ANALISIS PROSPECTIVO DE LAS AMENAZAS EN EL CIBERESPACIO EN URUGUAY

Trabajo presentado en el Calen – Ministerio de Defensa Nacional

Dra. Esc. María José Viega Rodríguez

INDICE

AMENAZAS EN EL CIBERESPACIO EN URUGUAY

1. INTRODUCCIÓN

El presente trabajo tiene como objeto estudiar distintas posibilidades de hacer frente a las amenazas que enfrenta nuestro país en el ciberespacio, partiendo del concepto amplio de Defensa Nacional establecido por la Ley N° 18.650 de 19 de febrero de 2010, en el que, además de la clásica defensa militar, incluye el ámbito civil.

El análisis de las amenazas en el ciberespacio resulta de interés en virtud a que es un espacio que se ha incorporado recientemente en la normativa uruguaya, vinculado a la Defensa Nacional, en la Ley Orgánica de las Fuerzas Armadas N° 19.775 de 26 de julio de 2019 y en el Decreto N° 371/020 de 23 de diciembre de 2020.

En el Decreto N° 371/020, al referirse a la situación mundial (Punto II) tiene en cuenta un nuevo paradigma caracterizado por la hibridez de las amenazas y la glocalidad en cuanto al área de operación e incidencia, incluyendo el plano cibernético como uno de los lugares en que se puede accionar.

Refiere al ciberespacio en los puntos III, VI y VII, mencionando dentro de los Objetivos Estratégicos del Estado: mantener la integridad territorial, marítima, aeroespacial y del ciberespacio del país. En el mismo sentido, se lo considera en el Punto VIII definiendo como Objetivos de la Defensa Nacional: asegurar la soberanía del Estado en los espacios terrestres, marítimos, aeroespaciales y del ciberespacio.

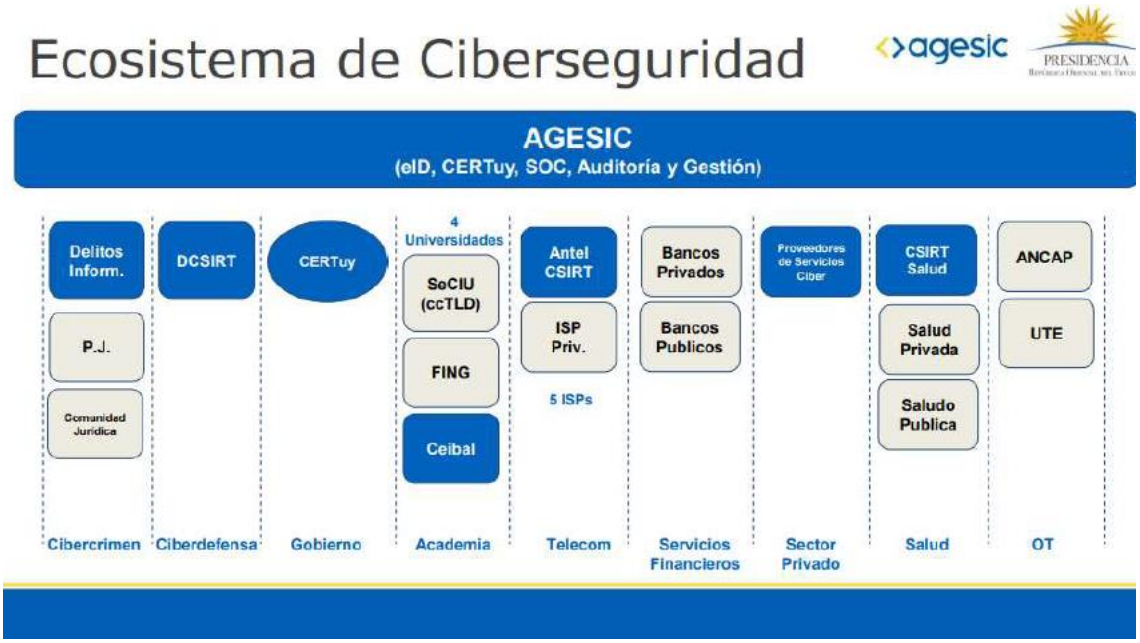
Por otra parte, en el punto IX, relativo a las Amenazas, considera en primer lugar la violación de nuestra soberanía terrestre, marítima, aeroespacial o del ciberespacio. En cuarto lugar, califica a los ciberataques como una amenaza que afectaría la disponibilidad, integridad o la confidencialidad de la información digital.

La ciberguerra, el ciberterrorismo y los ciberdelitos afectan a todos los factores del poder, porque tienen un impacto desde el punto de vista sicosocial, ya que perturban la seguridad, tanto individual, social y a nivel del Estado. También tiene consecuencias económicas muy importantes, en virtud a que uno de los principales objetivos de los ilícitos es económico. Además, es un elemento fundamental a considerar en la lucha contra estas nuevas amenazas el presupuesto destinado a los organismos competentes.

Por otra parte, el Cnel. Gustavo Vila (2021) conceptualiza al factor militar en forma más amplia, refiriéndose a éste como Seguridad y Defensa. En este sentido, podemos decir que es uno de los factores presente en este trabajo, porque la defensa nacional involucra a civiles y militares, conjuntamente con el Factor

Científico Tecnológico, considerando que el desarrollo de las TIC constituye el origen de la problemática planteada.

Con relación a las instituciones con competencias específicas en ciberseguridad encontramos las siguientes:



Fuente: Página web de Agesic

Es necesario diferenciar la ciberseguridad de la ciberdefensa y, por lo tanto, analizar las instituciones y el marco jurídico existente en ambos sentidos. A los efectos de determinar que posibles eventos futuros tendrían influencia y en qué medida sería conveniente o no llevarlos a cabo, se realizará una Lista de posibles eventos futuros y una Matriz de Impactos Cruzados. A partir de los resultados se realizará un análisis y una matriz FODA, que determine donde nos encontramos y que acciones deberían tomarse para mejorar la ciberseguridad en nuestro país.

2. LISTA DE POSIBLES EVENTOS FUTUROS

Si se realiza un análisis de que eventos relevantes podrían estar vinculados a los ciberdelitos, a posibles ataques a las infraestructuras críticas, a la ciberseguridad y a la ciberdefensa, encontramos los siguientes:

- Aumento significativo de los Ciberdelitos
- Ciberataques a infraestructuras críticas

- Aprobación de una ley de ciberdelitos
- Aprobación de política nacional de ciberseguridad
- Mayor presupuesto en ciberseguridad
- Creación de un Comando de Ciberdefensa en el Ministerio de Defensa
- Realización de campañas de educación en ciberseguridad

3. MATRIZ DE IMPACTOS CRUZADOS

Según Gallardo A. (2019, pág. 155) la matriz de impactos cruzados "se trata de una herramienta que relaciona en formato matricial, todas las variables constitutivas o estructurales de un análisis (análisis estructural), con la finalidad de identificar las variables influyentes y las dependientes".

Variables	Aumento significativo Ciberdelitos	Ciberataques a infraestructuras críticas	Aprobación Ley Ciberdelitos	Aprobación Marco Nacional Ciberseguridad	Mayor presupuesto en ciberseguridad	Creación Comando Ciberdefensa	Campaña de educación en ciberseguridad	Ratificar Convenio Budapest
Aumento significativo Ciberdelitos		↓	↑	↑	↑	↑	↑	↑
Ciberataques a infraestructuras críticas	↓		↑	↑	↑	↑	●	↑
Aprobación Ley Ciberdelitos	↑	↑		●	●	●	↑	↑
Aprobación Marco Nacional Ciberseguridad	↑	↑	●		↑	●	↑	●
Mayor presupuesto en ciberseguridad	↑	↑	●	↑		↑	↑	●
Creación Comando Ciberdefensa	●	↑	●	↑	↑		↑	●
Campaña de educación en ciberseguridad	↑	↑	●	●	↑	●		●
Ratificar Convenio Budapest	↑	↑	●	●	↑	●	↑	

↑	Efecto positivo
●	Efecto neutro
↓	Efecto negativo

De la Matriz de Impactos Cruzados podemos concluir que el mayor efecto positivo está dado por el ciberataque a las infraestructuras críticas, no porque el evento sea positivo en sí mismo, todo lo contrario, sino por el impacto que causaría. Un ataque de este tipo pondría el tema sobre la mesa y se visualizaría la necesidad de contar con un Comando en ciberdefensa, con un presupuesto importante, con normativa

específica en materia de ciberseguridad y de ciberdelitos, así como contar con cooperación internacional a través de Convenios internacionales.

La misma idea subyace en el aumento de los ciberdelitos, hecho que ya está sucediendo hoy día, y ha provocado que se comenzaran a discutir ciertos temas y se visualizara la necesidad de adoptar determinadas medidas.

Los otros dos factores que se encuentran en un mismo plano, también provocando un efecto positivo son: la existencia de un presupuesto mayor y la realización de campañas de capacitación.

Efectos negativos encontramos puntualmente en el aumento de los ciberdelitos y en los ataques a las infraestructuras críticas.

La aprobación de la Ley de Ciberdelitos aparece con la mayor cantidad de aspectos de neutralidad, lo cual entiendo que es correcto, porque una ley por sí misma no provoca grandes cambios, si por ejemplo no tiene un presupuesto asociado, una campaña de educación, entre otras medidas.

4. MÉTODO FODA

Heuer y Pherson (2011) conceptualizan el Método FODA, como “un diagnóstico interno y externo de la organización o situación buscando evaluar Fortalezas, Oportunidades, Debilidades y Amenazas (FODA en castellano, en inglés SWOT):

- Fortalezas y Debilidades: Ámbito interno / controlables.
- Amenazas y Oportunidades: Ámbito externo / no controlables”.

FORTALEZAS	DEBILIDADES
1. Aprobación de una Ley de Ciberdelitos 2. Aprobación de un Marco Nacional de Ciberseguridad 3. Realización de campañas de educación en ciberseguridad	1. No tener un presupuesto apropiado en ciberseguridad 2. No tener un Comando de Ciberdefensa en el Ministerio de Defensa
OPORTUNIDADES	**AMENAZAS**
1. Adherir al Convenio de Budapest	1. Aumento significativo de los ciberdelitos 2. Ataques a infraestructuras críticas

Si se analizan las Fortalezas, las Debilidades, las Oportunidades y las Amenazas aplicando las técnicas de correlación y de conversión,

Factores internos / **Factores externos**	**Lista de Fortalezas** 1. Aprobación de una Ley de Ciberdelitos 2. Aprobación de un Marco Nacional de Ciberseguridad 3. Realización de campañas de educación en ciberseguridad **CORRELACIÓN**	**Lista de Debilidades** 1. No tener un presupuesto apropiado en ciberseguridad 2. No tener un Comando de Ciberdefensa en el Ministerio de Defensa **CONVERSIÓN**
Lista de Oportunidades 1. Adherir al Convenio de Budapest	**FO (Maxi-Maxi)** La Aprobación de la Ley de Ciberdelitos habilita al país para que pueda adherir al Convenio de Budapest	**DO (Mini-Maxi)** La Adhesión al Convenio de Budapest permite al país contar con cooperación internacional, lo que no tendría costo presupuestal y sería beneficioso para la ciberdefensa
Lista de Amenazas 1. Aumento significativo de los ciberdelitos 2. Ataques a infraestructuras críticas	**FA (Maxi-Mini)** 1. La aprobación de una Ley de Ciberdelitos puede ser un elemento disuasor para cometer este tipo de conductas, muchas de las cuales hoy día causan daño, pero no están tipificadas penalmente, por lo tanto, quedan sin una pena. 2. La aprobación de una Marco o Política Nacional de Ciberseguridad establecería la obligación de las instituciones de mejorar la ciberseguridad, por lo que sería más difícil cometer delitos informáticos y/o atacar las infraestructuras críticas. 3. Un buen nivel de capacitación de las personas en general y de los funcionarios, aseguraría que no se cayera en determinados engaños, como por ejemplo el phishing, y la seguridad no se quebraría por el factor humano.	**DA (Mini-Mini)** 1. Los ciberdelitos podrían minimizarse con una ley que los tipifique y un marco de ciberseguridad que fortalezca las redes en todas las instituciones. 2. Los ataques a las infraestructuras críticas podrían evitarse con la aprobación de un marco de ciberseguridad, pero también creando un comando de ciberdefensa y aumentando el presupuesto para la ciberseguridad y la ciberdefensa.

5. CONCLUSIONES

Del análisis realizado es posible concluir que son varias las medidas que pueden adoptarse para hacer frente a las diferentes amenazas que pueden plantearse en el ciberespacio.

Desde el punto de vista legal resulta relevante la aprobación de una ley de ciberdelitos y una política nacional de ciberseguridad, para lo cual es necesario una decisión política.

Desde el punto de vista de las instituciones que refieren a la ciberseguridad la infraestructura parece suficiente, sin embargo, en cuanto a la ciberdefensa sería necesaria la Creación de un Comando de Ciberdefensa, con competencias específicas en este ámbito, en el Ministerio de Defensa.

Desde el punto de vista económico es necesario contemplar presupuestalmente los objetivos que se plantee, tanto a nivel legal como institucional, en el ámbito de la ciberseguridad y la ciberdefensa.

Finalmente, la realización de campañas de educación constituye un elemento fundamental para que las personas en general conozcan los nuevos riesgos a los que se enfrentan cuando actúan en el ámbito del ciberespacio.

BIBLIOGRAFIA

Gallardo A., (2019) Manual de métodos de prospectiva: uso práctico para analistas. Centro de Estudios e Investigaciones Militares.

Heuer, R. y Pherson, R. (2011) Structured Analytic Techniques for Intelligence Analysis. Washington DC, USA: CQ Press.

Vila G., (2019) Los ciberataques como amenazas a las infraestructuras y recursos críticos de un Estado. Revista Estrategia Tercera época Número 6. Centro de Altos Estudios Nacionales.

Ley N° 18.650 de 19 de febrero de 2010. Ley Marco de Defensa Nacional. Disponible en el Centro de información Oficial (IMPO): https://www.impo.com.uy/bases/leyes/18650-2010

Ley N° 19.775 de 26 de julio de 2019. Ley orgánica de las Fuerzas Armadas. Disponible en el Centro de información Oficial (IMPO) https://www.impo.com.uy/bases/leyes/19775-2019/4

Decreto N° 371/020. Política de Defensa Nacional. Disponible en el Centro de información Oficial (IMPO): https://www.impo.com.uy/bases/decretos-originales/371-2020