Mesa de trabajo “Ciberdefensa”

Autor
Agesic

Fecha de creación
26/09/2024

Tipo de publicación
Informes

Resumen

Informe del intercambio realizado en la quinta mesa de trabajo “Ciberdefesa" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad del 17 de junio al 21 de junio del 2024.

Participaron representantes de: sector público, sector privado, academia, sociedad civil y organismos internacionales.

Introducción

En el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay, del 17 al 21 de junio de 2024 se realizaron ocho mesas de diálogo para recoger aportes respecto a la propuesta borrador. Participaron diferentes actores de las instituciones públicas, del sector privado, de la sociedad civil y de la academia, con el objetivo de intercambiar ideas que permitan cocrear la ENC. En este espacio, se dialogó acerca del alcance de la Estrategia, los principios, objetivos y acciones específicas a impulsar.

En la jornada del 20 de junio se realizó el análisis del pilar “Ciberdefensa” de la Estrategia, este documento presenta en forma sintética los intercambios en esta mesa.

Participantes

Agesic (Institución pública), Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. Martin Albornoz, Victor Blanco, Joaquín Cabrera, Nicolas Correa, Sebastián Gómez, Pablo Pajon, Natalia Salazar, Gabriel Vidal.

ANCAP (Institución pública), Administración Nacional de Combustibles, Alcoholes y Portland. Osvaldo Barrios, Patricia Marquez.

Armada Nacional de Uruguay (Institución pública), Rubén Botarro, Pablo Santos, Alejandro Vega.

BPS (Institución pública), Banco de Previsión Social. Luis Repetto.

DNA (Institución pública), Dirección Nacional de Aduana. Santiago Manduca, Álvaro Saldarini.

DNSFFAA (Institución pública), Dirección Nacional de Sanidad de las Fuerzas Armadas. Enzo Barreto.

ESMADE (Institución pública), Estado Mayor de la Defensa. Claudio López.

Fuerza Aérea Uruguaya (Institución pública), Marcelo Camacho.

Instituto Antártico Uruguayo (Institución pública), Rafael Fraga.

Instituto Militar de Estudios Superiores (Institución pública), Johnny Da Silva.

LACNIC (Sociedad civil), Registro de Direcciones de Internet para América Latina y el Caribe. Graciela Martínez.

MATRIZ y empresas del Grupo ANCAP (Sector privado), Daniel Perez.

MDN (Institución pública) Ministerio de Defensa Nacional, Rivera Elgue.

MI (Institución pública) Ministerio del Interior, Javier Jaureguiberry.

SIEE (Institución pública), Secretaría de Inteligencia Estratégica de Estado. Jorge Alliaume, Robert Figueroa.

Unidad de Ciberdefensa del Ejército (Institución pública), Pablo Camps, Pedro Gómez, Javier Soria.

UDE (Academia), Universidad de la Empresa. Daniel Jenci.

UDELAR (Academia), Universidad de la República. Alejandro Blanco.

UTE (Institución pública), Administración Nacional de Usinas y Transmisiones Eléctricas. Evelyn Antón.

Resumen del intercambio

A continuación, se presenta el informe general de la mesa de trabajo “Ciberdefensa” donde se encuentran sistematizados y sintetizados los aportes de cada subgrupo. Se mantuvo la estructura estipulada en la agenda de la actividad, que consistió en dos rondas de intercambio.

Sin embargo, esta mesa tuvo un formato diferente al propuesto originalmente: consistió en una primera ronda en común con todos los participantes, donde éstos aportaron observaciones generales y específicas a la Ciberdefensa. En la segunda ronda, las personas participantes se dividieron en subgrupos, para desarrollar sus aportes estratégicos y actividades.

Parte 1. Ronda de intercambio sobre el borrador

En esta primera ronda, todos los participantes en conjunto realizaron aportes sobre el borrador. En la primera parte identificaron aportes generales sobre la propuesta borrador, mientras que en la segunda identificaron aportes específicos para el pilar “Ciberdefensa”.

Parte A. Aportes generales sobre la propuesta borrador.

En esta primera parte, la pregunta disparadora fue: ¿Qué aspectos consideran más relevantes en la propuesta del primer borrador de la Estrategia Nacional de Ciberseguridad para abordar eficientemente retos y desafíos en torno a la Ciberdefensa?

Se parte de la base que se deben buscar soluciones antes de que ocurran los potenciales ataques, y se habla de dos temas principales que deben ser resueltos: la elaboración de un glosario y el desarrollo de la gobernanza.

Glosario

- Se debe definir un vocabulario común sobre ciberseguridad, especialmente en relación con incidentes en infraestructuras críticas. Entre los términos que deben ser claramente definidos se encuentran principalmente “ciberdefensa” y “ciberseguridad”, pero también otros conceptos como “incidentes mayores”, “desastres mayores”.
- Más generalmente se debe elaborar claramente la distinción entre ciberdefensa y ciberseguridad para determinar explícitamente quién tiene cada rol y responsabilidad en estos ámbitos. Por lo tanto, el glosario debe ser el punto de partida
- La definición de infraestructuras críticas e infraestructuras críticas de la información es muy importante para el rol de las Fuerzas Armadas en la ciberdefensa. Como punto de partida, hay que definir el umbral que permitirá saber qué es crítico y qué no. Esto debe ser definido a nivel nacional, no solo en el ámbito de la defensa u otra área específica. Así se marcará un estándar conocido de ciberseguridad que todos podrán cumplir.

Gobernanza

Esto es transversal. Actualmente existen distintos marcos de gobernanza para distintos temas (ciberseguridad, ciberdefensa). Hay que canalizar los esfuerzos a organizar y nuclearlos.

- Se señala que ya se ha desarrollado una cierta cantidad de normativa en ciberdefensa y ciberseguridad, pero también se subrayan las carencias actuales: la falta de un responsable principal y de distribución de responsabilidades, y la falta de implementación de medidas de seguridad.
- Se resalta la necesidad de coordinación entre las infraestructuras críticas: se debe asignar roles y responsabilidades, crear un plan de protección eficaz e implementar mecanismos de control.
- Se debe incluir a todos los actores relevantes (incluyendo a los actores privados).
- Hay que realizar una revisión y evaluación nacional de riesgos, en continuidad con los esfuerzos ya realizados.
- Se subraya la necesidad de criterios de aceptación de niveles mínimos de ciberseguridad en organismos que manejan infraestructuras críticas. El Sistema Nacional de Emergencias (SINAE) podría ser el regulador adecuado.
- También se menciona la necesidad de implementación de medidas preventivas y educativas en el área de la defensa.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

En esta parte, se preguntó a los y las participantes: ¿Qué aspectos específicos de gobernanza creen que podrían mejorarse o añadirse en el pilar “Ciberdefensa”?

Se elaboraron nuevas propuestas respecto a los dos ejes dibujados en la primera ronda (glosario y gobernanza), y también se añadieron dos temas más: la coordinación y la prevención.

Glosario

Al igual que en la primera ronda, se recalcó reiteradas veces la necesidad de un glosario. Se resaltó que es importante desambiguar la información sobre infraestructuras críticas para evitar confusiones, y se propuso retomar los trabajos de definición de infraestructuras críticas de información iniciados en 2014 para evitar errores pasados. Se hizo hincapié en la ausencia de representantes de la gestión de infraestructuras críticas en Uruguay, y la necesidad de que estos expertos definan las infraestructuras críticas, en vez de los directores.

Además, se subrayó que al ser una Estrategia que junta y coordina a diversos órganos estatales, que quizá conciben los conceptos de manera ligeramente diferente, es aún más importante ponerse de acuerdo sobre los términos “ciberseguridad” y “ciberdefensa”.

Respecto a la definición de “incidentes mayores”, es fundamental esclarecer los criterios para definirlos. Se aportó que no deben considerarse solamente los ciberataques, sino también otros ciber-incidentes causados por factores como los desastres naturales. Se propuso tomar como referencia a la normativa de EE.UU. o de la UE en la materia.

Gobernanza

Se destacó la importancia de crear grupos de trabajo para avanzar en la implementación de tácticas, señalando que hasta el momento ha sido difícil definir responsables y llevar las estrategias a la acción. También se propuso que las actividades se podrían llevar a cabo con proyectos puntuales.

Otro aspecto que se destacó como fundamental es la necesidad de identificar todas las organizaciones del Estado que tienen capacidades para responder a incidentes, tanto desde el punto de vista de Recursos Humanos como de recursos materiales. Deben ser agregadas a la Estrategia, y se les debe otorgar responsabilidades. El documento es una estrategia para la cual es importante la participación de todas las fuerzas que están involucradas en el tema de ciberseguridad.

También se propuso determinar los desafíos de seguridad cibernética, y se subrayó que es importante que haya un Observatorio que identifique cuáles son las principales amenazas y cuáles son los principales objetivos para establecer prioridades.

Se resaltó que se deben clarificar las responsabilidades: debe haber un CSO para coordinar los altos cargos y un equipo que esté al tanto de lo que se maneja a nivel nacional sobre las infraestructuras críticas.

Por otro lado, se sostuvo que hay que hacer foco en dos temas importantes para efectivizar la Estrategia: actuar conjuntamente y prevenir.

Coordinación

Se señaló que hay muchos trabajos y esfuerzos hechos por separado, que tienen que nuclearse. Debe haber una institución que nuclee todos esos esfuerzos para elaborar una estrategia. No puede haber políticas únicas para cada organismo, sino que tiene que haber una política nacional: todos los organismos están correlacionados, por lo que si cae uno, cae el resto. Por esta razón es de suma importancia tener una política de colaboración.

Se debería seguir pensando en qué recursos e información se pueden ir compartiendo en los espacios de articulación entre los organismos.

Prevención: formación, capacitación, educación

Respecto a la necesidad de prevención, se señaló que hay un problema de base que es la falta de recursos humanos capacitados. Si falta esto, habrá un problema en la esencia de los sistemas críticos.

Para establecer estándares, es un punto importante que la población esté capacitada.

También es imprescindible la capacitación de los técnicos de todas las infraestructuras críticas. Se destacó la responsabilidad de la academia en la formación de las nuevas generaciones y en establecer estándares más altos. Se identificó una deficiencia en la formación de grado en ciberseguridad.

Se apoyó la iniciativa de una estrategia general, que no se empantane en lo puntual. El compromiso tiene que ser su ejecución: hay que estar listos para un ataque. El gran mensaje fue pasar a la acción.

Parte 2. Aportes estratégicos, priorización e identificación de actores para el pilar de la mesa

La segunda parte del intercambio se dividió en tres partes centradas en aportes estratégicos que incluían plantear objetivos, proponer actividades específicas y analizar su viabilidad.

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

En esta parte las personas participantes discutieron acerca de los objetivos planteados en el pilar "Ciberdefensa".

Antes de pasar a los objetivos propiamente dichos, se sugirió realizar cambios a los dos párrafos que aparecen como preámbulo del pilar de Ciberdefensa.

Párrafo 1

Se propusieron algunas modificaciones en la redacción:

- Eliminar "Como ya ha ocurrido en países de nuestra región", ya que no aporta nada al pilar o a la ENC en general.
- Cambiar "grupos cibercriminales" por "actores del ciberespacio".
- Eliminar "coordinada".
- Terminar el párrafo en "la sociedad en su conjunto", eliminando "como consecuencia de una acción coordinada, ejecutada por grupos cibercriminales". Otros cambios propuestos agregarían en su lugar, luego de "la sociedad en su conjunto": "como consecuencia de una acción, ejecutada por actores del ciberespacio".

Además de estos cambios sintácticos, se sugirió agregar algunas aclaraciones:

- Se debe definir "infraestructuras de información crítica": Es importante saber qué se entiende por "infraestructuras de información crítica" mediante una definición única.
- Debe haber mayor claridad en "que afecte a la sociedad en su conjunto": tiene que haber un umbral de impacto para saber cómo definirlo y poder ubicar un límite; se sugieren los siguientes umbrales: medir el impacto en base a un porcentaje de la población, sobre el porcentaje de cierta actividad o servicio esencial, o en base a porcentaje del PBI afectado. A la vez, previo a definir el umbral hay que definir un catálogo de la sociedad, que podría dividirse de forma sectorial.

Párrafo 2

Algunos participantes sugirieron eliminar el segundo párrafo por completo, mientras que otros defendieron su ubicación dentro del preámbulo. Otros propusieron convertirlo en línea de acción, cambiando "escenarios" por "el desarrollo de capacidades".

Definición de nuevo objetivo

Se propuso definir un nuevo objetivo que explore los límites de las acciones de la ciberinteligencia dentro de la ciberdefensa.

Observaciones respecto al Objetivo 1: "Identificar y fortalecer las capacidades nacionales en ciberdefensa"

- Se hizo hincapié en la necesidad de definir "ciberdefensa".
- También se señaló que hay mucho trabajo hecho. Se deben conocer los trabajos que ya están, los antecedentes, y recoger toda la información existente. Ese es el primer paso: identificar cuáles son los medios que contamos para hacer frente a una amenaza, y qué brechas existen.
- A partir de ahí se debe definir un estándar para que todas las organizaciones se entiendan y manejen terminología, lenguajes y estructuras comunes; y definir un conjunto de capacidades mínimas que deben tener los organismos que se van a encargar de la Estrategia y del cumplimiento de las líneas de acción. Se

planteó la necesidad de identificar qué capacidades se necesitan para responder a estas líneas de acción, qué organismos tiene la capacidad para responder y, si no existen, generar esas capacidades.

Observaciones respecto al Objetivo 2: “Incrementar las capacidades de respuesta en ciberdefensa ante incidentes mayores”

- Se mencionó como vital la coordinación entre los organismos públicos, la academia y el sector privado. La mayoría de las infraestructuras críticas están en manos privadas, por lo que tendría que haber parámetros de ciberseguridad con el sector privado, así como medidas de higiene.
- También se mencionó el papel fundamental de la academia en la concientización de la población. Las oportunidades de capacitación deben estar explícitas en la estrategia y ser parte del documento.

Se destacó que no hay que olvidar definir el alcance de los objetivos, así como sus limitantes. Se señaló que otro punto fundamental es que faltan normativas para legislar e implementar estos objetivos.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Las personas participantes aportaron actividades y acciones para el pilar “Ciberdefensa”. Detalladas a continuación se encuentran las actividades pensadas según cada objetivo, y luego acciones propuestas de manera más general.

Líneas de acción del primer objetivo

En la línea de acción iii, se sugirió eliminar el final de la línea de acción para que pase a ser “Implementar ejercicios conjuntos, a nivel nacional”. En caso de permanecer “que reproduzcan eventos mayores de desastres” como final, se recomendó agregar “definidos”

También respecto a esta línea de acción, se subraya que se debería explicitar e implementar tanto en TI como en la parte industrial, donde hay más dificultades en este tema.

Se propone agregar dos nuevas líneas de acción:

- Una que consista en identificar cuál es la capacidad real, actual de ciberdefensa y compararla con lo que se busca a futuro.
- Otra respecto al desarrollo de un glosario de términos referidos a la ciberseguridad y ciberdefensa (se especificó que la ciberseguridad es parte de todo el ecosistema mientras que la ciberdefensa es más específica).

Se debería tomar en cuenta a la inteligencia artificial como factor de desarrollo de capacidades e identificación de amenazas, particularmente en la línea de acción iii, que menciona la capacidad de respuesta ante incidentes.

Líneas de acción del segundo objetivo

En la primera línea de acción hubo un debate sobre si “y/o privadas” debería de eliminarse o no, ya que por un lado el área de la ciberdefensa corresponde a las Fuerzas Armadas, pero por otro lado los privados pueden asistir.

Respecto a la segunda línea de acción (“Desarrollar un plan de respuesta nacional conjunto ante incidentes mayores”), se reiteró que se debe marcar la diferencia entre TI y el sector industrial, que debe estar incluido.

Surgió la idea de crear una tercera línea de acción: “Establecer un protocolo de activación y desactivación de la respuesta de ciberdefensa”, con el fin de definir el inicio y la finalización de la situación de emergencia.

Otras líneas de acción puestas a consideración

Se identificaron nuevas líneas de acción, sin especificar en qué objetivo deberían incorporarse:

- La necesidad de legislar sobre el rol claro que tiene el Ministerio de Defensa en un ciberataque (no queda claro cuál es su responsabilidad y su alcance en la actuación frente a un ciberataque).
- La importancia de generar un órgano de gestión independiente.

Actividades propuestas

- Es necesario hacer una compilación de los distintos documentos respecto a lo que se entiende como infraestructuras críticas, incluyendo en especial lo que se está haciendo en la Secretaría de Inteligencia. Es necesario recopilar la información para no volver a caer en los mismos errores que en el pasado.

- Es importante contar con un glosario. Particularmente, se debe acordar la definición de ciberdefensa y ciberseguridad, así como el ámbito de competencias de cada uno. Se sostuvo que cuando es un evento que se repite debe entrar en el ámbito de defensa nacional.

- Es importante tener claro cuáles son las infraestructuras críticas, armando un listado, así como los criterios para identificar un ataque a una infraestructura técnica y su grado de gravedad (sea por cantidad de personas afectadas o por afectación en el producto bruto interno – aunque se señaló que esto es engañoso, por lo que se debe evaluar el impacto nación más allá del monetario).

- Hay que definir qué grado de involucramiento tiene el Ministerio de Defensa cuando se afectan las infraestructuras críticas. Esto incluye analizar cuáles son los disparadores para que se separe el ámbito civil del militar. En ciberseguridad se abren muchas ramas, por lo que se debe determinar quién tiene que intervenir y en qué casos. Sería necesario contar con un Comité de emergencia en ciberseguridad, que se convoque ante cualquier incidente para definir si es un evento de defensa nacional.

- También se debe decidir qué grado de información se comparte en el caso de un ataque.

- Se necesita un marco legal.

- Se debe continuar con la articulación entre los organismos y crear un grupo de personas capacitadas para que corra la información.

- Se debe concientizar a nivel político del riesgo cibernético y a los responsables de las infraestructuras críticas. También es importante educar a toda la población.

- Los ejercicios de simulacros frente a ataques cibernéticos son muy importantes, tanto en IT como en el sector industrial.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

Las personas participantes realizaron análisis de viabilidad, priorizaron ciertas acciones e identificaron actores relevantes.

La priorización acordada es la siguiente:

- Ante todo, se destacó la importancia de un glosario. Especialmente, se solicitó definir “ciberdefensa” (se planteó referirse a la Ley 18.650, y se hizo hincapié en definir las capacidades de ciberdefensa) y “ciberseguridad”.

- También es de suma importancia identificar el estado actual planteado en las líneas de acción que están propuestas: qué organismos hoy tienen capacidades, cuáles son las acciones, en qué consiste la respuesta. La normativa tiene que ser clara respecto a la definición de los incidentes de ciberdefensa para que el ente autónomo lo reconozca como un ataque, y pueda llamar por ejemplo al SINAE al cual hay que agregarle un área de ciberseguridad/ciberdefensa. El SINAE, que hoy en día no tiene un componente de atención y respuesta ante ciber-emergencias, deberá referirlo a quien corresponda.

Respecto a los actores:

El SINAE debe tener un rol en la determinación de una ciber-emergencia, así como pasa frente a desastres naturales. Debe tener la capacidad de actuar, de reaccionar, de movilizar medios del Estado en respuesta a una ciber-emergencia.

Además, se identificaron como otros actores a incluir a los entes autónomos, especificando que debe haber un responsable en cada uno, y a actores que no han sido mencionados ni participaron en las Mesas de diálogo como OSE y ciertos actores del ámbito privado.

Se propuso que los actores deben coordinarse como en cualquier empresa: el directorio establece las políticas, la gerencia los planes estratégicos y la auditoría interna mira lo que se ha hecho

Anexo

A continuación, se detalla el intercambio realizado y los emergentes surgidos en cada ronda y en cada subgrupo.

- Plenario
- Subgrupo 1
- Subgrupo 2
- Subgrupo 3

Plenario

- Moderadora: Orlando Garcés, OEA.
- Relatora: Olivia Dominguez, Sofía Lopes, Marta Manent, Daniel Miranda, Sabrina Piffaretti, ICD.
- Participaron 33 (treinta y tres) personas de 19 (diecinueve) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Ronda 1. Intercambio sobre el borrador

Parte A. Aportes generales sobre la propuesta borrador

ESMADE (Institución pública) - Claudio López

Abre el diálogo comentando que la Estrategia detalla las líneas a futuro que debemos seguir en materia de ciberseguridad. El esquema concebido fue uno de defensa en profundidad: cuanto más grave la situación que se pueda dar, hay un mecanismo de respuesta nuevo para levantar. Parte de la discusión fue la clasificación de los incidentes según su gravedad. Basándose en la experiencia internacional, se llegó a la conclusión que hoy en día las mayores agresiones del ciberespacio se llevan a cabo con fines financieros, y las víctimas son víctimas colaterales. Sin embargo, si bien no es siempre el caso, esto no quiere decir que no puedan tocar órganos críticos. El incidente ocurrido en Costa Rica, un país parecido a Uruguay, lo demuestra. Es un evento que se separa de la norma: no se buscaba un beneficio financiero, sino que se buscaba el daño, el colapso del país. Los responsables manifestaron que fue una prueba – es decir, se piensa volver a intentar en el futuro. Es nuestro deber, por lo tanto, no tomarlo como un hecho casual que ya pasó; podría pasar algo así en Uruguay. ¿Qué pasaría si, de repente, las infraestructuras críticas caen? No podemos esperar ese momento que ojalá no se presente: debemos pensar soluciones antes.

MDN (Institución pública) - Rivera Elgue

El Subsecretario destaca la necesidad de la iniciativa y enfatiza la importancia de definir claramente términos como amenazas y agresiones, así como implementar medidas preventivas y educativas en la defensa en profundidad. Señala que la mayoría de las infraestructuras críticas en Uruguay son de propiedad estatal, lo cual exige una gran coordinación debido a la autonomía administrativa de estas empresas. Esta situación dificulta la asignación de responsabilidades y la creación de un plan de protección eficaz. Subraya la problemática de la designación de responsabilidades en el país y la necesidad de definir claramente quién se encarga de qué. Menciona al sistema nacional de emergencia como un ejemplo de estructura con distintos niveles de responsabilidad, y señala que el principal obstáculo en la administración de infraestructuras críticas es la falta de control y asignación de responsabilidades. Además, destaca la importancia de incluir a todos los actores relevantes en las discusiones y definiciones, citando la coordinación efectiva durante la pandemia de 2020 como un ejemplo de la importancia de tener un plan nacional con objetivos claros y responsabilidades asignadas.

SIEE (Institución pública) - Jorge Alliaume

Reafirma la importancia de lo mencionado anteriormente, señalando que un estudio de campo comprobó que uno de los principales obstáculos es la falta de un responsable principal para la infraestructura física y la implementación de medidas de seguridad.

ANCAP (Institución pública) - Osvaldo Barrios

Coincide con la necesidad de definir un vocabulario común y claros conceptos sobre ciberseguridad, especialmente en relación con incidentes en infraestructuras críticas. Plantea que un incidente en una infraestructura crítica podría indicar un problema mayor y que es crucial identificar responsables específicos. También subraya la importancia de criterios de aceptación de niveles mínimos de ciberseguridad en organismos que manejan infraestructuras críticas y menciona los esfuerzos de ANCAP en capacitación, destacando la necesidad de equipos multidisciplinarios y técnicos. Propone que el SINAE, debido a su rol en coordinación, podría ser el regulador adecuado. Además, señala que ya hay un trabajo en marcha en ANCAP, incluyendo una revisión y evaluación nacional de riesgos, y enfatiza la necesidad de generar continuidad en estos esfuerzos y la inclusión de actores privados.

Unidad de Ciberdefensa del Ejército (Institución pública) - Pablo Camps

Primero, encuentra crucial definir el término de “ciberdefensa”, ya que hay diferentes concepciones: por un lado, entre el nivel internacional y el nivel nacional; y, por otro lado, dentro de la legislación y la experiencia. Encontrar una definición común es un punto de partida crucial para luego poder definir las responsabilidades de cada uno.

Luego hace un detalle sobre la evolución de la normativa relacionada a la ciberseguridad:

1. Ley Marco de Defensa Nacional (2010): Modernizó el concepto de “Defensa Nacional” e incorporó las actividades civiles dentro de la Defensa Nacional. A la vez, enfoca la defensa nacional al bienestar de la población, aplicándolo, naturalmente, de forma total al ciberespacio.

2. D-CSIRT (2015): A nivel del Ministerio de Defensa, se crea este Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa.

3. Decreto en el ámbito de la Comisión Interministerial de Defensa Nacional, ámbito permanente del CODENA (2018): Trató el tema de la protección de infraestructuras críticas y se incorporó en este concepto de protección la dimensión ciberespacial, destacando la necesidad de no solo proteger la seguridad física, sino también proteger contra el daño en el ciberespacio.

4. Modificación de la Ley Orgánica de las Fuerzas Armadas (2019): Se dio un paso importante en el ciberespacio como un ámbito de soberanía del Estado. Deja de ser una cuestión tratada desde la voluntad para pasar a ser una directiva de comenzar a desarrollar este tipo de capacidades para estar a la altura de la misión. También se impulsa la tarea de participar en la ciberseguridad y la ciberdefensa. Sin embargo, la redacción tiene matices.

5. Aprobación de la propuesta de Política de Defensa Nacional, formulada por el Consejo de Defensa Nacional (CODENA) (2020): Establece directivas para el quinquenio a nivel nacional de seguir con equipos de respuesta y fortalecer el ecosistema de ciberseguridad. Además, en el ámbito del CODENA en coordinación con el SINAE impulsa la evolución y protección natural de las infraestructuras críticas físicas y ciberespaciales, y fomenta al Ministerio de Defensa Nacional a avanzar en la creación de un ámbito conjunto de trabajo y generar capacidades dentro de las Fuerzas Armadas.

Esta evolución representa el rol que tiene la Unidad de Ciberdefensa del Ejército.

La ciberdefensa es una cuestión que puede tener igualdad y correspondencia con el anterior medio físico. Cuenta con diferentes responsabilidades y niveles en que se puede escalar hasta llegar a ser un problema de defensa nacional. Por este motivo, es crucial seguir trabajando en una definición, agregando la dimensión “ciber”.

Entiende que ya hubo una mesa específica de infraestructuras críticas, pero cree que es muy importante para el rol de las Fuerzas Armadas en la ciberdefensa. Como punto de partida, hay que definir el umbral que permitirá saber qué es crítico y qué no. Esto debe ser definido a nivel nacional, no solo en el ámbito de la defensa u otra área específica. Así se marcará un estándar conocido de ciberseguridad que todos podrán cumplir. Por este motivo, la protección de las infraestructuras críticas no es trivial.

Desde la perspectiva de las capacidades de la ciberdefensa, las Fuerzas Armadas están trabajando desde la directiva de 2019 con la Modificación de la Ley Orgánica de las Fuerzas Armadas. Sin embargo, aún hay avances por hacer.

Es fundamental ponerse de acuerdo sobre qué es la ciberdefensa, qué es ciberseguridad, y quién tiene cada rol y responsabilidad en estos ámbitos. La ciberdefensa no es posible si no se conoce qué se debe defender. Ya hay ciertos consensos sobre el tema, pero no se encuentra de forma segura o explícita, por lo que hay que ponerse de acuerdo. Por este motivo reitera que el punto de partida debe de ser el glosario.

Unidad de Ciberdefensa del Ejército (Institución pública) - Pedro Gómez

Recuerda la mesa de infraestructuras críticas, donde se comentó lo que se está haciendo para el desarrollo de las infraestructuras críticas por parte del SINAE en colaboración con Agesic.

Parte B. Aportes específicos sobre el pilar a analizar en la mesa

UDELAR (Academia) - Alejandro Blanco

Está de acuerdo con la necesidad de definir claramente los términos y menciona una deficiencia en la formación de grado en ciberseguridad. Señala que es importante desambiguar la información sobre infraestructuras críticas para evitar confusiones. Propone retomar los trabajos de definición de infraestructuras críticas de información iniciados en 2014 para evitar errores pasados. Destaca la importancia de crear grupos de trabajo para avanzar en la implementación de tácticas y en la práctica, señalando que hasta el momento ha sido difícil definir responsables y llevar las estrategias a la acción y operativa.

MATRIZ y empresas del Grupo ANCAP (Sector privado) - Daniel Perez

Subraya la importancia de que todos los actores trabajen en conjunto, sabiendo de qué se está hablando en este ámbito de la ciberseguridad. Es importante generar una infraestructura de trabajo. Se debería seguir pensando en qué recursos e información se pueden ir compartiendo en los espacios de articulación entre los organismos.

LACNIC (Sociedad civil) - Graciela Martínez

Considera que el documento es una estrategia, para la cual es importante la participación de todas las fuerzas que están involucradas en el tema de ciberseguridad. Se busca alcanzar ciertos objetivos que estén al alcance de todos. Las actividades se podrían llevar a cabo con proyectos puntuales; para eso es importante saber cuáles son las infraestructuras críticas. Se acaba de decir que el ciberespacio es un ámbito de soberanía nacional, lo que cambia mucho la fuerza que debe tener esta estrategia y es muy importante. También hay que definir cuál es el impacto que se produce en la infraestructura crítica para saber cuándo el sistema de emergencia tiene que actuar. Como estrategia general lo planteado está bien, y no hay que empantanarse en situaciones puntuales. Hay que definir bien lo que sería un impacto para una ciberdefensa; es importante a la hora de prepararnos para actuar de forma proactivamente. El compromiso tiene que ser que la política de ciberseguridad se escriba y se ejecute, porque un ataque puede suceder en cualquier momento.

Armada Nacional de Uruguay (Institución pública) - Pablo Santos

Considera que es fundamental ponernos de acuerdo en los términos, principalmente porque, si bien dentro del Ejército se pueden entender porque emplean los mismos términos, están trabajando muchas agencias del Estado. Hay que empezar definiendo los términos “ciberseguridad”, “ciberdefensa”. También cuando se hace referencia a los accidentes mayores, destaca que es fundamental esclarecer los criterios para definirlos.

Otro aspecto que destaca como fundamental es la necesidad de identificar todas las organizaciones del Estado que tienen capacidades para responder a incidentes. Hay muchas organizaciones y agencias del Estado que tienen capacidades tanto desde el punto de vista de Recursos Humanos como de recursos materiales para responder a un ciberataque; deben ser identificados para agregarlos a la Estrategia y otorgarles responsabilidades.

Señala que hay muchos trabajos y esfuerzos hechos por separado, y considera que tienen que nuclearse. Debe haber una institución que nuclee todos esos esfuerzos para elaborar una estrategia.

También propone definir los desafíos de seguridad cibernética, y subraya que es importante que haya un Observatorio que identifique cuáles son las principales amenazas y cuáles son los principales objetivos para poner prioridades.

UDE (Academia) - Daniel Jenci

Comenta que hay dos temas importantes que son: prevenir y actuar conjuntamente. Hay un problema de base que es quiénes construyen y quiénes ejecutan los sistemas de seguridad. Es necesario contar con recursos humanos capacitados, sino habrá un problema en la esencia de los sistemas críticos. Si la población está capacitada es un punto importante para establecer estándares, así como es imprescindible la capacitación de los técnicos a nivel de todas las infraestructuras críticas. Hay responsabilidad de la academia en la formación y en establecer estándares más altos. Es necesario tener sistemas más resistentes.

UTE (Institución pública) - Evelyn Antón

Hace hincapié en la ausencia de representantes de la gestión de infraestructuras críticas de Uruguay, y la necesidad de que estos expertos definan las infraestructuras críticas, no los directores. Subraya la importancia de clarificar las responsabilidades: se debe tener un CSO para coordinar los altos cargos y un equipo que esté al tanto de lo que se maneja a nivel nacional sobre las infraestructuras críticas. A su vez, los organismos deben estar coordinados entre sí; se debe mejorar eso. Además, señala que no solo deben considerarse los ciberataques, sino también otros factores como los desastres naturales y siniestros causados por animales. Agrega que en EE.UU. y en la UE ya existen normas e inventarios definidos para estos escenarios, que se podrían tomar como referencia. Hay que ir más rápido.

DNA (Institución pública) - Álvaro Saldarini

Trae a la mesa el ejemplo mencionado de ciberataque en Costa Rica, que lo vivió de cerca debido a su trabajo en Aduanas y vio así el gravísimo impacto. Además, comenta que durante la pandemia de COVID-19 se agudizaron los intentos de hackear información, porque, a partir de ese momento, la información de las operaciones comenzó a tener un costo; debido a esto, tuvieron que comenzar a tomar medidas y acciones. Sin embargo, la Aduana no debe de tener una política única, sino que tiene que haber una política nacional. Esto se debe a que todos los organismos están correlacionados, por lo que si uno cae, el resto también lo hace. Por tanto, hay que tener una política de colaboración.

Subgrupo 1

- Moderadora: Arianne Palau, Agesic.
- Relatora: Marta Manent, Sabrina Piffaretti, ICD.
- Participaron 9 (nueve) personas de 6 (seis) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Instituto Militar de Estudios Superiores (Institución pública) - Johnny Da Silva

Las líneas de acción del objetivo 1 son “identificar”, “fortalecer” e “implementar”. Sin embargo, partimos de la base entonces de que ya existe una capacidad mínima de ciberdefensa, pero en ningún lado se propone hacer un estudio de cuál es la capacidad de ciberdefensa que tenemos. Quizás falte una línea de acción que consista en identificar cuál es la capacidad real, actual de ciberdefensa respecto a lo que se busca a futuro

UDE (Academia) - Daniel Jenci

A su vez se debe definir un estándar para que todas las organizaciones se entiendan y manejen terminología, lenguajes y estructuras comunes.

Unidad de Ciberdefensa del Ejército (Institución pública) - Pablo Camps

Concuerda con la necesidad de definir “ciberdefensa” para poder hablar de capacidades actuales en ciberdefensa.

Por otro lado, subraya que AGESIC tiene estadísticas y hay mucho trabajo hecho. Se deben conocer los trabajos que ya están, los antecedentes, y recoger toda la información para no repetir el trabajo. Eso es lo primero en la elaboración de la estrategia: identificar cuáles son los medios que contamos para hacer frente a una amenaza.

Con relación a establecer alianzas estratégicas con organizaciones extranjeras, también ya hay varias, tanto bilaterales como multilaterales. En la parte de ciberdefensa hay foros donde se integra eso.

Además, la respuesta es fundamental: si no hay respuesta, los atacantes perseverarán.

UDE (Academia) - Daniel Jenci

Más allá de todo eso, menciona que hay un problema de base: los profesionales que construyen o compran cosas no son conscientes de la seguridad, por lo que no alcanza con capacitar en ciberseguridad. Faltan normativas.

MATRIZ y empresas del Grupo ANCAP (Sector privado) - Daniel Perez

Menciona que la parte de seguridad industrial debería estar incluida en todo esto. Si bien la línea de acción iii del Objetivo 1 (“Implementar ejercicios conjuntos, a nivel nacional, que reproduzcan eventos mayores de desastres”) está mucho más aceitada a nivel de TI, donde hay más iniciativa de llevar a cabo esos ejercicios, en la parte industrial falta sensibilización. Es importante que haya normativas, así como hay obligaciones de hacer simulacros de incendios. Debe haber conciencia de los riesgos. Lo mismo para desarrollar planes de respuesta nacional. Aboga por que se marque esa diferencia entre TI y el sector industrial, que debería estar incluido.

Agesic (Institución pública) - Nicolás Correa

Cree prioritario identificar y establecer una línea de base de la situación actual de la ciberdefensa para poder medir los avances y determinar en qué aspectos hay que trabajar más.

Armada Nacional de Uruguay (Institución pública) - Pablo Santos

Se debe definir un glosario que establezca qué entendemos por los términos más importantes, para hablar todos el mismo idioma sobre ciberseguridad y ciberdefensa.

Armada Nacional de Uruguay (Institución pública) – Alejandro Vega

Propone que se necesita un paso previo a esto; definir un conjunto de capacidades mínimas que deben tener los organismos que se van a encargar de esta estrategia y del cumplimiento de estas líneas de acción.

Armada Nacional de Uruguay (Institución pública) - Pablo Santos

Plantea la necesidad de identificar qué capacidades se necesitan para responder a estas líneas de acción, qué organismos tiene la capacidad para responder y, si no existen, generar esas capacidades. Propone ver todos los

antecedentes en ciberseguridad para no repetirlos. Hay que preguntarse: con qué medios contamos, cuáles son las amenazas, si tenemos estadísticas, y cuáles son los principales ciberataques que se han perpetuado en el país.

Menciona como vital la coordinación entre los organismos públicos, la academia y el sector privado. La mayoría de las infraestructuras críticas están en manos privadas por lo que tendría que haber parámetros de ciberseguridad con el sector privado y la academia, así como medidas de higiene sobre ciberseguridad.

Dice que ya se poseen las capacidades por lo que hay que bajar a tierra esas líneas de acción, determinando quién tiene la responsabilidad de hacerlo. Se deben tomar las líneas de acción y ver cuáles organismos tienen la capacidad para responder, qué es lo que deben hacer (tarea concreta), quién es el responsable y qué recursos se tienen para llevarla adelante. La normativa para legislar esto es otro punto que identifica como clave.

También menciona el papel fundamental de la academia en la concientización de la población. Las oportunidades de capacitación de los recursos deben estar explícitas en la estrategia y ser parte del documento.

Unidad de Ciberdefensa del Ejército (Institución pública) - Javier Soria

Menciona a la inteligencia artificial vinculada a las capacidades y la capacidad de respuesta ante amenazas (automatización de procesos). Aún falta mucho y en tema de capacidades defensivas y ofensivas este fenómeno es clave. Cree que lo estamos viendo de reojo y es algo que incide mucho en el tema de fortalecer las capacidades.

Agesic (Institución pública) - Víctor Blanco

Refiere que no hay que olvidar definir el alcance de los objetivos, así como sus limitantes. Esto lo tiene que hacer cada organismo para ayudar a mitigar cualquier incidente en ciberseguridad.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Las líneas de acción propuestas por la mesa, para complementar las actuales, son:

- Identificar el estado actual de la ciberdefensa.
- Desarrollo de un glosario de términos referidos a la ciberseguridad y ciberdefensa (se especificó que la ciberseguridad es parte de todo el ecosistema mientras que la ciberdefensa es más específica).
- Una vez desarrollado lo anterior, abordar los lineamientos de acción del borrador:
- IA como factor de desarrollo de capacidades e identificación de amenazas.
- Incluir a la seguridad industrial y al personal operativo.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

La priorización acordada es la siguiente:

- Lo primero es tener como punto de partida las definiciones de ciberdefensa y de función de capacidades de ciberdefensa. Se planteó que la pata de ciberdefensa se refiera, como lo establece la Ley 18.650, a la ciberdefensa militar. Se subrayó que todo parte de la ciberseguridad y que todos tenemos que cumplir en nuestros ámbitos, incluso en el ámbito personal, para hacer a toda la red segura.
- Se debe identificar el estado actual planteado en las líneas de acción que están propuestas: quiénes hoy tienen capacidades, cuáles son las acciones, cuáles son los organismos que tienen capacidad, en qué consiste la respuesta. Cuando se habla de respuesta a incidentes hay un matiz a tener en cuenta: el agresor podría ser un Estado. En el mundo físico ya está resuelto, son las Fuerzas Armadas quienes se encargan de eso, por lo que se podría establecer que sea igual en el ámbito ciberespacial, ya que se trata de la protección del ciberespacio como ámbito de la soberanía del Estado.
- Otro punto importante que vino a colación es el tema de la OT, que debe estar incluida en ejercicios y en simulacros.

Además, se identificaron como otros actores a incluir a los entes autónomos, especificando que debe haber un responsable en cada uno.

La normativa tiene que ser clara respecto a la definición de los incidentes de ciberdefensa para que el ente autónomo lo reconozca como un ataque, y pueda llamar por ejemplo al SINAE al cual hay que agregarle un área de ciberseguridad/ciberdefensa. El SINAE, que hoy en día no tiene un componente de atención y respuesta ante

ciber-emergencias, deberá referirlo a quien corresponda.

El SINAE debe tener un rol en lo que es la determinación de una ciberemergencia, así como pasa frente a desastres naturales. Debe tener la capacidad de actuar, de reaccionar, de movilizar medios del Estado en respuesta a una ciber-emergencia.

Subgrupo 2

- Moderadora: Nancy Ibarra, Agesic.
- Relatora: Analía Bettoni, Daniel Miranda, ICD.
- Participaron 10 (diez) personas de 9 (nueve) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Aportes Estratégicos, priorización e identificación de actores para el pilar de la mesa

En este subgrupo, las tres partes de la ronda se desarrollaron en conjunto.

Agesic (Institución pública) - Pablo Pajon

Comenta que las líneas estratégicas son trabajar en la prevención, así como en auditorias integrando a otros organismos que trabajan en ciberseguridad. Es necesaria la prevención para lo cual es importante conocer cuáles son las brechas que tienen los organismos y el país.

MI (Institución pública) - Javier Jaureguiberry

Valida los objetivos de la estrategia. Identifica dos líneas de acción adicionales: la necesidad de legislar sobre el rol claro que tiene el Ministerio de Defensa en un ciberataque y la importancia de generar un órgano de gestión independiente. A la legislación le falta profundizar las potestades del Ministerio de Defensa porque no queda claro cuál es su responsabilidad y su alcance en la actuación frente a un ciberataque.

ANCAP (Institución pública) - Osvaldo Barrios

Subraya que en las líneas de acción es necesario hacer la integración de los distintos documentos respecto a lo que entendemos como infraestructuras críticas, en especial lo que se está haciendo en la Secretaría de Inteligencia.

Es necesario recopilar la información para no volver a pasar por los mismos problemas y situaciones que ya se han tenido.

Es importante acordar lo que entendemos por ciberdefensa y ciberseguridad.

Es importante tener claro cuáles son las infraestructuras críticas, armando un listado, así como los criterios para identificar un ataque a una infraestructura técnica y su grado de gravedad (sea por cantidad de personas afectadas o por afectación en el producto bruto interno). También se debe decidir qué grado de información se comparte en el caso de un ataque. Finalmente, hay que definir qué grado de involucramiento tiene el Ministerio de Defensa cuando se afectan las infraestructuras críticas.

UDELAR (Academia) - Alejandro Blanco

Afirma que hay que definir lo que se entiende por Infraestructura crítica y definir el ámbito (especificar si es solo de información o si también se incluyen activos físicos). También tiene que existir un órgano que articule y dé los lineamientos políticos, y una continuidad al trabajo ya que la experiencia ha demostrado que es necesario que pase por revisiones. Ese órgano debe tener un mecanismo definido para ejercer control y hacer efectivas las propuestas. Sería importante ver que es lo que ya hay hecho. Por ejemplo, ya existe una normativa según la cual todos los organismos deben tener un responsable de seguridad, pero no se cumple en su totalidad. Por más modelos, marcos regulatorios y estándares que se definan, si no tenemos un mecanismo que pueda medir el grado de cumplimiento y lograr hacerlo cumplir, no será efectivo.

También hay que definir la ciberseguridad y la ciberdefensa, que tienen áreas de contacto, y evaluar el alcance de las responsabilidades. El tercer eje es la parte de formación. Sin gente preparada en estos temas, es muy difícil llevar adelante una estrategia y controlarla.

BPS (Institución pública) - Luis Repetto

Destaca que es muy relevante que el Ministerio de Defensa esté en esta reunión.

También resalta que los laboratorios farmacéuticos deberían formar parte de la infraestructura crítica.

Respecto a la responsabilidad, es como en cualquier empresa. El directorio establece las políticas, la gerencia los planes estratégicos y la auditoría interna mira lo que se ha hecho.

SIEE (Institución pública) - Jorge Alliaume

Concuerda con que es necesario identificar la infraestructura crítica, y agrega que se debe concientizar a nivel político del riesgo cibernético y a los responsables de las infraestructuras críticas. Hay otros actores que faltan en esta instancia, como OSE y ciertos actores del ámbito privado.

Hay que trabajar en la parte técnica, pero es necesario también hacer ejercicios de simulacros frente a ataques cibernéticos.

UTE (Institución pública) - Evelyn Antón

Para lograr el cumplimiento del marco de ciberseguridad se debe tener un grado de madurez donde cada uno debe cumplir las normativas, y debe haber un control para que se cumplan. Hay que obligar a nivel normativo a mejorar. Por último, hay que educar a toda la población en ciberseguridad, por ejemplo, a todos los usuarios del Plan Ceibal.

Agesic (Institución pública) - Joaquín Cabrera

Respecto al tema de infraestructura critica, se debe analizar cuáles son los disparadores para que se separe el ámbito civil del militar. En ciberseguridad se abren muchas ramas, por lo que se debe determinar quién tiene que intervenir y en qué casos.

ESMADE (Institución pública) - Claudio López

Hay que publicar inmediatamente el estudio de infraestructuras críticas que ya se ha hecho. En cuanto a definir cuando un evento es ciberseguridad o ciberdefensa, hay que tener en cuenta que cuando es un evento que se repite, ahí entra al ámbito de defensa nacional. El criterio del impacto en el producto bruto interno puede ser engañoso en algunos casos, por lo que es importante evaluar el impacto nación más allá del monetario. Sería necesario contar con un Comité de emergencia en ciberseguridad, que se convoque ante cualquier incidente para definir si es un evento de defensa nacional.

DNSFFAA (Institución pública) - Enzo Barreto

Hace énfasis en que se necesita un marco legal o un punto de dónde partir. Es importante tomar lo que ya está hecho y empezar a trabajar desde eso. Es necesario contar con un glosario y definir conceptos como las infraestructuras críticas. Se debe continuar con la articulación entre los organismos, crear un grupo que entienda del tema y que corra la información.

Subgrupo 3

- Moderadora: Natalia Salazar, Agesic.
- Relatora: Sofía Lopes, Mauro Parada, ICD.
- Participaron 12 (doce) personas de 8 (ocho) Instituciones públicas, Organizaciones de la Sociedad Civil, Academia y/o Sector Privado.

Parte A. Validar los objetivos planteados en el capítulo del pilar de la mesa

Antes de pasar a los objetivos propiamente dichos, se sugirió realizar cambios a los dos párrafos que aparecen como preámbulo del pilar de Ciberdefensa. En general, todos los cambios se decidieron por consenso; en caso de que una propuesta haya causado debate y falta de aprobación por todos o gran parte de los participantes, se detallará.

Párrafo 1

- Eliminar “Como ya ha ocurrido en países de nuestra región”: no les parece que aporte nada al pilar o a la ENC en general.
- Definir “infraestructuras de información crítica”: Es importante saber qué se entiende por “infraestructuras de información crítica” mediante una definición única. No se profundizó en esto porque los participantes de la mesa entendían que el mismo reclamo surgió de la mesa que trató el tema de infraestructuras críticas de forma específica.
- Mayor claridad para “que afecte a la sociedad en su conjunto”: Falta de claridad en el impacto que llevaría a afectar a la sociedad en su conjunto. Se considera que puede haber consecuencias críticas para cierto sector de la sociedad pero no necesariamente representan el conjunto. Tiene que haber un umbral de impacto para saber cómo definirlo y poder ubicar un límite; se sugieren los siguientes umbrales: medir el impacto en base a un porcentaje de la población, sobre el porcentaje de cierta actividad o servicio esencial, o en base a porcentaje del PBI afectado. A la vez, previo a definir el umbral hay que definir un catálogo de la sociedad, que podría dividirse de forma sectorial.
- Cambiar “grupos cibercriminales” por “actores del ciberespacio”:
- Quien tiene responsabilidad sobre las cuestiones criminales es el Ministerio del Interior, por lo que “grupos cibercriminales” acota la posibilidad de que haya otros actores responsables, como Defensa. “Actores del ciberespacio” es más general, pero es fundamental definir las responsabilidades de cada actor para saber cuándo debe de actuar cada uno.
- “Grupos cibercriminales” implica que el crimen siempre se comete por parte de grupos, cuando no siempre es el caso, pudiendo ser un solo individuo o varios individuos no organizados. “Actores del ciberespacio” contempla todo tipo de actores, ya sean grupos o individuos.
- Eliminar “coordinada”: No hay forma de saber si la acción es coordinada; se requeriría de una investigación. Además, la acción puede que no sea voluntaria, dándose como un accidente.
- Terminar el párrafo en “la sociedad en su conjunto”, eliminando “como consecuencia de una acción coordinada, ejecutada por grupos cibercriminales”. Otros cambios propuestos dejarían este último fragmento en “como consecuencia de una acción, ejecutada por actores del ciberespacio”. Se debatió sobre este cambio y no se llegó a un acuerdo:
- Argumentos a favor de que el párrafo termine en “la sociedad en su conjunto”: El final “como consecuencia de una acción, ejecutada por actores del ciberespacio” solo suma la idea de “ciberespacio”, lo cual no convenció de que valiera la pena, ya que lo encuentran repetitivo al entenderse en el marco de la Estrategia en su conjunto. Además, especificar “ciberespacio” podría eliminar cuestiones de ciberdefensa que se mezclan también con el ámbito físico.
- Argumentos a favor de que el párrafo termine en “como consecuencia de una acción, ejecutada por actores del ciberespacio”: “Ciberespacio” tiene que encontrarse escrito de forma explícita, porque, si no se menciona, se pasa al ámbito físico también. Con esta especificación, claramente se entiende que para activar la ciberdefensa, la acción tiene que producirse en el ciberespacio. Vale aclarar que esto no implica que lo físico queda por fuera, porque el impacto puede estar en lo físico o el disparador de la falla puede ser físico; pero sí descarta acciones que existen en lo físico y no son del ciberespacio en absoluto

En suma, en base a las diferentes propuestas, el primer párrafo de Ciberdefensa cambiaría a dos posibles maneras, considerando el último debate:

1. “Nuestro país deberá estar preparado para responder ante un evento de disrupción masiva de sus infraestructuras de información crítica, que afecte a la sociedad en su conjunto.”

2. “Nuestro país deberá estar preparado para responder ante un evento de disrupción masiva de sus infraestructuras de información crítica, que afecte a la sociedad en su conjunto, como consecuencia de una acción, ejecutada por actores del ciberespacio.”

Además de estos cambios al texto, se debe definir las infraestructuras de información crítica, así como el umbral de impacto para que las acciones afecten “a la sociedad en su conjunto”.

Párrafo 2

- Cambiar “escenarios” por “el desarrollo de capacidades”: No se planifica en base a escenarios, sino en base al desarrollo de capacidades. “Escenarios” confunde con un método de planificación estratégica. Por lo tanto, se sugiere cambiar “escenarios” por “el desarrollo de capacidades”. De todas formas, se entiende que es una cuestión de glosario, por lo que si se definiera “escenarios”, podría incluirse.

- Debate sobre la necesidad del segundo párrafo: No se llegó a un acuerdo entre los participantes de la mesa sobre la necesidad del segundo párrafo. Algunos sugieren descartarlo porque creen que se encuentra previsto en las líneas de acción, por lo que se vuelve repetitivo. Otros consideran que es importante que esté, porque funciona como preámbulo a lo que serán las líneas de acción. Otros consideran que debería encontrarse planteado como una línea de acción, en vez de ser parte del preámbulo.

En suma, el segundo párrafo podría eliminarse por completo, o encontrarse dentro del preámbulo o como línea de acción con el cambio de “escenarios” por “el desarrollo de capacidades”.

Objetivos

Definir un nuevo objetivo que explore los límites de las acciones de la ciberinteligencia dentro de la ciberdefensa.

Parte B. Aportes sobre actividades/acciones para el pilar específico de la mesa

Líneas de acción del primer objetivo

En la línea de acción iii. sugieren eliminar el final de la línea de acción para que pase a ser “Implementar ejercicios conjuntos, a nivel nacional”, ya que “que reproduzcan eventos mayores de desastres” lo encuentran redundante.

En caso de permanecer “que reproduzcan eventos mayores de desastres” como final, se recomendó agregar “definidos” luego de “desastres”.

Líneas de acción del segundo objetivo

Surge la idea de crear una tercera línea de acción: “Establecer un protocolo de activación y desactivación de la respuesta de ciberdefensa”. Lo ven necesario para definir el inicio y la finalización de la situación de emergencia.

En la primera línea de acción hubo un debate sobre si “y/o privadas” debería de eliminarse o no:

- Argumentos a favor de eliminar “y/o privadas”: El argumento para esta propuesta fue que la ciberdefensa es una acción militar que está sujeta al Derecho Internacional de los Conflictos Armados, por lo que civiles como privados no pueden tomar este tipo de acciones, ya que está prohibido. Un militar, por motivos de credibilidad del país y legales, está identificado como legítimo para ejercer este tipo de acciones. Los privados y otro tipo de civiles podrían proporcionar sistemas, plataformas y asesoramiento, pero el que concreta la acción debe ser militar.

- Argumentos en contra de eliminar “y/o privadas”: La línea de acción detalla que los privados pueden “asistir”. “Asistir” no necesariamente implica que los privados sean los que ejercen la acción, así violando el Derecho Internacional de los Conflictos Armados, sino que puede significar otras acciones que no son consideradas ilegítimas, como proporcionar sistemas, plataformas y asesoramiento. Por lo tanto, no creen que el problema sea “y/o privadas”, sino que la falta de definición de qué implica “asistir” específicamente para los privados.

Parte C. Analizar viabilidad, priorizar acciones e identificar actores vinculados

Se destacó la importancia de un glosario. Especialmente, se solicitó definir “ciberdefensa” y la soberanía del ciberespacio de Uruguay.