DIPUTADOS
ARGENTINA

La Honorable Cámara de Diputados de la Nación Argentina

RESUELVE:

Solicitar al Poder Ejecutivo Nacional, en los términos del artículo 100 inc. 11 de la Constitución Nacional, que, a través del Ministerio de Defensa, brinde a esta Honorable Cámara de Diputados información precisa y detallada en relación a la designación de un asesor en ciberseguridad del Departamento de Estado de los Estados Unidos de América en el ámbito del Ministerio de Defensa, el Estado Mayor Conjunto, los Estados Mayores Generales de cada fuerza, como así también en los organismos descentralizados, desconcentrados y empresas de la jurisdicción de la Defensa, designación que se desprende de las notas GDE "NO-2024-67875717-APN-SAID#MD" y "NO-2024-85906245-APN-SSC#MD".

Requerimos información minuciosa y con el mayor nivel de detalle en relación a los siguientes puntos:

1. *¿Cuál es el contenido del memorando que celebró el día 25 de marzo de 2024 el Ministro de Defensa Luis Petri con el embajador de los EEUU?*
2. *¿Cuáles son los objetivos generales y específicos que contienen las cláusulas de entendimiento con EEUU?*
3. *¿Qué aspectos específicos de la ciberseguridad se abordan en el memorando mencionado?*
4. *¿A qué actividades se comprometió el Ministerio de Defensa en ese memorando?*
5. *¿Cómo se llevarán a cabo? ¿En qué organismos, unidades, dependencias, empresas del Ministerio de Defensa se realizarán estas actividades?*

6. *¿El asesor en ciberseguridad y ciberdefensa, realizará sus evaluaciones, actividades y propuestas en conjunto con los especialistas en ciberseguridad argentinos?*
7. *¿En el caso que lo haga junto con ellos, qué necesidad encuentra el Ministerio de Defensa de acceder a un analista de otro país?*
8. *¿Considera el Ministerio de Defensa que la jurisdicción no dispone de personal idóneo para diseñar y ejecutar el plan de ciberseguridad/ciberdefensa?*
9. *¿Considera el Ministerio de Defensa que en el país y en particular en la Jurisdicción Defensa, no se cuenta con instituciones que formen adecuadamente recursos humanos en la materia?*
10. *¿Considera el Ministerio de Defensa que las instituciones de formación de las Fuerzas Armadas (Facultad de Ingeniería del Ejercito, Facultad de la Fuerza Aérea, Instituto de Ciberdefensa y otros), no poseen la capacidad de formación necesaria en materia de ciberdefensa, ni aún la Maestría de Ciberdefensa que se dicta en esas instituciones?*
11. *¿Qué intercambio habrá con los analistas argentinos en ciberseguridad?*
12. *¿Este intercambio en forma de memorando es recíproco?*
13. ¿Se evaluaron los riesgos de seguridad al disponer ceder información clasificada en su mayoría, a una nación extranjera?
14. *¿Cómo afecta la injerencia de un analista de ciberseguridad estadounidense en la confidencialidad, seguridad, secretismo y elementos reservados de la información militar?*
15. *¿A qué documentos, software, aplicaciones, bases de datos, listado de personal militar, retirados, pensionistas y agregados en el exterior va a tener acceso el analista propuesto por Estados Unidos?*
16. *¿Cómo se administra la protección de datos sensibles y el ciclo de planeamiento para conservar el secreto militar y la protección de los datos?*
17. *¿Qué relación tiene la asesoría de EE.UU con los lineamientos aprobados en la DPDN, AREMIL, DEMIL y PLANCAMIL, como así también en la elaboración de los planes de campaña y en los lineamientos de ciberdefensa?*
18. *¿Qué organismo, entidad o unidad de auditoría va a controlar el trabajo que realice el analista?*

19. *¿Cómo se alinea este memorando con la estrategia nacional de ciberseguridad de Argentina?*
20. *¿Qué medidas de protección de datos personales de acuerdo a la ley 25.326 va a tomar la República Argentina y el Ministerio de Defensa en relación a la actividad del asesor del Departamento de Estado de EE.UU?*
21. *¿Cómo se asegura que la colaboración con Estados Unidos no comprometa el secreto militar y los elementos confidenciales del Ciclo de Planeamiento de la Defensa?*
22. *¿Cómo puede asegurar el Ministerio de Defensa que los datos y sus sistemas críticos no atraviesen una vulneración por ser revelados o auditados por una potencia extranjera?*
23. *¿Qué intervenciones en hardware, software, telecomunicaciones y datos se realizarán en el marco del citado Memorando?*
24. *¿Cómo piensa el Ministerio de Defensa ordenar la legislación vigente en relación a la seguridad nacional y de datos personales con el trabajo del asesor de Estados Unidos?*
25. *En caso de querer salir de las obligaciones que surgen del Memorando, ¿cómo tienen pensado deshacer lo actuado hasta el momento?*
26. *¿Es posible revertir lo actuado por el asesor en el marco de su intervención en los sistemas informáticos del Ministerio de Defensa?*
27. *¿Por qué razón fueron elegidos los organismos, unidades militares y dependencias públicas que aparecen en la NO-2024-85906245-APN-SSC#MD?*
28. *¿Qué protocolos de seguridad se van a establecer para garantizar que la información sobre nuestras capacidades militares no sea utilizada en el marco de los acuerdos de Estados Unidos con terceros países?*
29. *¿Qué actividades puntuales va a realizar el asesor en cada uno de los organismos?*
30. *En particular en el IAFPRPM, que actividad va a realizar y puntualmente si la misma va a comprometer los datos personales de los retirados y pensionistas militares*
31. *En relación al IAFPRPM, ¿el asesor va a tener acceso a las inversiones que realiza el fondo de capitalización del mencionado organismo previsional?*
32. *¿Qué actividades va a realizar el asesor en el EMCO y los EMGE, EMGA, EMGFA?*

33. *¿En relación al Servicio Meteorológico Nacional, que actividades va a realizar el asesor del Departamento de Estado de EE.UU?*
34. *¿En relación al Instituto Geográfico Nacional, que actividades va a realizar el asesor del Departamento de Estado de EE.UU?*
35. *En relación al IGN, ¿cuál es el interés del Ministerio de Defensa que EE.UU revise y audite los sistemas? ¿Va a tener acceso EE.UU a los mapas y la topografía que realiza el IGN de nuestro territorio?*
36. *¿Qué actividades va a realizar el asesor en Instituto de Investigaciones Científicas y Técnicas para la Defensa - CITEDEF?*
37. *¿Cómo se va a resguardar la información sensible de los proyectos y los prototipos en desarrollo de CITEDEF?*
38. ¿Se tiene conocimiento de que otras naciones de Sudamérica hayan aceptado el mismo tipo de cooperación que está aceptando el Ministerio de Defensa?
39. Se solicita que el Ministerio de Defensa detalle antecedentes y títulos del advisor, informe si es civil o militar, y refiera a qué organismo del gobierno de los EEUU reporta.

Diputado Eduardo Toniolli
Diputado Germán Martínez
Diputado Jorge Neri Araujo Hernández
Diputado Jorge Antonio Romero
Diputada Roxana Monzón
Diputado Julio Cesar Pereyra
Diputada Hilda Aguirre
Diputado Martín Aveiro
Diputada Carolina Yutrovic
Diputado Ariel Rauschenberger
Diputada Ana María Ianni
Diputada Victoria Tolosa Paz
Diputado Martín Soria
Diputado Ricardo Herrera
Diputada Eugenia Alianiello

Fundamentos

El Ministerio de Defensa, en cabeza del Ministro Luis Petri, celebró un acuerdo de entendimiento con el embajador de Estados Unidos, Mark Stanley, el 25 de marzo de 2024. Este acuerdo, que aborda la cooperación en ciberseguridad y ciberdefensa, fue detallado en un artículo del portal Infobae.com (https://www.infobae.com/politica/2024/03/26/el-gobierno-firmo-un-memorandum-con-estados-unidos-para-la-cooperacion-en-ciberdefensa-los-detalles/). En la noticia, el Ministro afirma textualmente: *"La defensa digital del país también se construye cooperando con todos los actores que lideran el proceso de transformación digital en el mundo. Este acuerdo nos permite defendernos mejor de las amenazas persistentes que existen en el ciberespacio"*.

En los últimos días se hicieron públicos algunos documentos que exponen que, en el marco del citado acuerdo, el ministro Petri designó como asesor en ciberseguridad del Ministerio de Defensa a un experto contratado por la embajada de los EEUU, que relevará "el estado de situación en materia de ciberseguridad" de las Fuerzas Armadas argentinas.

Es necesario señalar que, si bien existe un consenso internacional en torno a la necesidad de cooperar en materia de ciberseguridad y ciberdefensa (ya que el ambiente operacional es accesible y transversal a todas las naciones, contiene a sus infraestructuras críticas y sistemas de defensa, y por el carácter transfronterizo de muchas amenazas), sin embargo, una cosa es cooperar mediante el intercambio de información, la capacitación de recursos humanos y los ejercicios conjuntos, y otra muy distinta es que un asesor se interiorice de todos los aspectos clasificados de la seguridad cibernética de un Estado, o de su defensa.

Es importante señalar además que dentro de las FFAA, como dentro de la Subsecretaría de Ciberdefensa, hay personal altamente calificado y que trabaja en la temática desde el 2014, año de creación del Comando Conjunto de Ciberdefensa.

La gravedad de este acuerdo radica en la sensibilidad y el secretismo de la información generada por las Fuerzas Armadas. Esta información abarca tanto a los uniformados en actividad, que son, en algunos casos, parte de unidades de élite y de la fuerza de comandos, como a los miles de retirados y pensionistas que se encuentran en situación de retiro. De acuerdo con el Ciclo de Planeamiento de la Defensa y los programas de adquisiciones de medios y material bélico, la información de las Fuerzas Armadas es confidencial y no debería ser compartida con terceros ajenos a su labor. Esta confidencialidad es esencial en el adiestramiento y en la doctrina militar argentina, porque hace a la capacidad de adelantarse a amenazas. Que nuestros datos e información sensible sean auscultados por otros países conlleva un alto riesgo de fracaso en la estrategia militar y en el empeñamiento de los medios y el personal, más aún si en la lista de unidades que serán auditadas y evaluadas por el asesor estadounidense, se encuentran organismos que gestionan información sensible como la Dirección Nacional de Inteligencia Militar, el Comando Conjunto de Ciberdefensa, el Instituto de Ciberdefensa de las Fuerzas Armadas, y los institutos de formación en Ciberdefensa e Inteligencia de cada una de las tres fuerzas y el Estado Mayor Conjunto.

La intromisión en los asuntos de ciberseguridad y ciberdefensa de Argentina representa un grave problema de confidencialidad, especialmente considerando que Estados Unidos es miembro de la OTAN junto con el Reino Unido y ambos comparten el sistema de inteligencia Five Eyes, del cual también forman parte Australia, Canadá y Nueva Zelanda.

Esta entrega de información sensible a una potencia extranjera es un grave atentado contra las Fuerzas Armadas, la soberanía y el conjunto de la seguridad del Estado, y merece nuestro más abierto rechazo.

Es por lo expuesto que solicito a mis pares que acompañen el proyecto.

Diputado Eduardo Toniolli
Diputado Germán Martínez
Diputado Jorge Neri Araujo Hernández

Diputado Jorge Antonio Romero
Diputada Roxana Monzón
Diputado Julio Cesar Pereyra
Diputada Hilda Aguirre
Diputado Martín Aveiro
Diputada Carolina Yutrovic
Diputado Ariel Rauschenberger
Diputada Ana María Ianni
Diputada Victoria Tolosa Paz
Diputado Martín Soria
Diputado Ricardo Herrera
Diputada Eugenia Alianiello