Juan Pablo Darioli

Trabajo Integrado Final

Diplomatura Internacional: Comunicación y Defensa Nacional

Cohorte 2021

Universidad de la Defensa Nacional

Título: Ciberdefensa

Tema: En la historia reciente, algunos hechos internacionales dieron cuenta de la importancia estratégica de la ciberdefensa en el mundo actual. Un repaso de estos hechos, nos otorga perspectiva para plantear los desafíos del área.

Objetivos: Fijar conceptos básicos y generales sobre el lugar que ocupa hoy la ciberdefensa y desarrollar una perspectiva histórica de hechos que den cuenta del surgimiento de ésta como área estratégica para los Estados nacionales.

Informe periodístico extendido:

La soberanía política en el siglo XXI no puede prescindir del desarrollo de estrategias para el ciberespacio, entendido éste como un nuevo ámbito operacional para las políticas de defensa. Como se define en el Manual de Tallin, el ciberespacio es un "entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de redes informáticas". Muchas veces se hace alusión a los nuevos escenarios creados por las Tecnologías de la Información y la Comunicación como evanescentes o etéreos (la idea de la nube), pero de esta forma se invisibiliza la infraestructura material que hace posible el funcionamiento de las redes, y ahí es donde Oscar Niss, Secretario de Ciberdefensa del Ministerio de Defensa de Argentina, afirma que "el ciberespacio no es un espacio independiente de los otros ámbitos espaciales y no es soberano per se, sino que es una infraestructura sobre la que se ejerce soberanía".

Al mismo tiempo, el ciberespacio interactúa e influye en los ámbitos operacionales preexistentes, terrestre, marítimo, aéreo y espacial, es un ámbito transversal, que plante escenarios de conflicto no convencionales, con modos de acción silenciosos e invisibles, donde es muy dificultoso identificar con certeza a los atacantes. Es imprescindible pensar en este cambio de paradigma y las transformaciones que trae aparejado para tomar real dimensión de las implicancias de la nueva realidad. Por eso, pensar desde una perspectiva histórica, con hechos puntuales que han ido sucediendo y aportando para la conceptualización es un forma pedagógica de darle lugar en la agenda de contenidos periodísticos.

Para el primer capítulo del podcast, trabajamos el caso de Estonia donde un ciberataque generó un punto de inflexión para el desarrollo de políticas de defensa. Se

titula “LA BATALLA DEL SOLDADO DE BRONCE” porque el conflicto se inicia con el traslado de una estatua conmemorativa de los soldados caídos en la 2da Guerra Mundial:

“La mañana del 27 de Abril se expande la noticia sobre la estatua del Soldado de Bronce: fue cambiada de lugar. Cerca de las 9 de esa mañana, las páginas webs de bancos, medios de comunicación y organismos gubernamentales del país se pusieron en blanco. Una red de robots informáticos estaba provocando un nivel de tráfico sin precedentes que hacía colapsar los sistemas de uso cotidiano para la población, como los cajeros automáticos o los canales de televisión. Este tipo de agresión se llama Ataque de Denegación de Servicio, o DdoS por sus siglas en inglés. Las páginas oficiales pasaron de tener mil visitas diarias a recibir esa cantidad de tráfico por segundo.” (Fragmento del podcast).

Sobre el cambio de paradigma y lo que implica en términos operacionales, Niss explica que “la Ciberdefensa no es la defensa militar del ciberespacio sino la Defensa del Ciberespacio de interés Militar”. Entonces, por un lado, el objetivo de las políticas de defensa soberanas son las infraestructuras y el tráfico que por allí se genera: tener capacidades de monitorear, diagnosticar y operar sobre ellas.

En el caso de Estonia, claramente no estaba preparada para una ciber agresión de esta magnitud por lo cual la vulnerabilidad era alta. En términos geopolíticos, Roberto Galizia analiza que en “el caso de Estonia fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro”. En los tradicionales ámbitos operacionales, la OTAN es un actor importante pero cuando se produjeron los hechos de Estonia no solo no tenía un procedimiento sino que las características de los ciber ataques le impidieron dar un veredicto concluyentes sobre las responsabilidades, por tanto tampoco hunbo sanciones. Después de los hechos, comenzaron a desarrollarse en el país políticas y estrategias en materia de seguridad informática, al punto de ganarse el mote de “E-Estonia”, prefijo que se le suma a toda palabra para indicar que se encuentra adaptada a la Sociedad de la Información.

Tiempo después, en 2013, luego de tres años de trabajo se publicó el ya mencionado Manual de Tallin, que justamente lleva el nombre de la capital de Estonia donde el grupo de analistas que lo redactaron sindican el primer ataque cibernético contra un país. Si bien no se trata de cuerpo normativo oficial, el manual sirve para tener lo que no había cuando sucedió el ciber ataque de Estonia, un procedimiento, una serie de pasos a seguir y cómo actual en tal caso.

Hoy en día, la soberanía nacional de los Estados se disputa en un nuevo ámbito, que al mismo tiempo afecta a los ya tradicionales. Es necesario entender la magnitud del desafío, no solo entre especialistas e interesados, sino también entre toda la sociedad. Desde sus inicios se busco que internet se consagre como un territorio virtual soberano, horadando la capacidad de acción de las naciones sobre lo que sucedía en su interior. Ahora son las potencias globales y las grandes corporaciones las que, de hecho, actúan sobre las redes, apropiándose del plusvalor que se genera allí y accionan para que se regule lo menos posible. La soberanía sobre las infraestructuras y la propiedad de los datos, resultan de los puntos más conflictivos en las mesas de gobernanza global.

Es deseable que se tome el tema como una prioridad de las agendas gubernamentales y que se desarrollen capacidades para la defensa, así como también que los pueblos comprendan la dimensión de los desafíos de la soberanía en el siglo XXI.

- Niss, Oscar (2021). Ciberespacio. Políticas de Defensa. Desafíos y ejes fundamentales en el contexto actual. Universidad de la Defensa Nacional. Videoconferencia.
- Trama, Gustavo Adolfo (2017). Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional. Ciudad Autónoma de Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.
- Galizia, Roberto Claudio (2014). El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra. Ciudad Autónoma de Buenos Aires: Revista de la Escuela Superior de Guerra, N°588.
- Lenoir, Ricardo (02/10/2017). La batalla del Soldado de Bronce: lecciones del primer episodio de ciberguerra con Rusia. El confidencial.

Público objetivo: Personas de entre 18 y 40 años, interesados en la actualidad global, la tecnología y con interés en profundizar en temáticas nodales.

Plataforma elegida para la publicación: Plataformas de podcast tales como Spotify, Soundcloud, Google Podcast, etc.

Descripción del formato comunicacional: El formato elegido es el podcast, que está en crecimiento por su facilidad de realización, su accesibilidad para el consumo y las posibilidades de producción que presenta. El podcast es un formato que por lo general se utiliza para contenidos profundo y no tan generales, por eso es ideal para el público al que se pretende llegar.

Esquema discursivo general: En este caso, el esquema se desarrolla con una apertura y una introducción permanente, donde se fijan conceptos básicos y generales sobre ciberdefensa, y un contenido original para cada capítulo sobre hechos históricos.

Pieza comunicacional:
https://drive.google.com/file/d/13_3PL_xf8CNSSJk0fjAyyua-8duX_LKV/view?usp=sharing

Breve estrategia de difusión en otros medios/plataformas/redes sociales: Una articulación que da buenos resultados es entre los formatos podcast y twitter, sobretodo para los de contenido más profundo y menos artísticos. Crear una cuenta propia en esta red social de micro-blogging y retroalimentar los capítulos, generar interacciones y diálogos, sumar información complementaria para profundizar, es una buena estrategia.