CONCURSO ANEPE 2015 **PROYECTO 201519**

Investigador Responsable	JUAN IGNACIO NICOLOSSI BAEZA
Código Proyecto	201519
Título Proyecto	CIBER-SEGURIDAD Y CIBER-DEFENSA; Tareas pendientes para la protección de la soberanía del Estado de Chile en un mundo globalizado.

Resumen

El proyecto busca generar un documento desde una perspectiva del análisis cualitativo, respecto de los procesos paralelos (civiles y castrenses) para implementar las estrategias Nacionales de Ciberseguridad Interna, y Ciberdefensa ante amenazas foráneas.

El presente estudio plantea la hipótesis donde el retraso en el proceso de estructuración de un Sistema Nacional de Ciberdefensa y Ciberseguridad hace al Estado de Chile vulnerable, dejando un flanco abierto en la seguridad y defensa de la soberanía nacional.

Es opinión de este autor que la falta de una estrategia nacional de frente a las amenazas del ciberespacio, se deben principalmente, a la falta de una visión conjunta respecto de cómo enfrentar el problema y oportunidades que el área ofrece, los organismos responsables, recursos necesarios, estructura orgánica, doctrina y planificación de corto, mediano, y largo plazo.

El retraso a nivel comparado respecto de la implementación del ciberespacio como frontera virtual de la soberanía del estado, la protección que requiere, las amenazas, las capacidades y beneficios que este ofrece al país son urgentes y de extrema necesidad, puesto que la evolución de las tecnologías es esencialmente exponencial (Ley de Moore), es decir, mientras más demore el proceso en comente, mayor será la dificultad y retraso del país para adecuarse a las necesidades estratégicas que plantea el siglo XXI.

Objetivos,

1. Generar material académico desde la perspectiva cívico-militar en relación al concepto de Ciber Seguridad en aspectos internos y Ciber Defensa en los aspectos de protección de los intereses externos del Estado y sus implicancias para una reforma estructural, frente a las nuevas amenazas virtuales que reflejan efectos en el espacio físico.
2. Establecer un análisis comparado frente a los avances de países desarrollados en la materia, utilizando como base el Trabajo bilateral entre Estados Unidos y Rusia del 2011 (Critical Terminology Foundations, Russia – US Bilateral on Cybersecurity),y el estudio comparado con las estructuras y estrategias actuales de Reino Unido, EE.UU., Israel, España, Brasil, Perú, Bolivia, Argentina, y Alemania, para generar una línea de base (benchmark), que permita al
3. Estado de Chile priorizar sus reformas según la experiencia y mejores prácticas internacionales.
4. Crear un documento que genere una primera aproximación a las potenciales reformas para la creación de una orgánica Nacional que permitan modernizar el sistema ante las, amenazas Informáticas (Ciberseguridad), y las capacidades defensivas y ofensivas (Ciber defensa), que el espacio virtual ofrece.

Metodología,

1. Análisis Histórico de tipo cualitativo que permita identificar el “estado de situación” del estado de Chile en el proceso de formación de un Sistema de Ciberseguridad y Ciberdefensa para el país.
2. Análisis de Contenido Comparado basados en las modificaciones estratégica, legales, estructurales, y doctrinarias en los procesos de modernización de los servicios de protección del ciberespacio estudiando los modelos implementados por Reino Unido, EE.UU., Israel, España, Brasil, Perú, Bolivia, Argentina, y Alemania, utilizando las distintas estrategias y planes de reforma presentados en los últimos 10 años por dichos países para hacer frente a las amenazas en comente, derivadas de las experiencia.
3. Proceso de entrevistas personales con expertos en el área de la Ciberseguridad y Ciberdefensa (técnicos informáticos nacionales y extranjeros, analistas, académicos, Directores de Servicio, Agregados diplomáticos, etc.), con la intención de contrastar la hipótesis del presente trabajo, con la experiencia de aquellas personas involucradas directa o indirectamente con la materia en estudio.

Resultados,

1. Establecer un análisis de la situación actual del Estado de Chile frente a las amenazas del ciberespacio, los planes en desarrollo, las distintas problemáticas para su implementación, tanto en el ámbito de la seguridad interna como externa.
2. Generar un análisis comparado respecto de la estructura, doctrina y planificación estratégica entre los sistemas de protección de países desarrollados, para la conformación de una línea de base para establecer estándares internacionales en los que el Estado de Chile se pueda basar para futuras reformas –o creación- al sistema actual.
3. Creación de un documento que permita presentar un proyecto que incluya directrices básicas para la formulación de una Estrategia Nacional de Ciberseguridad y Ciberdefensa para el siglo XXI en concomitancia con las necesidades experimentadas por aquellos países a la vanguardia del tema, tomando en consideración los recursos disponibles

RESULTADOS OBTENIDOS **PROYECTO 201519**

Título Proyecto	CIBER-SEGURIDAD Y CIBER-DEFENSA; Tareas pendientes para la protección de la soberanía del Estado de Chile en un mundo globalizado

Artículos

Autor(es)	Juan Ignacio Nicolossi										
Título	Historia. Guerra, Computación y la creación del Ciberespacio										
Publicado							Indexada				
Referencia	Ciudad		Año		N°		Págs.		Links		
Enviado a	Revista ESD Estudios de Seguridad y Defensa						Aceptado	X	En prensa		

Autor(es)	Juan Ignacio Nicolossi										
Título	Arquitectura del Ciberespacio										
Publicado							Indexada				
Referencia	Ciudad		Año		N°		Págs.		Links		
Enviado a	Revista ESD Estudios de Seguridad y Defensa						Aceptado		En prensa		

Congreso, Evento, Jornada

Autor (es)	Juan Ignacio Nicolossi Ayudantes; Francisco Borie y Rodrigo Peña			
Título Ponencia	CiberSeguridad y Ciberdefensa			
Congreso Evento Jornada	Exposición Técnica para el Estado Mayor Conjunto.			
Referencia General	Institución Organizadora	Ciudad	Año	Links
	Ministerio de Defensa	Santiago	2015	

Autor (es)	Juan Ignacio Nicolossi Ayudantes; Francisco Borie y Rodrigo Peña			
Título Ponencia	CiberSeguridad y Ciberdefensa en Chile			
Congreso Evento Jornada	Exposición Técnica para Comisión de Defensa del Senado de la República de Chile			
Referencia General	Institución Organizadora	Ciudad	Año	Links
	Congreso nacional. Senado de la república	Santiago	2016	

Informe Final

Título	Informe Final Proyecto de Investigación Concurso Anepe 2015					
Autor	Juan Ignacio Nicolossi	Ciudad	Santiago	Año	2016	

Resultados Obtenidos

I.- Objetivos Generales Planteados Originalmente

1) **Generar material académico desde la perspectiva cívico-militar en relación al concepto de CiberSeguridad en aspectos internos y Ciberdefensa en los aspectos de protección de los intereses externos del Estado y sus implicancias para una reforma estructural frente a las nuevas amenazas virtuales que reflejan efectos en el espacio físico.**

En este punto, hemos logrado a lo largo del trabajo, y especialmente en el capítulo denominado Terminología, rescatar y analizar las bases conceptuales del término

Ciberseguridad y Ciberdefensa, tanto en lo que respecta a su similaridad y diferencias, pero sobre todo, identificando y logrando explicar los principios tras dichos términos.

- **Cybersecurity: "Is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover."**

- **"Es una propiedad del ciberespacio que corresponde a la habilidad de RESISTIR, amenazas tanto intencionales como NO intencionales, y RESPONDER y RECUPERARSE" (traducción NO oficial)**

En el área de la seguridad cibernética nos encontramos con un término basado –en su sentido técnico-, en al Critical Terminology Foundations, diccionario al que ya nos hemos referido con anterioridad. Sin embargo, de dicha definición logramos identificar las bases del mismo, logrando establecer que la Ciberseguridad se compone en su base por la protección a los sistemas y redes informáticas, de los efectos de intervención de entidades NO autorizadas. Por otra parte, se entiende de la definición que la seguridad del ciberespacio es una propiedad del mismo, por tanto, de no existir, el ciberespacio tal como lo conocemos degenera en un fenómeno distinto.

Finalmente, se logra establecer el fondo que implican los conceptos referentes a RESISTIR, RESPONDER y RECUPERAR, establecidas en la definición base. En el caso de la presente triada se establece incluso el ciclo de inversión recomendado respecto de la instalación misma de al ciberseguridad en una estructura eficiente y eficaz. Es así como identificamos la lógica que existe desde la perspectiva financiera destinada a soportar –a través de recursos estatales-, a saber, quienes invierten mayormente sus recursos en las etapas de resistencia, tienden a tener que destinar menores recursos en las áreas de respuesta y recuperación, y viceversa.

- **Cyber Defense: "Is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack."**
- **"Es la capacidad organizada para PROTEGER, MITIGAR, RECUPERAR rápidamente, en contra de de un ciberataque" (traducción NO oficial)**

Por otra parte, en lo que refiere a ciberdefensa, si bien se denota las similitudes entre los verbos rectores, la implicancia de su redacción implica que la ciberseguridad de los sistemas y redes, es parte de las capacidades de ciberdefensa, sin embargo, el principio en este caso no es reversible, es decir, la ciberseguridad, no necesariamente implica el área de la defensa como uno de sus componentes. En la definición, según se profundiza en el borrador, el concepto de ciberdefensa está orientado a la infraestructura necesaria en el espacio físico (recursos humanos, instituciones (hardware y softwares, etc.), que se requieren para la protección de la infraestructura cibernética que cobija el Estado. En este caso se refiere en la práctica a una institucionalidad dedicada a proteger los intereses del Estado en el ciberespacio Instituciones tales como CSIRTS o CERTS nacionales, cibercomandos, servicios de ciberinteligencia, control democrático, derechos, legislación, etc.). Para que la ciberdefensa logre mantener un estándar de seguridad en los sistemas y redes que protege, se requiere necesariamente de una infraestructura que la cobije, y el diseño de la misma es de la mayor importancia.

2) **Establecer un análisis comparado frente a los avances de países desarrollados en la materia, utilizando como base el Trabajo bilateral entre Estados Unidos y Rusia del 2011 (Critical Terminology Foundations, Russia - US Bilateral on Cybersecurity),y el estudio comparado con las estructuras y estrategias actuales de Reino Unido, EE.UU., Israel, España, Brasil, Perú, Bolivia, Argentina, y Alemania, para generar una línea de base (benchmark), que permita al Estado de Chile priorizar sus reformas según la experiencia y mejores prácticas internacionales.**

En el caso de la utilización a lo largo del proyecto de las definiciones que nos entrega el texto producto de las bilaterales celebradas entre EE.UU. y Rusia, tanto en 2011, como 2014, he de reconocer que el aporte a sido invaluable para la posibilidad de estructurar y

explicar los términos claves que componen las bases de tanto la ciberseguridad como la ciberdefensa.

En bajo el nuevo formato, hemos podido extendernos significativamente y en detalle de los conceptos que el texto ofrece tanto para el desarrollo de terminologías básicas comunes, sino que también para el desarrollo de políticas públicas, ya sean está a nivel nacional o internacional. El valor del trabajo no solo ha permitido elucubrar sobre las lógicas técnicas tras las definiciones, al mismo tiempo de entregar una herramienta única para guiar el discurso en la materia.

En lo que respecta al valor político, estratégico, técnico del trabajo realizado por ambos países, implica un claro desafía al resto de la comunidad internacional respecto a que términos van a ser aceptados –y aquellos que no-, a la hora de determinar la existencia de un conflicto REAL entre súper poderes respecta. El desafío consiste en la adopción de dic ha terminología como referencia base para el desarrollo de políticas comunes a nivel mundial, dado la estructura global del ciberespacio.

Respecto a la legitimidad del trabajo para ser considerado un "benchmark" para guiar el foco de la discusión, me remito a lo señalado anteriormente, respecto de la importancia de ambos en los movimientos de geopolítica internacional. Por último, si consideramos el aspecto político más básico de las filosofías políticas que ambas Federaciones representan, y si aceptamos que ambas corresponden a los modelos base de los Estados modernos, vemos el rasgo de objetividad que impide que la protesta sobre la legitimidad a nivel político de estas definiciones se tornen difíciles tanto por parte de los ejes de derecha, centro o izquierda. En pocas palabras, el texto en comente no solo entrega un decálogo de términos útiles a nivel técnico, sino que definen un valor de necesidad y unidad única en lo que a política internacional y su carácter ejemplificador para otras naciones refiere, independiente de las ideologías que las gobiernen.

En lo que refiere al análisis comparado, este aun estar en proceso de ser modelado respecto del nuevo modelo, lo cual pareciere consistente con la intención de esperar a los resultados de la Consulta pública realizada por el ministerio del Interior y Seguridad Publica llevo adelante en los últimos meses, destinada a mostrar parte de las conclusiones emitidas por la mesa Intersectorial creada por el Decreto 533 de fecha 17-07-2015. Tanto el trabajo como los elementos discutidos a lo largo de casi un año por la mesa, dieron paso a una propuesta que se ofreció a la sociedad chilena para su conocimiento, como parte del proceso de legitimación de la misma. Parece prudente esperar los resultados oficiales para conocer de los resultados oficiales que el trabajo de dicha Mesa género, ya que ello abriría la posibilidad de compararlos con los productos similares de otros países. Sin embargo, en caso de que los resultados no sean publicados en su totalidad en un tiempo razonable –antes del segundo semestre-, se procederá a recurrir a la Ley de transparencia para la recopilación de tal materia por vía oficial, como todo ciudadano.

3) **Crear un documento que genere una primera aproximación a las potenciales reformas para la creación de una orgánica Nacional que permitan modernizar el sistema ante las, amenazas Informáticas, y las capacidades defensivas y ofensivas que el espacio virtual ofrece.**

En este apartado, hemos logrado identificar tanto la naturaleza defensiva como ofensiva que ofrece el ciberespacio. Desde la identificación del concepto de ataque cibernético, sus potenciales daños, y las amenazas fuente de dicha potencialidad. En este caso se aplicó una metodología de análisis basada en el antiguo principio en lo que a manejo de riesgos refiere, a saber, "Vulnerabilidad + Amenaza =Riesgo". El trabajo hasta el momento muestra resultados claros y simples en lo que a la identificación de los distintos componentes de dichas variables implican. El análisis de vulnerabilidades estructurales de la red, tales como la dependencia física, la interconectividad "peer to peer" (P2P), o la misma persona –usuario- del ciberespacio representan desde el núcleo del mismo.

Por otra parte, las amenazas tales como el cibercrimen, activismo político vía internet (grupos como Anonimous, Lultz Sec, etc.), el ciberespionaje, ciberterrorismo, y la

ciberguerra representan como fuente originadora de dichas amenazas. Finalmente, respecto de los riesgos, el autor cree que estos son inherentes e inevitables al minuto de decidir participar del ciberespacio, es decir, el riesgo de ser víctima de alguna amenaza que explote las distintas vulnerabilidades que el ciberespacio ofrece, implican un riesgo latente, directo y por tanto inminente, en lo que al uso de la internet refiere. Dicha conclusión por si sola ha llevado al autor a aprovechar el nuevo formato del trabajo para trabajar y comprobar –según creo- dicha teoría en la práctica.

II.- Objetivos Específicos Planteados Originalmente

1) Establecer un análisis histórico fidedigno que nos permita delimitar el estado de situación actual del país frente a las amenazas que el ciberespacio ofrece.

En lo que refiere el análisis histórico, creo se logró cabalmente integrar el desarrollo del Estado de Chile hasta principios de los 90s en paralelo con la historia universal en lo que al proceso de creación del ciberespacio respecta. En el capítulo uno hemos trazado una línea histórica que va desde los anales de la II Guerra Mundial, hasta la llegada de la Internet a Chile.

Creo que en este caso se ha logrado un producto rico en lo que a contextualización del fenómeno refiere, considerando el análisis histórico no solo como una introducción debida del tema en comente, sino que al poder extendernos en los fondos y formas que llevaron a la creación, se establece en el trabajo que la historia es la columna vertebral que da un direccionamiento básico para cualquier lector hacia el resto del trabajo, ya sea dicho lector un académico, ingeniero, o un lego en la materia que desea introducirse al tema. En lo que respecta al análisis más profundo del área histórica del trabajo, mantengo lo señalado en el informe de avance del mes de Septiembre, respecto de la importancia de dicho tipo de análisis.

2) Generar un análisis comparado respecto de la estructura, doctrina y planificación estratégica entre las estructuras actuales del Estado de Chile, y sus contrapartes en países desarrollados, contrastando las capacidades actuales frente a las amenazas descritas en el Marco Teórico.

En lo que al marco Teórico refiere, creo se ha logrado establecer con claridad las amenazas, vulnerabilidades y daños que el ciberespacio presenta en su interacción con los usuarios. En lo que respecta al análisis comparado, dentro del presente borrador se realizan comparaciones respecto de la Ley Penal en lo que a delitos informáticos respecta, los fundamentos técnicos de la redacción de cada articulado contenido. Por otro lado se analizó la misma legislación con su estándar internacional representado por la convención de Budapest de año 2001 sobre cibercrimen. En lo que refiere al análisis comparado, el trabajo si bien esta aun en progreso y pretende ser el pilar en lo que al borrador N°3 respecta –se propone el mes de Mayo-, se incluye la primera parte referida al análisis estratégico tanto a nivel de seguridad como del sector defensa de los EE.UU., pudiendo establecer los principios básicos que constituyen ambos documentos. En lo que respecta a Chile, me refiero a lo expresado respecto a esperar un plazo razonable para poder incluir en el presente estudio, los Resultados de la Mesa Intersectorial mencionada anteriormente.

3) Crear un análisis académico que logre posicionar los temas de Ciberseguridad y Ciberdefensa como prioridades de primera necesidad para el ente gubernamental, defensa y seguridad, para buscar el fortalecimiento de las estructuras estratégicas de las cuales dependen la protección de los intereses del estado chileno.

En esta parte me refiero a lo señalado en el acápite anterior respecto de la evolución que el proyecto tuvo respecto de transitar desde in informe meramente académico, hacia un trabajo bajo la prospectiva de un libro que logre un alcance mayor, pasando obviamente por la academia, pero sin embargo, focalizado para incluir a ingenieros y la sociedad en general. Lo que implico sendos cambios tanto en la retórica del material, como en la construcción del mismo, con la intención de profundizar los temas al punto de

simplificarlos de tal manera, que las complejidades del fenómeno fuesen fáciles de digerir para cualquier lector, independiente de su origen y conocimiento del tema. El BORRADOR N°2, entrega una estructura rica en simplicidad bajo la premisa de la educación e introducción al tema, más que una análisis crítico a la situación local, el cual, por cierto también será incluido, pero desde una perspectiva más constructiva y digerible, para lograr el producto deseado bajo este nuevo prisma educativo hacia el que evolucionó el presente trabajo.

III.- Nuevo Objetivo

1) **Educar al respecto de las nociones básicas referentes al ciberespacio, su seguridad y defensa desde una dialéctica simple que permita tanto al académico como el lego, educarse e interactuar en el área a modo improductivo.**

En este sentido, con la colaboración de profesionales en el área de la edición, se ha trabajado en un modelo de trabajo que espero sea lo9 suficientemente entendible y útil independiente del nivel de conocimientos en el área que el lector posee, En el trabajo se han agregado soportes mediante esquemas visuales, junto con las herramientas vía links que permitan al lector interactuar directamente desde el informe –en su versión digital- a las fuentes de información referenciadas. Si bien las referencias bibliográficas en todo trabajo de este tipo, la mismas tecnologías descritas en el trabajo permiten un nivel de relación directa entre el lector y la fuente original de la información referenciada, ya no solo permitiendo acceso a material acabado para que este interactúe con él, sino que creando un ambiente didáctico para que el lector tenga los incentivos suficientes -y a mano-, para responder a sus inquietudes, si así lo requiriese. Eventualmente espero que en la versión digital del producto final, dicha interacción se acentué al punto de incorporar material audiovisual útil para el entendimiento cabal y dinámico de las estructuras conceptuales tratadas en el presente trabajo, que si bien aún esta en progreso, ya muestra señales de poder servir de material para el direccionamiento del discurso político, técnico, o un simple debate entre entusiastas del área.