Protección de activos vinculados con la información: preparación para la Ciberdefensa

Alejandro Moresi [1] *y Antonio Castro Lechtaler* [1,]

[1] Universidad de la Defensa, Escuela de Guerra Conjunta de las Fuerzas Armadas, Proyecto: Observatorio de CiberDefensa - OBSCIBER, Buenos Aires, Argentina, C1426.

alejandro.moresi@conjunta.undef.edu.ar; antonio.castrolechtaler@gmail.com

RESUMEN

Como consecuencia de diversos estudios realizados en distintas instituciones, se define la necesidad de crear un foro de información y conocimiento de la problemática de un nuevo ambiente operacional, que es la Ciberespacio. Éste fue muy bien caracterizado por su virtualidad, y por el Manifiesto de John Perry Barlow con la Declaración de Independencia del Ciberespacio[1].

Hasta nuestro días, éste ámbito de la vida es exclusivo y único del ser humano. Crece y se multiplica a cada instante de la mano de las llamadas: "Tecnologías de la Información y las Comunicaciones" (TIC), y se extiende al mundo de la movilidad, con el continuo crecimiento del uso de diversos equipos que utilizan las transmisiones inalámbricas, los que pueden ir desde un simple teléfono móvil a equipos más sofisticados.

Por otra parte, el acceso de estos equipos al uso de anchos de banda cada día mayores, permiten millones de transacciones por segundo y movimientos de información entre variados puntos del planeta, en una cantidad hasta hace muy poco impensada.

Ello ha provocado un cambio en los hábitos de la humanidad que impacta de manera radical en todos ámbitos de la vida.

La Universidad de la Defensa Nacional (UNDEF), a través del Programa UNDEFI, se encuentra financiando un Proyecto de un Observatorio de Ciberdefensa a través de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas (ESGC), la que para cumplir su cometido, inicialmente se ha asociado mediante convenios ya firmados con la Facultad de Informática de la Universidad de La Plata y con acuerdos con la Subsecretaría de Ciberdefensa del Ministerio de Defensa y el Centro de Estudios General Mosconi de la Escuela Superior Técnica del Ejército, también perteneciente a la UNDEF.

También se espera en el futuro, incorporar otros organismos privados y estatales como parte de este esfuerzo.

Este proyecto para desarrollar y poner en funcionamiento un Observatorio de Ciberdefensa fue recientemente sometido a un concurso púbico con jurados externos, dentro de un Programa de Investigación de la citada universidad denominado UNDEFI.

En dicho marco de referencia, y luego de esa evaluación, al mismo se le otorgó un subsidio especial [1] de $ 100.000,00 para comenzar su ejecución durante el año 2018.

La idea del mismo es brindar al público relacionado e interesado en conocimientos de nivel político, estratégico y tecnológico de alto nivel, tanto en el plano internacional como nacional, información actualizada acerca de problemáticas tales como: Ciberdefensa; Ciberseguridad; Cibercrimen y Ciberterrorismo, entre otros.

Palabras Clave:

Ciberdefensa - Ciberseguridad - Cibercrimen - Ciberterrorismo.

[1] https://danwin1210.me/uploads/%20__%CE%90%C5%8B%E2%82%A3%C3%B8%E1%B4%9Am%CE%94%E2%80%A0%E1%B8%AF%C3%B8%CE%B7%20%C3%8E%C2%A7%20%E2%92%B6%C4%BF%C2%A1%E2%93%8B%CE%9E/manifiesto_de_john_perry_barlow-1.pdf

CONTEXTO

El Observatorio de CiberDefensa fue creado por la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, dependiente de la Universidad de la Defensa (UNDEF). El mismo se encuentra instalado en dicha Escuela Superior y está orientado a satisfacer distintas necesidades de la Defensa Nacional en general y del Ministerio correspondiente en particular.

Tiene por objeto el desarrollo de un programa de investigación, extensión y formación de recursos humanos instituido en el año 2017, conformado por un conjunto de entidades educativas que fueron convocadas por la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas dependiente de la Universidad de la Defensa (UNDEF).

En el futuro funcionará también como un órgano consultivo.

Según ISACA (*Information Systems Audit and Control Association)*[2], se define la CiberDefensa como "*protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*".[2]

La idea es poner en el conocimiento de especialistas en Sistemas de Seguridad Informática, Criptografía, CiberDefensa y Ciberseguridad, etc., mediante informes trimestrales, cuál es el estado del arte en la materia, desde una perspectiva estratégica y técnica.

La información se obtendrá por medios propios y mediante el uso de un motor de búsqueda específico para el tema, para lo cual se ha tomado contacto y se han firmado convenios con otras universidades nacionales.

El motor de búsqueda está configurado para un rastreo de carácter global sobre portales y redes específicas, así como en medios periodísticos y otros similares, desde los cuales se pueda capturar información relacionada con sistemas cibernéticos, los cuales se clasificarán en:

- Tecnologías cibernéticas
- Ataques e incidentes cibernéticos
- Estrategias en el Ciberespacio
- Ciber Forensia

A partir de la información recogida, el equipo de investigación realizará un análisis de la misma y sacará las conclusiones de cómo los hechos censados pueden actuar de forma sinérgica con elementos propios del sistema de ciberdefensa.

Ello permitirá advertir acerca de nuevas capacidades detectadas en el ambiente ciberespacial y establecer la manera en que el mundo orientará su accionar en el espacio cibernético, observar las tácticas y acciones desarrolladas a través del ciberespacio y realizar un análisis tecnológico acerca de cómo los sistemas pueden haber sido vulnerados y/o atacados, cuáles fueron las contramedidas y cómo las mismas han sido detectadas.

Paralelamente, se establecerán las estrategias y características para la preparación y adiestramiento de recursos humanos propios.

La información será diseminada a través de una página web creada al efecto, la que contendrá foros de tratamiento de los temas específicos, además del envío personalizado a entidades, centros estratégicos empresas, medios y personal relacionado o interesado en la materia.

1. INTRODUCCIÓN.

El ciberespacio [3] constituye un ámbito virtual, nuevo e intangible creado por los medios informáticos a partir de los diversos modos de conectarse, los cuales si bien constituyen una infraestructura de comunicaciones y sistemas informáticos, desde el punto de vista físico, los conceptos, ideas y acciones que en ese ámbito circulan son estrictamente procesos abstractos propios de la virtualidad.

Poseen la capacidad de dañar física, intelectual y moralmente, ello los convierte en un ámbito de construcción de poder, en este caso el poder del conocimiento y el convencimiento, de allí la necesidad, por parte de quienes ejercen el poder, de

[2] Asociación de Auditoría y Control sobre los Sistemas de Información.

establecer medidas para su vigilancia, control y explotación.
El elemento de acción en este campo es el software, concepto inherente a la forma de accionar con los medios informáticos y esencia que caracterizada por diferentes nombres: sistemas operativos, navegadores, aplicaciones de trabajo profesional, procesadores de textos, planillas de cálculo, bases de datos, programas de diseño, CAD-CAM, virus, gusanos, troyanos, malware, spyware, ransomware, antivirus, firewall, entre otros.
Todos ellos actúan en el ciberespacio proyectando las capacidades de quien desea ejercer acciones, tales como transmitir una información, generar un conocimiento, promover un espacio de reflexión, diversión o esparcimiento, o quien pretende ejercer el poder desde este nuevo ambiente operacional.
La República Argentina ha iniciado su accionar en el tema de seguridad informática, a través de carreras de postgrado en diferentes universidades y centros de investigación. Un segundo peldaño, en la cuestión ciberespacial, se constituye desde el aspecto de la Defensa en el año 2014, con la creación del Comando Conjunto de Ciberdefensa, Resolución MD N° 343/14 de fecha 14 de mayo de 2014, cuya misión es: "*Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar*".
La seguridad de la información es un aspecto tratado por el hombre desde el principio de los tiempos, se conceptualizó la idea de información como elemento de poder de los estados, en los 80/90 a partir de diferentes estudios. La información comenzó a ser considerada un objeto esencial al poder (más allá de que siempre lo fue).
Fue en el siglo XXI, donde la información y la capacidad de incidir sobre el pensamiento de las sociedades pasaron a tener una preeminencia estratégica superior, que se manifiesta con mayor fuerza e intensidad, durante los procesos de crisis y conflicto. Esto ocurre, tanto en el campo político, como en el militar, el económico o el social.
Esta capacidad, y las características mismas de tratarse de un ambiente completamente nuevo y casi libre de restricciones, permiten que tanto los Estados, como organizaciones lícitas e ilícitas, puedan explotar su empleo para beneficio de la humanidad o para cometer sabotaje, espionaje y otras acciones delictivas.
La característica de intangibilidad, velocidad y capacidad de escalar las acciones que se llevan a cabo en el ciberespacio, constituyen un factor de vulnerabilidad y desestabilización social, que no solo es difícil de prevenir, sino de controlar con el evento en ejecución.
Analizando lo que establece el artículo 2° de la Ley de Defensa Nacional -Ley N° 23.554- es esencial a la Defensa poseer la capacidad de ejecutar medidas contundentes tendientes a impedir la supremacía informática de cualquier posible enemigo de la sociedad argentina [4].

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO.

Las líneas de Investigación y desarrollo son las siguientes:

2.1. Desarrollar un servicio de excelencia, con información en el estado del arte, respecto de la problemática de control y negación del ciberespacio, métodos, tecnologías y estrategias de aplicación.
2.2. Realizar investigaciones sobre el marco de la ciberdefensa de forma general y aplicada.
2.3. Establecer y comprobar los elementos necesarios para tener sistemas de información fiable.
2.4. Estudiar y sugerir propuestas orientadas a la toma de decisiones sobre las políticas en aspectos relativos a la CiberDefensa y Ciberseguridad.
2.5. Crear un Reservorio de Documentación que estimule el estudio y la investigación.
2.6. Realizar y fomentar encuentros entre profesionales y expertos sobre los resultados

obtenidos en investigaciones similares e intercambiar experiencias comunes.
2.7. Elaborar planes de formación sobre temas de Ciberseguridad y CiberDefensa a nivel profesional y para la ciudadanía en general.
2.8 Medir el estado actual y la evolución del bienestar y calidad de vida en base a la mayor concienciación en materia de CiberDefensa y CiberSeguridad.
2.9. Conformar un grupo de analistas relacionados con el área, a los efectos de elaborar estudios y conclusiones sobre los datos obtenidos, que permitan,

- Actuar de forma sinérgica con elementos propios del sistema de ciberdefensa.
- Advertir acerca de nuevas capacidades detectadas en el ambiente ciberespacial.
- Observar el estado del arte en el nivel mundial y su orientación en el cibernético.
- Conocer y difundir tácticas y acciones desarrolladas a través del ciberespacio.

2.10. Investigar los distintos trabajos existentes sobre la seguridad que ofrecen los diferentes tipos de Redes de Comunicaciones [5] para su uso seguro y a los fines de mejorar los aspectos que hacen a la toma de decisiones acerca de su implementación en distintos ambientes.

3. RESULTADOS OBTENIDOS / ESPERADOS.

Como este proyecto es de reciente constitución, a la fecha no se pueden mostrar aún, resultados obtenidos.
Se esperan obtener los siguientes resultados:
3.1. Generar una base de datos sobre CiberDefensa, Ciberseguridad, su estado del arte y de los sistemas asociados a estas materias.
3.2. Generación de indicadores objetivos que permitan la correlación y comparación evolutiva de variables relacionadas con esta temática.
3.3. Publicar y difundir los materiales generados a través de los diferentes estudios e investigaciones.
3.4. Elaborar un reporte anual de CiberDefensa, en el cual se recoja un diagnóstico que permita conocer la situación y cuáles son las herramientas disponibles para la evaluación y la medida de los diferentes fenómenos que intervienen en la percepción de la Defensa.
3.4 Asesorar técnicamente a Fundaciones, Administraciones, Organizaciones, Sociedades, Instituciones y Universidades en materia de CiberDefensa y Ciberseguridad así como seguir los proyectos de cooperación exterior.
3.5. Sistematizar, analizar y procesar datos, para obtener información útil, generar reportes y opiniones de expertos a diferentes usuarios, así como métricas que serán el objeto de este observatorio.
3.6. Creación de materiales pedagógicos dirigidos a los jóvenes en particular y a la ciudadanía en general, en el ámbito de la CiberDefensa.
3.7 Plasmar en un Foro Anual presencial las investigaciones y conclusiones que se van manejando en el ámbito de la CiberDefensa y Ciberseguridad.

4. FORMACIÓN DE RECURSOS HUMANOS.

Desde el año 2017 en este grupo trabajan investigadores formados y categorizados, investigadores en formación, y alumnos de las carreras de grado y posgrado vinculadas con los temas que hacen a la Ciberdefensa y a la Ciberseguridad en el ámbito de la Defensa Nacional, fundamentalmente aquellos pertenecientes a las carreras que se desarrollan en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas; como así también en la Escuela Superior de Guerra (Ejercito), Escuela Superior de Guerra Naval, Escuela Superior de Guerra Aérea y Escuela Superior Técnica del Ejercito.
Durante este año 2018, se sumarán al proyecto nuevos investigadores formados y en formación y alumnos de las distintas Unidades Académicas antes mencionadas.
Existe también la posibilidad de que algunos alumnos de las instituciones mencionadas,

realizaran monografías sobre alguno de los temas que aborda la presente línea de investigación, ya se dentro de los planes de estudio, o como trabajos de fin de carrera. Atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso en abstenerse de realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA.

[1] Resolución Rectoral UNDEF Nº 282/2017 de fecha 27 de octubre de 2017. Expediente Nº 606/2016.

[2] https://www.isaca.org/pages/default.aspx

[3] Julio Gerardo Lucero. La Dimensión Desconocida. El ciberespacio como nuevo ámbito operacional. CEFADIGITAL. Repositorio Digital del Centro Educativo de las Fuerzas Armadas. http://www.cefadigital.edu.ar/bitstream/123456789/225/1/VC%2012-2015%20LUCERO.pdf

[4] Torres Soriano, Manuel. Hackeando a la Democracia: operaciones de influencia en el ciberespacio. Instituto Español de Estudios Estratégicos. 2017.

[5] Corletti Estrada, Alejandro. Seguridad en Redes. Learning Consulting S. L. Madrid. 2016.