia para asegurar la continuidad operativa de sus servicios.

Juzgan que lo anterior requiere, sin duda, un impulso desde el propio Estado, el que ha elevado la importancia de esta materia a la categoría de defensa de la soberanía del país. Así, precisan, lo establece la referida Política de Ciberdefensa al declarar, en su introducción, que ella complementa la de Ciberseguridad en aquellos aspectos relacionados directamente con la defensa de la soberanía del país, a través de las redes digitales, con la protección de la infraestructura crítica de información y con la de los derechos humanos de todas las personas que habitan en el territorio. Además, prosiguen, reafirma dicho concepto al referirse a la aplicación de las políticas de la Defensa Nacional al ciberespacio, señalando que “el Estado de Chile protegerá su infraestructura crítica de la información, ejerciendo su soberanía sobre aquellas redes y recursos digitales, y que la Defensa Nacional se ocupará de identificar la ocurrencia de ataques, facilitar o permitir su correcta atribución a otros Estados o grupos no estatales, aplicar las contramedidas adecuadas, y dar cumplimiento a la obligación internacional de identificar y detener los ataques que otros países puedan realizar a través de su infraestructura de información.”.

Advierten que de la misma forma en que la ciberseguridad requiere del fomento y desarrollo tanto de una cultura asociada a ella, como de una industria que sirva a sus objetivos estratégicos, la protección de la Infraestructura Crítica de la Información y su Resiliencia demanda un constante ejercicio en torno a la educación, buenas prácticas, responsabilidad, prevención y generación de capacidades de respuesta ante situaciones adversas que permitan la continuidad de los servicios esenciales para el bienestar y la seguridad de la ciudadanía. En este punto, hacen presente que, como prueba de ello, los países que han logrado estándares aceptables en el desarrollo de esta materia, contemplan dentro de su Sistema Nacional de Ciberseguridad una institucionalidad adecuada a dichos fines, siendo este el caso del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) de España.

Relatan que en la experiencia comparada se han adoptado sucesivas y continuas medidas en orden a incorporar y mantener la protección de la infraestructura crítica como una prioridad estratégica. Ejemplo de ello, puntualizan, fue la proclamación en Estados Unidos, el pasado 29 de octubre de 2021, del mes noviembre como el Mes de la Seguridad de la Infraestructura Crítica y su Resiliencia. Acotan que en dicha ocasión se hizo un llamado a la ciudadanía para que reconozca la importancia de proteger la infraestructura de la nación y destine ese mes a observar las medidas apropiadas para mejorar la seguridad y resiliencia nacional.

Indican que el mismo espíritu se encuentra contenido en los principios que invoca la Agencia de Seguridad de Infraestructura y

Ciberseguridad estadounidense (CISA), al señalar que “cada noviembre se celebra como el Mes de la Seguridad de la Infraestructura (…) es el esfuerzo anual de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) para educar e involucrar a todos los niveles de gobierno, propietarios y operadores de infraestructura (…) sobre el papel vital que desempeña la infraestructura crítica en el bienestar de la nación y por qué es importante fortalecer su seguridad y resiliencia.”.

Consideran que contar con un mes en el que se concentren los esfuerzos en orden a concientizar en esta materia, es una instancia que otorga la oportunidad de dar a conocer los recursos y las medidas claves que pueden adoptar las organizaciones y la ciudadanía, además de las iniciativas que influyen en el futuro de la seguridad y la resiliencia de las infraestructuras críticas, incluyendo la nueva legislación, la política y la doctrina.

Remarcan que los beneficios de dicho ejercicio alcanzan ámbitos tan importantes y sensibles como (i) el compartir información sobre las mejores prácticas, realizar evaluaciones para identificar las vulnerabilidades, crear asociaciones en la comunidad de infraestructuras críticas, ofrecer formación y proporcionar herramientas a las partes interesadas en las infraestructuras críticas; (ii) contribuir a la seguridad de la democracia mediante la creación de una mayor resiliencia en el proceso electoral, y (iii) reconocer la experiencia y las capacidades únicas de los sectores gubernamental, privado y sin fines de lucro e integrarlos en el esfuerzo nacional para aumentar la resiliencia de las infraestructuras críticas del país, entre otros.

Afirman que en Chile se ha abierto y destinado un espacio para la promoción y realización de ejercicios nacionales en materia de ciberseguridad, mediante la dictación de la ley N° 21.113, que declaró el mes de octubre de cada año como el "Mes Nacional de la Ciberseguridad", de octubre del año 2018, completando a la fecha cuatro versiones en que se ha puesto de relieve la importancia en la concientización de dicha materia y su desarrollo en el país.

Asimismo, sostienen que la protección y resguardo de la Infraestructura Crítica es también objeto de algunos proyectos de ley que actualmente se encuentran en tramitación en el Congreso Nacional.

En la misma línea, destacan la dictación de la ley N° 20.478, de 2010, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones, que incorporó a la ley N° 18.168, General de Telecomunicaciones, un Título VIII, “De las Infraestructuras Críticas de Telecomunicaciones”.

Reconocen que, si bien dichos hitos constituyen avances, Chile requiere ser un actor y no un mero espectador en esta materia, generando las condiciones y las instancias necesarias para fomentar y ampliar el ámbito de interés hacia una cultura de protección de las ICI que permita lograr estándares

adecuados de desarrollo, seguridad y resiliencia de las mismas. A mayor abundamiento, reiteran que las infraestructuras críticas de la información proporcionan servicios esenciales que la ciudadanía utiliza a diario, y en la actualidad se constituyen como uno de los pilares de la seguridad institucional y social de los países.

En atención a lo expuesto, concluyen que el presente proyecto de ley propone instituir al mes de noviembre de cada año, como el “Mes Nacional de la Infraestructura Crítica y su Resiliencia”, proveyendo así de un periodo de tiempo adecuado, para efectuar actividades de concientización, compartir información, realizar ejercicios nacionales, participar en asociaciones, fomentar la cooperación, difundir conocimiento, generar el encuentro de los diferentes actores nacionales, tanto públicos como privados involucrados en el desarrollo de esta materia, y mantener la periodicidad para enfrentar de forma coordinada y actualizada las múltiples amenazas que afectan a la Infraestructura Crítica, que requieren de a lo menos una instancia anual para comprobar las capacidades y los avances logrados en el país.

- - -

ASPECTOS CENTRALES DEL DEBATE

Las infraestructuras críticas son soportes estratégicos cuyo funcionamiento es indispensable y no permite soluciones alternativas. Por consiguiente, su perturbación o destrucción supone un grave impacto sobre los servicios esenciales.

A la luz de lo expuesto, contar con un mes dedicado adquirir conciencia respecto a la importancia de ellas, su protección y resiliencia constituye un fundamental primer paso.

Conforme a los datos proporcionados en la sesión dedicada al estudio de esta iniciativa de ley, España -modelo que siempre debiera tenerse a la vista en materia de ciberseguridad- cuenta, desde abril del año 2011, con una ley que establece medidas para su resguardo. Chile, por su parte, diez años después, aún no posee con un cuerpo normativo sobre el particular.

Estados Unidos, en tanto, tras recibir, el 7 de mayo de 2021, uno de los ataques ransomware más grandes y paralizantes a una infraestructura crítica -el que recayó en el oleoducto Colonial Pipeline, limitando el 43% del combustible de la costa este y afectando instantáneamente a más de 50 millones de personas- dedica noviembre de cada año a ellas, fomentando el desarrollo de acciones concretas para enfrentar posibles agresiones.

Chile posee áreas especialmente críticas, siendo éste el caso del sector minero y del de la salmonicultura. En efecto, su afectación podría

comprometer el trabajo de 70.000 personas. El sistema electoral, a su turno, es también parte de estos pilares estratégicos que merecen protección y cuidado.

De aprobarse esta proposición de ley, Chile será el primer país-después de Estados Unidos- en declarar un mes para centrar la atención en las infraestructuras críticas y su resiliencia, permitiendo anticiparse a eventos que las impacten.

Los miembros de la Comisión estuvieron contestes en la importancia de respaldar esta iniciativa legal. Sin embargo, advirtieron que el texto presentado a tramitación no señala un organismo coordinador de las actividades que se desarrollarán en dicha oportunidad. A juicio de uno de sus autores, la justificación de tal ausencia radica en que de lo contrario se arriesgaría su declaración de inadmisibilidad, por ser ello una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República.

A fin de evitar que esta futura ley se transforme en una mera declaración de buenas intenciones, los integrantes de esta instancia legislativa propusieron que el proyecto que crea la Agencia Nacional de Ciberseguridad contemple como función de esta entidad la gestión de las acciones necesarias para este mes, así como aquellas que derivan de la ley N° 21.113.

- - -

DISCUSIÓN EN GENERAL Y EN PARTICULAR[1]

A.- Presentación del proyecto de ley por parte del Honorable Senador señor Pugh y debate preliminar en la Comisión.

Comenzando el análisis la iniciativa de ley en estudio, **el Honorable Senador señor Pugh** estimó que resulta indispensable tener un mes dedicado adquirir conciencia respecto a la importancia de la infraestructura crítica, su protección y resiliencia.

Consignado lo anterior, puso de relieve que España -modelo que siempre debiera tenerse a la vista en materia de ciberseguridad- cuenta, desde abril del año 2011, con una ley que establece medidas para la protección de las infraestructuras críticas. Connotó que Chile, por su parte, diez años después, aún no posee con un cuerpo normativo sobre el particular, pese a la importancia que reviste esta materia.

---

[1]A continuación figura el link de la sesión que la Comisión dedicó al estudio de esta iniciativa de ley (11 de enero de 2022): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-01-11/122253.html

Explicó que, conforme a la legislación referida, las infraestructuras críticas se definen como “las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.”.

Agregó que en dicho modelo diversas Secretarías de Estado se vinculan a ellas y se verían afectadas en caso de ataque. Entre ellas, puntualizó, se encuentran el Ministerio del Medio Ambiente y Medio Rural y Marino y el Ministerio de Sanidad, Política Social e Igualdad. Así, alertó, se trata de un asunto interministerial.

En sintonía con lo anterior, afirmó que existen dos conceptos que destacan en las infraestructuras críticas; a saber, la dependencia y la interdependencia. Así, ahondó, es posible advertir si se toma como ejemplo una casa. Ella, prosiguió, se alimenta de electricidad, servicio provisto en la Región de Valparaíso por Chilquinta, de propiedad de State Grid, empresa china, y de agua, otorgada por Esval, cuyos propietarios son canadienses. Estas dos dependencias, destacó, son esenciales para su funcionamiento.

Expresó que la interdependencia, en tanto, es aquella que se produce con un tercero y permite que otras infraestructuras operen adecuadamente. Tal es el caso, puntualizó, del transporte eléctrico a través de Transelec.

Los conceptos indicados, continuó, son parte de un fenómeno que debe entenderse adecuadamente, porque puede ocurrir que el lugar más débil no sea el que se piensa. En efecto, profundizó, muchas veces se cree que debe protegerse la gran infraestructura y no un nodo central de distribución, el que puede ser el causante de una catástrofe mayor.

Por otro lado, previno que todos los sistemas, además, recogen datos de las personas. En consecuencia, sentenció, no sólo resulta necesario proteger las infraestructuras críticas, sino también estos últimos, y apuntó que todos los actores involucrados debieran contribuir en ello.

Juzgó que el escenario expuesto se complica aún más en un mundo totalmente conectado y digitalizado. Al respecto, recordó que el 16 de diciembre del año 2021, se lanzó la red 5G, lo que hará que todas estas infraestructuras críticas se conecten. Algunas, notó, con tecnologías de alta generación, pero otras lo harán con tecnología antigua, sin sistema seguro y sin encriptación, lo que generará altos grados de vulnerabilidad. Planteó que lo señalado anteriormente permite concluir que los riesgos tanto para las personas como para las infraestructuras se incrementarán exponencialmente en el ciberespacio.

Postuló que, de todas las infraestructuras, la más crítica es la de la información, y destacó que en tal situación se encuentra el cable de fibra óptica de 13.180 kilómetros que unirá Valparaíso con Sydney, Australia.

Aseguró que la pregunta que surge al respecto es quién cuidará estas infraestructuras críticas submarinas. Sobre el particular, consideró que tal labor corresponderá al Ministerio de Defensa Nacional, el que deberá tener la capacidad de custodiar todos estos elementos que son indispensables para el quehacer del país.

Presentando el modelo británico, comentó que en él toda la inteligencia que se hace en el ciberespacio está dirigida por la Cancillería, de la cual depende el Servicio de Inteligencia Secreto (MI6) y la Inteligencia Técnica (GCHQ). Sin embargo, aclaró, la protección física corresponde a Home Office, Cartera de Estado equivalente al Ministerio del Interior y Seguridad Pública, el que cuenta con un organismo que se ocupa de la seguridad interior (Security Service).

Informó que la protección de la infraestructura crítica en el ciberespacio es tarea del Centro Nacional de Ciberseguridad, mas la protección física y la integración corresponden al Centro de Protección de Infraestructura Crítica. Adicionalmente, hizo presente que el sistema de inteligencia es el encargado de dar las alertas de estos sistemas. En este punto, recordó que Chile tramita un proyecto de ley de inteligencia que se hace cargo de la infraestructura crítica (Boletín N° 13.086-07). Ello, remarcó, será algo que deberá tenerse en cuenta en el mes cuya creación se propone.

Resaltó que el modelo expuesto permite entender que la protección de la infraestructura crítica supone dos dimensiones: la física y la del ciberespacio.

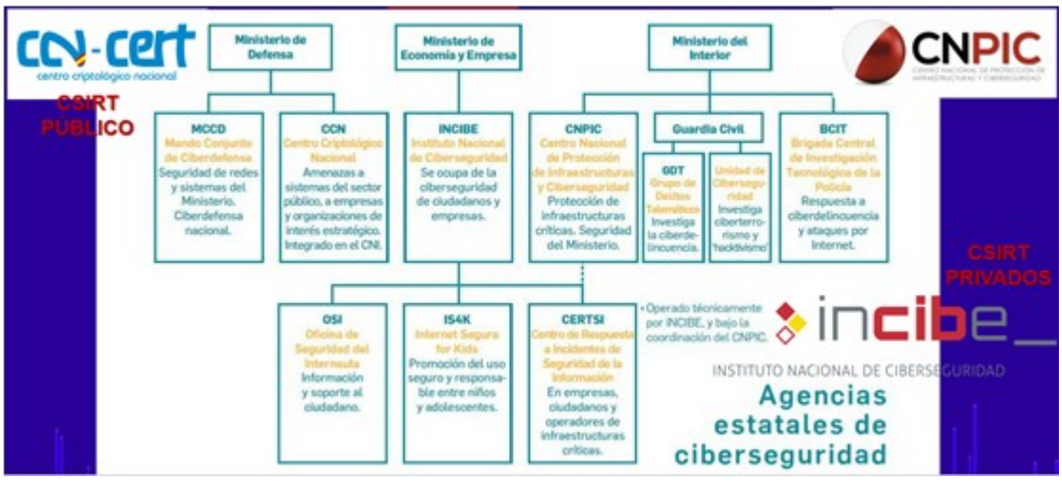
Continuando con la exposición del modelo británico, relató que las infraestructuras críticas deben reportar cualquier incidente dentro de un plazo acotado, el que no puede superar las 72 horas.

Fijando su atención en el Centro de Ciberseguridad Nacional, puso de manifiesto que éste se compone tanto por miembros del sector público y como del privado, y consideró que tal diseño debiera tenerse a la vista a la hora de incorporar soluciones en la legislación nacional.

Adentrándose en el modelo español, destacó que, en él, la protección de la infraestructura crítica posee una organización especial, a través del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Sin embargo, precisó, también presenta un componente digital.

Notó que en el CNPIC se desempeñan 54 personas, de las cuales veintisiete provienen de la policía nacional y las veintisiete restantes, de Carabineros, aportando ambas instituciones de igual manera.

Indicó que los ministerios que intervienen son los siguientes:



Acotó que en el Ministerio de Defensa está el ámbito de inteligencia, mientras que en el Ministerio de Económica, la protección digital de las infraestructuras críticas; ello, arguyó, porque gran parte de ellas son operadas por el mundo privado.

Agregó que el Instituto Nacional de Ciberseguridad (Incibe) monitorea toda la infraestructura crítica privada. Resaltó, además, que la protección de la infraestructura crítica privada no depende directamente del Estado, sino que es subcontratada.

Fijando su atención en la institucionalidad nacional, subrayó que Chile aún no tiene un marco jurídico de ciberseguridad. Aseguró que resulta indispensable que éste se base en un sistema nacional de interoperabilidad; que se avance en la tramitación del proyecto de ley sobre protección de datos personales (Boletín N° 11.092-07); que se genere la legislación necesaria para proteger la infraestructura crítica de la información; que se dé paso a una cultura de ciberseguridad y crear una ley marco de gobernanza y ciberseguridad.

Destacó que el modelo planteado se complementa con ley N° 19.223, que tipifica figuras penales relativas a la informática, la ley N° 19.628, sobre protección de la vida privada, y la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad. De esta manera, detalló, el modelo quedaría como se aprecia en el gráfico que sigue:



Agregó que el escenario anterior se complementará con el Sistema Nacional de Ciberseguridad, el que estará compuesto de la Agencia Nacional de Ciberseguridad, del Instituto Nacional de Ciberseguridad y del Centro de Protección de Infraestructura Crítica. Ahondando en este último, estimó que debiera considerar la integración adecuada para hacerse cargo tanto de los aspectos físicos como virtuales.

En línea con lo anterior, recordó que Su Excelencia el Presidente de la República anunció, en su última cuenta pública del estado administrativo y político de la Nación ante el Congreso Pleno, la creación de la Agencia Nacional de Ciberseguridad, y anheló que dicha proposición legal ingresara prontamente a tramitación.

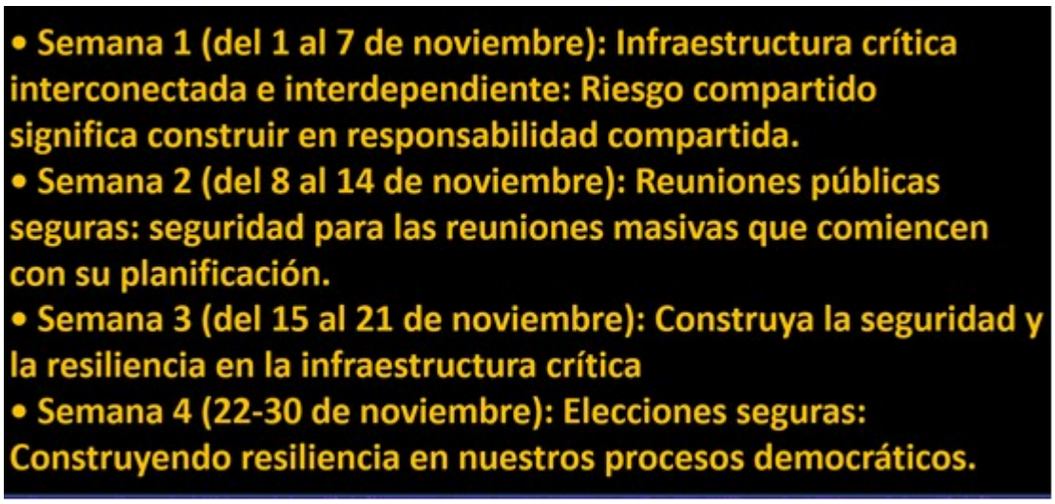
En otro orden de ideas, relató que el 7 de mayo de 2021, ocurrió en los Estados Unidos uno de los ataques ransomware más grandes y paralizantes a una infraestructura crítica, el que recayó en el oleoducto Colonial Pipeline, limitando el 43% del combustible de la costa este y afectando instantáneamente a más de 50 millones de personas. Aseveró que tal ataque obligó a una pronta resiliencia por parte de la empresa afectada.

Remarcó que el 25 de agosto del mismo año, el Presidente de Estados Unidos, Joe Biden, convocó a todos los expertos en la materia, especialmente a los representantes de las grandes empresas que mueven los datos: Apple, IBM y Google.

Connotó, asimismo, que el día 25 de octubre del mismo año, la Casa Blanca creo una unidad especializada para enfrentar este tipo de amenazas.

Adicionalmente, enfatizó, el 29 de octubre, el Primer Mandatario de dicho país dictó una orden ejecutiva proclamando el mes de noviembre de cada año como el mes de la infraestructura crítica y su resiliencia, fomentando el desarrollo de acciones concretas para enfrentar este tipo de situaciones.

De esta manera, apreció, el día 1 de noviembre pasado, se dio inicio, en los Estados Unidos, por primera vez, al primer mes destinado a promover estos conceptos. Puntualizó que cada una de las semanas de dicho espacio de tiempo se dedicó a diferentes temas, los que se observan en la imagen siguiente:



Centrando su atención en la tercera semana, llamó a tener en cuenta que en Chile, el sector minero y el de la salmonicultura son áreas especialmente críticas, cuya afectación podría comprometer el trabajo de 70.000 personas.

En relación con las actividades desarrolladas en la última semana, en tanto, subrayó que la democracia y el estado de derecho también están en riesgo en el ciberespacio. Por ello, abogó por entender que el sistema electoral es parte de las infraestructuras críticas que merecen protección y cuidado.

Dando a conocer la propuesta legal, señaló que ésta se basa en un artículo único, cuyo tenor literal es el que sigue:

“Artículo único. – Institúyese el mes de noviembre de cada año, como el “Mes Nacional de la Infraestructura Crítica y su Resiliencia”, con el fin de promover el desarrollo de las capacidades nacionales para fortalecer la seguridad y resiliencia de las infraestructuras críticas.”.

Afirmó que lo anterior supondrá acciones de parte de quienes operan, controlan y hacen uso de referidas infraestructuras.

Finalmente, destacó que, de aprobarse esta ley, Chile será el primer país, después de Estados Unidos, en declarar un mes para la infraestructura crítica y su resiliencia, permitiendo anticiparse a eventos que las afecten.

El Honorable Senador señor Alvarado concordó con el objetivo perseguido por la iniciativa de ley. No obstante, advirtió que la norma propuesta no establece cuál será la autoridad encargada de coordinar las actividades pertinentes a desarrollarse durante el mes de noviembre. Sin ellas, enfatizó, la proposición de ley corre el riesgo de ser una mera declaración de principios.

Por su lado, **el Honorable Senador señor Guillier**, en línea con lo expuesto por el legislador que le precedió en el uso de la palabra, consultó qué actores serán los encargados de ejecutar las acciones necesarias que la creación del mes aludido supone.

A la luz de lo anterior, planteó la necesidad de buscar los mecanismos adecuados para que el proyecto de ley en estudio no se transforme en una mera declaración de buenas intenciones.

Atendiendo las inquietudes de los miembros de la Comisión, **el Honorable Senador señor Pugh** sentenció que establecer un órgano responsable de tales labores en el proyecto de ley arriesgaría su declaración de inadmisibilidad, por ser ello una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo dispuesto en el artículo 65, inciso cuarto, número 2°, de la Constitución Política de la República. Con todo, planteó que el proyecto de ley que crea la Agencia Nacional de Ciberseguridad debiera contemplar como función de este órgano el deber gestionar el desarrollo de las acciones necesarias para el proyecto en estudio, así como aquellas que derivan de la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad.

Por último, **el Presidente de la Comisión, Honorable Senador señor Elizalde** coincidió con el Honorable Senador señor Pugh en que encomendar a algún órgano la función de coordinar las acciones que supondrá instituir el mes de noviembre como mes nacional de la infraestructura crítica y su resiliencia escapa a las atribuciones que poseen los parlamentarios, en atención a lo prescrito en la norma anteriormente mencionada.

En atención a lo expuesto, celebró la propuesta realizada por el mismo señor Senador, en orden a que el proyecto de ley que crea la Agencia Nacional de Ciberseguridad considere como un deber de dicho órgano desarrollar las acciones que derivarán de este mes, así como también aquellas que supone el mes nacional de la ciberseguridad. Puntualizó que para ello habrá que hacerlo presente, en la oportunidad correspondiente, al Ejecutivo para que lo incluya dentro de la citada propuesta legal. Sin un órgano responsable, concluyó, esta futura ley será una mera declaración de principios.

B.-Votación en general y en particular

- Puesto en votación el proyecto de ley, en general y en particular, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Alvarado, Araya, Elizalde, Guillier y Pugh.

- - -

TEXTO DEL PROYECTO

En mérito del acuerdo anterior, la Comisión de Defensa Nacional recomienda a la Sala aprobar el proyecto de ley en informe, tanto en general como en particular, en los siguientes términos:

PROYECTO DE LEY:

"Artículo único. – Institúyese el mes de noviembre de cada año, como el "Mes Nacional de la Infraestructura Crítica y su Resiliencia", con el fin de promover el desarrollo de las capacidades nacionales para fortalecer la seguridad y resiliencia de las infraestructuras críticas.".

- - -

ACORDADO

Acordado en sesión celebrada el día 11 de enero de 2022, con la asistencia de los Honorables Senadores señores Álvaro Elizalde Soto (Presidente), Claudio Alvarado Andrade, Pedro Araya Guerrero, Alejandro Guillier Álvarez y Kenneth Pugh Olavarría.

Valparaíso, a 14 de enero de 2022.

Pilar Silva García de Cortázar
Abogada Secretaria Accidental de la Comisión

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE DEFENSA NACIONAL, RECAÍDO EN EL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, QUE INSTITUYE EL MES DE NOVIEMBRE COMO EL MES NACIONAL DE LA INFRAESTRUCTURA CRÍTICA Y SU RESILIENCIA (BOLETÍN N° 14.732-02)

I. OBJETIVO (S) DEL PROYECTO PROPUESTO POR LA COMISIÓN: Instituir noviembre de cada año como el Mes Nacional de la Infraestructura Crítica y su Resiliencia, para generar el conocimiento sobre la necesidad de fortalecer sus capacidades y seguridad.

II. ACUERDOS: aprobado en general y en particular por unanimidad (5x0), Senadores Alvarado, Araya, Elizalde, Guillier y Pugh.

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: el proyecto consta de un artículo único.

IV. NORMAS DE QUÓRUM ESPECIAL: no tiene.

V. URGENCIA: no tiene.

VI. ORIGEN E INICIATIVA: Senado. Moción del Senador señor Kenneth Pugh, de las Senadoras señoras Carmen Gloria Aravena y Ximena Rincón y de los Senadores señores Pedro Araya y Álvaro Elizalde.

VII TRÁMITE CONSTITUCIONAL: primero.

VIII. INICIO TRAMITACIÓN EN EL SENADO: 6 de diciembre de 2021.

IX. TRÁMITE REGLAMENTARIO: primer informe, en general y en particular.

X. LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: 1.- Ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad. 2.- Ley N° 20.478, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones. 3.- Decreto supremo N° 533, de 2020, que crea el Comité Interministerial sobre Ciberseguridad. 4.- Ley N° 20.424, estatuto orgánico del Ministerio de Defensa Nacional.

Valparaíso, a 14 de enero de 2022.

Pilar Silva García de Cortázar
Abogada Secretaria Accidental de la Comisión