



Ministerio de Defensa Argentina

**Diplomatura Internacional en
Comunicación y Defensa Nacional**

UNDEF Universidad de la
Defensa Nacional



Ministerio de Defensa
Argentina

- 2020 - "Año del General Manuel Belgrano" -

Alumno: Osvaldo Jorge Palacio

DNI: 10.102.782

Profesión: Productor periodístico

Locutor Nacional de Radio y TV (Carnet 3035)

Periodista Profesional (Ley 12.908)

Mail: palacios@delabu.com.ar

Celular: 291- 4424747

Domicilio: Pino Hachado 32420 - Bahía Blanca (CP 8000)

Provincia: Buenos Aires, República Argentina

Año: 2020/2021



Ministerio de Defensa Argentina

Diplomatura Internacional en Comunicación y Defensa Nacional

UNDEF Universidad de la
Defensa Nacional



Ministerio de Defensa
Argentina

- 2020 - "Año del General Manuel Belgrano" -

TEMA ELEGIDO:

Ciberdefensa: El nuevo paradigma bélico del Siglo Veintiuno

OBJETIVO GENERAL:

Producción de una pieza periodística escrita, que, relacionada con el tema y que ahonda sobre las nuevas amenazas y las guerras que ya se libran en la red.

INFORME PRELIMINAR:

La tarea está pensada en función de las amenazas existentes en materia de ciberdefensa y sobre los nuevos escenarios de características virtuales, que generan preocupación en nuestro Ministerio de Defensa y en la seguridad de los sistemas de información y comunicaciones en las Fuerzas Armadas. Nuestro país, se encuentra transitando un incipiente camino en esta materia, elaborando políticas y medidas tendientes a robustecer su sistema de defensa nacional, ante potenciales o posibles ciberataques.

Para la producción de la presente consigna, se llevaron a cabo tres conferencias telefónicas con el Roberto Uzal, especialista en Ciberdefensa y Licenciado en Sistemas de la UBA, Ingeniero Químico del Instituto Universitario del Ejército, Especialista en Administración Financiera también por la UBA. Egresó de la Universidad de Belgrano, como Doctor en Administración Universidad de Belgrano. Es docente universitario, investigador y entre otras funciones, organizador y director del Doctorado en Ingeniería Informática y de la Maestría en Calidad del Software de la Universidad Nacional de San Luis. Uzal, además, es teniente coronel (RE) del Ejército Argentino.

Se dio lectura, como consulta, a través de Internet al siguiente material.

Archivo disponible en la UNDEF, Sergio G. Eissa / Sol Gastaldi / Iván Poczynok / Elina Zacarías Di Tullio El ciberespacio y sus implicancias para la defensa nacional

Aproximaciones al caso argentino, Entrevista al Comandante Conjunto de Ciberdefensa, General de Brigada Aníbal Intini (extraída del portal Infobae), “El enfoque argentino sobre Ciberseguridad y Ciberdefensa” de Edgardo Aimar Gago. Bulcourf, Pablo (2004) “Continuidad, cambio y re conceptualizaciones en torno de las nuevas amenazas”, en Ernesto López y Marcelo Saín (comps.); Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil. Bernal: Universidad Nacional de Quilmes.

Castells, Manuel (2006) La era de la información, Buenos Aires: Siglo XXI; La guerra irrestricta o el nuevo reino de las armas de Homar Garcés, J. Marcelo Ramírez (2019) - La Sociedad como blanco de los nuevos tipos de Guerras. XIII Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires, Buenos Aires. LOS CIEGOS Y EL ELEFANTE: EL AMBIENTE OPERACIONAL HÍBRIDO Por CL (R) Gustavo Adolfo Trama, GB (R) Gabriel Jorge Guerrero y GD (R) Evergisto de Vergara; Geopolítica ¿QUÉ ES LA “GUERRA SIN RESTRICCIONES”? del General de División de la Fuerza Armada Nacional Bolivariana: Barrios Quintero.

Ballesteros Miguel Ángel, Hacia una Estrategia de Seguridad Nacional, Instituto de Estudios Estratégicos de España y Feliú, Ortega Luis, El espacio cibernético nuevo escenario de confrontación; “Los Nuevos Conflictos y la Supervivencia como Nación”, por Patricio Trejo publicado por “Zona Militar”, documental (Netflix) “Nada es privado” (dirigida por Karim Amer y Jehane Noujaim), cuya temática es la violación de la privacidad en la era de Internet y las redes sociales y la manipulación de datos. La producción, pone el foco en ese problema.

Clarín: Informe internacional sobre Argentina que es uno de los países que más ataques cibernéticos recibe en la región. La modalidad más repetida es el phishing, una técnica que utiliza links y formularios falsos para robar información; INFOBAE: Artículo “Así se se preparan las FF. AA. argentinas para hacer frente a la guerra electrónica

OPERACIONES MILITARES CIBERNÉTICAS General de División (RE) Evergisto de Vergara Contraalmirante (RE) Gustavo Adolfo Trama y lectura de material de los científicos Rain Ottis y Peeter Lorents; Flores, Héctor, “Los ámbitos no terrestres en la guerra futura: espacio cibernético y aeroespacio, Estado Mayor Conjunto de las Fuerzas Armadas, material del Gabinete de Estrategia Militar - Centro de ESTUDIOS PARA LA DEFENSA NACIONAL UNIVERSIDAD DE BELGRANO; “La defensa cibernética, alcances estratégicos, proyecciones doctrinarias y educativas” por Javier Ulises Ortíz, Claudia Fonseca, Miguel Ansorena Gratarcos y Luz Ivone Perdomo.

Ciberdefensa y ciberseguridad, más allá del mundo virtual, por Robert Vargas Borbúa, Luis Recalde Herrera y Rolando P. Reyes y CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL? UNIVERSIDAD MILITAR NUEVA GRANADA FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD ESPECIALIZACIÓN EN ALTA GERENCIA DE LA DEFENSA NACIONAL

INVESTIGACIÓN PERIODÍSTICA:

Introducción: Se trabajó sobre este tema de actualidad y que es de una realidad que es preciso entender y familiarizarse. Estamos sobre una cuestión que ya domina parte del escenario mundial y tiene implicancias tanto en la paz como en la guerra, que afecta infraestructuras tecnológicas y que cuenta con una gran capacidad de penetración en la actividad humana y en la vida de cada uno de nosotros.

Desarrollo del tema trabajado: El mismo se llevó a cabo luego de leer abundante material sobre el tema e investigar. Se tomó como parámetro la relevancia que tiene la ciberdefensa en el mundo y la importancia de sus ataques, que son una fuente de amenazas para las infraestructuras críticas de los países y que afectan de forma directa y simultánea a millones de personas. Por eso, se hizo hincapié en las estrategias nacionales de protección y sobre la necesidad de generar nuevas capacidades dentro de nuestro Ministerio de Defensa.

Esta publicación, contiene definiciones y conceptos sobre Ciberespacio, Ciberseguridad y Ciberguerra, enfoques sobre la responsabilidad del Estado y sus organismos dependientes y otras explicaciones técnicas. Además, un repaso sobre la denominada Guerra Híbrida y el Derecho Internacional Humanitario en las Ciberoperaciones. Igual criterio sobre la Guerra Irrestricada, el posicionamiento de nuestro país en ese sentido y otras consideraciones.

Presentación de la información

Realizada en formato periodístico de crónica, diagramada y con inserción de material fotográfico. Listo para su publicación en un medio gráfico, en este caso la edición dominical, tamaño tabloide, de un diario de tirada nacional y también para su aparición en su edición digital.

Conclusiones:

Lo realizado permite sostener que la ciberdefensa, es un tema clave a nivel mundial y su interés está expandiéndose rápidamente en nuestro medio. Argentina, ha adoptado un modelo de carácter defensivo y orientado al desarrollo de capacidades.

En este escenario, tomamos parte del ideario del general de brigada Aníbal Luis Intini, comandante conjunto de Ciberdefensa, que sostiene que “los conflictos son variados y su evolución exponencial obliga a las organizaciones a estar permanente actualizados en el conocimiento necesario para realizar las acciones que demandan el acompañamiento de las operaciones del instrumento militar y la protección de los Objetivos de Valor Estratégico. Esta circunstancia impone avanzar sobre la investigación, desarrollo e innovación nacionales, tendientes a evitar la dependencia externa y lograr soberanía tecnológica en esta área. El FONDEF, sostienen las autoridades, constituirá un aporte decisivo para materializarlo, y contribuirá al mejor aprovechamiento del talento tecnológico con que se cuenta”.

Contenidos y elementos a comunicar. Mención y descripción (la pieza o piezas deben ser presentadas en anexo)

El contenido y los elementos a comunicar, se acompañan en el formato elegido para la publicación de esta consigna. Se trata de una nota periodística de interés público.

Material creado para su publicación en la edición dominical de un medio gráfico de tirada nacional y para su plataforma digital.

Estrategia multimedia o transmedia elegida para difundir el trabajo.
Breve descripción y fundamentación:

Este material, de acuerdo al interés y necesidades de difusión, podría adaptarse a los actuales escenarios audiovisuales y comunicacionales multimediales. También el fraccionamiento del contenido para su viralización por múltiples **plataformas, soportes y canales (offline y online)**.



Ministerio de Defensa Argentina

**Diplomatura Internacional en
Comunicación y Defensa Nacional**


UNDEF Universidad de la
Defensa Nacional |  **Ministerio de Defensa
Argentina**
- 2020 - "Año del General Manuel Belgrano" -

Anexo 1:

CIBERDEFENSA

EL NUEVO PARADIGMA BÉLICO DEL SIGLO VEINTIUNO

Lo que no se sabe sobre las nuevas amenazas y las guerras que ya se libran en la red.



Lee la nota completa en la pág. 2

En estos tiempos donde la dinámica de la información le permite a las personas y a los estados cometer sabotajes, espionaje y otras acciones a una velocidad sin precedentes, la amenaza cibernética se constituye en un factor de vulnerabilidad y pérdida del control en la sociedad. Estas medidas deben ser contundentes para evitar catástrofes en un mundo totalmente interconectado y con una dependencia de la informática casi completa. Hoy, nos encontramos dentro de una guerra cibernética silenciosa y global que involucra a países, a compañías multinacionales, escuadrones terroristas y a todo tipo de organizaciones. Si bien en el mundo, se invierten exorbitantes cantidades de dólares anuales para mejorar los sistemas de ataque y defensa, la guerra cibernética se multiplica al infinito alrededor del planeta.

Por definición, un "delito informático" o "ciberdelincuencia" es la ilegalidad que tiene lugar por vías informáticas y cuyo objetivo es destruir y dañar ordenadores, medios electrónicos y redes de Internet. Estos actos, se denominan ciberataques. En el caso de nuestra Defensa Nacional, el abordaje de la problemática exige un trabajo coordinado, con amplio compromiso de las autoridades y la participación de las Fuerzas Armadas, con el asesoramiento de expertos en prevención tecnológica más y una acertada política de ciberdefensa.

Como ya no son tiempos de conflictos en espacios tradicionales como tierra, mar o el aire, surgen nuevas formas de enfrentamiento alejadas del uso de la fuerza militar. Son sistemas omnidireccionales, multimodales, difíciles de detectar y pueden ser confundidos con otro tipo de manifestación. Las sociedades modernas se encuentran bajo agresión a través de herramientas que se utilizan para desestructurar y debilitar los sistemas económicos, financieros, culturales, sociales o tecnológicos.

En el siglo pasado, los enfrentamientos bélicos se dividían convencionales y no convencionales. Los primeros eran los de las fuerzas armadas que usaban medios, estrategias y tácticas tradicionales y las operaciones no usuales eran actividades realizadas generalmente por fuerzas especiales. Actualmente, estos términos han quedado superados ya que en los últimos conflictos se han empleado métodos irregulares los cuales incluyen no solo actos militares, sino también diplomáticos, políticos, legales y sociales, utilizando una combinación de armas convencionales, tácticas irregulares, terrorismo, delincuencia, maniobras de información y operaciones cibernéticas.

En el caso de nuestro país, las denominadas operaciones híbridas, guerra cibernética y la seguridad estratégica eran, hasta hace muy pocos años escenarios de ciencia ficción, alejados de las preocupaciones del Gobierno y de los militares. Hoy, los cambios acelerados en materia tecnológica y las redes terroristas del ciberespacio obligan al Estado a replantearse cuáles son las nuevas amenazas a la Soberanía Nacional.

Esta cuestión es un tema de altísima sensibilidad y de vital importancia en el área de la Defensa ya que implica la protección de la "grilla" eléctrica del país, aseguramiento de las prestaciones de los aeropuertos, seguridad de las destilerías de petróleo y oleoductos, protección de la red ferroviaria, confiabilidad del sistema financiero, funcionamiento de hospitales, confianza en los sistemas de comunicaciones, continuidad de los servicios satelitales y de muchos otros ámbitos esenciales. El cambio de paradigma en cuanto a la Seguridad Informática muestra claramente que resulta estrictamente necesario que se conformen entre los países de la región bloques o alianzas político / tecnológicas.



CIBER- DEL INGL. CYBER-, ACORT. DE CYBERNETIC 'CIBERNÉTICO'. "1. ELEM. COMPOS. INDICA RELACIÓN CON REDES INFORMÁTICAS. CIBERESPACIO, CIBERNAUTA"

Este tipo de agresiones, también obliga a repensar las relaciones internacionales y a redefinir las incumbencias de lo que conceptualmente se entiende como Defensa Nacional. Está probado que gran parte de las armas cibernéticas no son "gusanos" o "worms" que se desplazan autónomamente por las redes de computadoras, la mayoría está compuesta por "bombas lógicas" o "caballos de Troya" que los estados-naciones plantan para determinados fines.

El objetivo es entender que hoy, el futuro está en establecer políticas y estratégicas de defensa del Ciberespacio, donde prime una coordinación más ágil y útil con los servicios de inteligencia, con los proveedores y contratistas privados, ya que el propósito primario es alcanzar objetivos dentro o a través del espacio, con acciones que incluyen operaciones de red de computadoras y actividades para accionar y defender la cadena global de información.

A pesar del tiempo transcurrido desde que se acuñara por primera vez, no es fácil explicar qué es la cibernética y cualquier definición seguramente ha de resultar imprecisa e insuficiente, pues generalmente dentro de la cibernética pueden distinguirse varios puntos de vista.

Para el Diccionario de la Real Academia Española ciber- Del ingl. cyber-, acort. de cybernetic 'cibernético'. "1. elem. compos. Indica relación con redes informáticas. Ciberespacio, cibernauta". Para el mismo diccionario, cibernética (del fr. cybernétique, este del ingl. cybernetics, y este del gr. κυβερνητική, arte de gobernar una nave) es el "estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología". Para Stuart Umpleby y Eric Dent35, el término aparece por primera vez en 1948 como título del libro "Cybernetics" escrito por Norbert Wiener, profesor de Matemáticas del Instituto de Tecnología de Massachusetts, que a su vez lleva un subtítulo que busca aclarar el alcance del ensayo: "Control y Comunicaciones en los Animales y las Máquinas". Para muchos especialistas, Wiener propuso la noción de una segunda revolución industrial. "La primera revolución industrial se produjo cuando las máquinas comenzaron a reemplazar la energía humana y la segunda cuando las máquinas empezaron a reemplazar la capacidad humana para procesar información y tomar decisiones". Otra acepción de la cibernética guarda relación con la electrónica. Según ella, durante la guerra de Vietnam, la investigación en los campus universitarios, apoyados por el Departamento de Defensa Norteamericano, comenzó a ser un tanto controversial. Un resultado de dicha discusión fue que los investigadores financiados por dicho organismo tenían que explicar la relevancia de sus investigaciones con respecto a la misión de las Fuerzas Armadas. Es así como los entendidos en inteligencia artificial, como una forma de justificar la financiación, crearon la idea de que en un futuro las batallas se librarían utilizando robots o sensores electrónicos. De ahí la razón por la que, durante la guerra de Vietnam, la cibernética contribuyó a la idea de un "campo de batalla electrónico". También se encuentra el término "cibernética de segundo orden" que fuera acuñado en 1970 por Heinz Von Foerster en su trabajo titulado "Cybernetics of cybernetics", que se ocupa del observador como parte de lo observado y se refiere a los sistemas que son capaces de modificar su objetivo o finalidad por sí mismos, sin necesidad de ser guiados por alguien o algo desde fuera del sistema. Para el Profesor del Instituto Tecnológico Buenos Aires, Roberto Bloch, "la Cibernética ha comenzado a adoptar una posición epistemológica más constructivista y constituye una disciplina que trata de realizar una conjunción de los datos suministrados por las matemáticas, la neurología, la mecánica electrónica, etc., con el fin de lograr un dispositivo capaz de realizar elevadas y complejas funciones similares al pensamiento". Por tal razón, para la medicina, la cibernética tiene dos desarrollos teóricos principales que son la Teoría de la Información y la Teoría de la Robótica. La primera es la rama más relacionada con el pensamiento, mientras que la otra se relaciona más con el desarrollo de partes funcionales; por ejemplo: prótesis auditivas, piernas ortopédicas, y gracias a la cibernética, existe información médica en abundancia y su accesibilidad no tiene paralelismo en la historia de la civilización.



El uso de computadoras e Internet para diagnósticos y evaluación iniciales, para decidir tratamientos, realizar investigaciones, prevención de enfermedades y - sobre todo - mejorar la vida de los pacientes, podría decirse que casi no tiene límites. También, gracias a las computadoras y a Internet, actualmente se puede operar y proyectar el poder en y desde el espacio cibernético para influir en el comportamiento de las personas o el curso de los acontecimientos.

También ya se libra una nueva forma de guerra, en la que aviones no tripulados o drones realizan misiones mientras su piloto se encuentra a miles de kilómetros de distancia, se puede controlar el sistema radar enemigo para crear información falsa en las pantallas y así desviar su atención hacia blancos inexistentes o identificar a un terrorista a miles de kilómetros de distancia por medio de la biometría.

El Espacio cibernético es lo que técnicamente se denomina un Global Common, entendiendo por tal, el entorno en los que ninguna persona o estado puede tener su propiedad o control exclusivo pero que son básicos para el desenvolvimiento de la vida de las personas y de las colectividades. Son global commons el mar, el espacio extraterrestre, el espacio electromagnético y por supuesto el espacio cibernético.

Para Rain Ottis y Peeter Lorents, "es un conjunto de sistemas de información interconectados dependientes del tiempo y los usuarios humanos que interactúan con estos sistemas". De manera similar, el Dr. Roberto Uzal, consultado para este trabajo, de la Universidad de San Luis, Argentina, lo define como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan". Héctor Flores coronel (RE) del Ejército Argentino, en un libro editado por el Estado Mayor Conjunto de las Fuerzas Armadas de la República Argentina, señala que es "el ámbito electrónico formado por ordenadores en redes y la infraestructura asociada a los mismos".

La Guerra Cibernética es asimétrica por lo que los países más avanzados son los que deben esforzarse en cubrir sus "flancos débiles" derivados del uso intensivo de redes teleinformáticas complejas. Las operaciones militares en el espacio cibernético son bastante similares a las que se llevan a cabo en el ámbito del mar, el aire, la tierra y el espacio. De estos dominios, tres de ellos son reales, y el quinto es virtual, pero con características que requieren una doctrina especializada, una política de empleo, recursos estandarizados entre las Fuerzas Armadas y expertos en el tema.

EL ESPACIO CIBERNÉTICO POSEE CARACTERÍSTICAS DIFERENCIALES DEL RESTO DE LOS ESPACIOS. EN RESUMEN:



- > El espacio cibernético es un entorno único, en el que el atacante puede estar en cualquier parte del globo.
- > En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se exige pues una estrecha coordinación entre todos ellos.
- > La confrontación en el espacio cibernético presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.
- > Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y, a menudo, sin delatarse.
- > Facilita también ejercer el chantaje; pero, al mismo tiempo, la defensa puede utilizarlo para la disuasión.
- > Evolucionan rápidamente siguiendo la evolución tecnológica de las Tecnologías de la Información y la Comunicación.

Lo que debe tenerse presente es que: El término ciberespacio no es neutral. Transmite varias representaciones algunas de las cuales, contradictorias entre sí, son el origen de varias concepciones del ciberespacio que se transcriben en las estrategias de los Estados. Estas representaciones se convierten en una herramienta de geopolítica. Algunos estados, como Rusia, han elegido en su estrategia no utilizar el término ciberespacio y prefieren el concepto de "espacio de información". El uso de un concepto más grande le permite a Rusia superar incluso el ciberespacio para permitir un control sobre la información de una manera global y sin tener en cuenta el vector por la cual se distribuye.



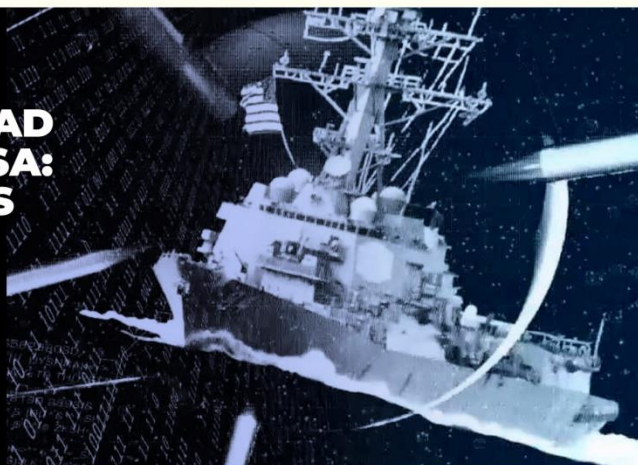
DERECHO INTERNACIONAL HUMANITARIO Y CIBEROPERACIONES DURANTE CONFLICTOS ARMADOS



Las ciberoperaciones son una realidad de los conflictos armados contemporáneos. Al Comité Internacional de la Cruz Roja (CICR) le preocupa el posible costo humano del aumento del recurso a las ciberoperaciones en esos contextos.

- Desde la perspectiva del CICR, el derecho internacional humanitario (DIH) limita las ciberoperaciones durante los conflictos armados, de la misma manera que limita, en ese marco, el empleo de todas las armas, medios o métodos de guerra, sean nuevos o tradicionales.
- Afirmar que el DIH es aplicable a la guerra cibernética no la legitima, de la misma manera que tampoco legitima ninguna otra forma de guerra. Todo uso de la fuerza —de forma cibernética o cinética— por parte de los Estados se rige por la Carta de las Naciones Unidas y las normas correspondientes del derecho internacional.
- Se ha vuelto sumamente importante para la comunidad internacional afirmar la aplicabilidad del DIH al recurso a las ciberoperaciones durante conflictos armados.
- En los últimos años, han ocurrido sucesos que ponen de relieve que las ciberoperaciones que pueden alterar el funcionamiento de infraestructuras civiles esenciales y obstaculizar la prestación de servicios fundamentales a la población. En el contexto de los conflictos armados, la infraestructura civil está protegida de los ciberataques gracias a los principios y las normas vigentes del DIH, en particular, los principios de distinción, proporcionalidad y precauciones en el ataque.
- Durante los conflictos armados, está prohibido el empleo de herramientas cibernéticas que ocasionen y propaguen daños de manera indiscriminada.
- La interpretación que hacen los Estados de las normas vigentes del DIH determinará en qué medida esta rama del derecho protege de los efectos de las ciberoperaciones.

LA CIBERSEGURIDAD Y LA CIBERDEFENSA: ¿QUÉ DIFERENCIAS EXISTEN ENTRE UNA Y OTRA?



En el mundo la Ciberseguridad se ha convertido en un elemento estratégico, y en situaciones extremas ataques de esa naturaleza ponen en riesgo la integridad de un país y de sus ciudadanos. Entonces, el enemigo virtual solo se puede combatir con Ciberdefensa.

Como lo hemos titulado en este artículo, la tecnología de la información y las comunicaciones ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas.

La Organización de las Naciones Unidas, establece cinco elementos fundamentales para desarrollar las estrategias de Ciberseguridad entre los que se encuentra el marco legal para la acción y de medidas técnicas o la aplicación de una cultura de ciberseguridad y de cooperación internacional.

El concepto de Ciberseguridad es complementario al de Ciberdefensa y materializa la defensa nacional digital, pero el desarrollo de conceptos como el Ciberterrorismo o el Cibercrimen, cada vez más presentes en nuestra sociedad.

En Argentina, el Ministerio de Defensa a través de sus mandos dependientes, se encarga de garantizar un acceso al ciberespacio y de dar respuesta ante amenazas o agresiones que puedan afectar a la defensa nacional. También trabaja para garantizar la disponibilidad, integridad y confidencialidad de la información y en la cooperación a nivel internacional.

PROBLEMÁTICA DE CIBERDEFENSA Y CIBERSEGURIDAD EN EL MUNDO

Los Estados realizan cambios permanentes, con el fin de lograr enfrentar las amenazas en el ciberespacio o disminuir su impacto. Los ejemplos son innumerables, entre los que podemos citar a Alemania, con el lanzamiento de su Estrategia de Seguridad Cibernética, la creación de su Centro Nacional de Ciberdefensa y la su Plan Nacional para la protección de Infraestructuras de información. España, que cuenta con un Centro y un Plan Nacional de Protección de las Infraestructuras Críticas y también un Mando Conjunto de Ciberdefensa.

Francia dispone de una Agencia de Seguridad para las Redes e Información y una Estrategia de Defensa y Seguridad de los Sistemas de información. Los países de Latinoamérica realizan aportes constantes a sus estrategias en ciberdefensa y ciberseguridad. Algunos ejemplos son: Colombia, que dispone de diferentes grupos de inteligencia para análisis del ciberespacio. Perú, que cuenta con un organismo de Coordinación de respuesta de Emergencia de Redes Telemáticas con una Política y Estrategia Nacional de Ciberseguridad. En nuestro país, la distinción categórica entre la responsabilidad de la Defensa y la Seguridad Interior no se basa únicamente en la experiencia histórica argentina, sino que tiene un fuerte respaldo consensual. Los ejes centrales de esta separación prohíben expresamente que Fuerzas Armadas realicen tareas de inteligencia criminal, al tiempo que suprimen las hipótesis de conflicto con los países vecinos, y apuntan hacia el efectivo gobierno civil de la Política de Defensa Nacional. En suma, esta delimitación permite establecer también los límites de acción para el Sistema de Defensa Nacional en lo estrictamente referido a la ciberdefensa.

LA GUERRA SIN RESTRICCIONES:

Qiao Liang y Wang Xiangsui, oficiales de la Fuerza Aérea del Ejército Popular de Liberación de China, han definido en su libro "La Guerra Irrestricada" (Unrestricted War), publicado en 1999, los nuevos ámbitos en que se desarrolla la guerra en el mundo contemporáneo como fenómeno social, reduciendo significativamente, como elemento central, la utilización rigurosa de instrumentos militares convencionales, lo cual termina por rebasar el marco de las leyes vigentes y el axioma de la guerra perpetuado por Carl Von Clausewitz.

Ellos explican que «mientras que estamos viendo una reducción relativa de la violencia militar, al mismo tiempo, definitivamente estamos viendo un aumento de la violencia en los ámbitos político, económico y tecnológico». Según este diagnóstico, la violencia dejó de referirse estrictamente al odio, el uso de la fuerza física y las muertes provocadas por armas de cualquier tipo. Ahora, como sucede en diversas latitudes, ésta se evidencia a través de la desinformación inducida (también conocida como postverdad), la militarización de la vida civil y política, el dominio (directo e indirecto) de algunos espacios estratégicos de un determinado país, como la economía y los recursos básicos (mediante la alteración de su valor en el mercado), la aplicación de las leyes estadounidenses y, por consiguiente, la negación de la soberanía nacional para el resto del planeta.

Tempranamente, al darse a conocer públicamente la obra en que asentaron sus ideas, Qiao Liang afirmó que «la primera regla de la guerra irrestricada es que no hay reglas, nada está prohibido». Ya la guerra, en este sentido, adquiere -como teoría- novedosos e inesperados matices, sobre todo, luego de producirse la demolición de las Torres Gemelas de Nueva York que, sirviéndole de excusa al gobierno de George W. Bush, precipitó una escalada guerrillera por parte de Estados Unidos visible, primordialmente en la región del Medio Oriente.

Ellos explican que «mientras que estamos viendo una reducción relativa de la violencia militar, al mismo tiempo, definitivamente estamos viendo un aumento de la violencia en los ámbitos político, económico y tecnológico». Según este diagnóstico, la violencia dejó de referirse estrictamente al odio, el uso de la fuerza física y las muertes provocadas por armas de cualquier tipo. Ahora, como sucede en diversas latitudes, ésta se evidencia a través de la desinformación inducida (también conocida como postverdad), la militarización de la vida civil y política, el dominio (directo e indirecto) de algunos espacios estratégicos de un determinado país, como la economía y los recursos básicos (mediante la alteración de su valor en el mercado), la aplicación de las leyes estadounidenses y, por consiguiente, la negación de la soberanía nacional para el resto del planeta. Tempranamente, al darse a conocer públicamente la obra en que asentaron sus ideas, Qiao Liang afirmó que «la primera regla de la guerra irrestricada es que no hay reglas, nada está prohibido». Ya la guerra, en este sentido, adquiere -como teoría- novedosos e inesperados matices, sobre todo, luego de producirse la demolición de las Torres Gemelas de Nueva York que, sirviéndole de excusa al gobierno de George W. Bush, precipitó una escalada guerrillera por parte de Estados Unidos visible, primordialmente en la región del Medio Oriente.

En el contexto de la geopolítica mundial actual, con poderes fácticos supranacionales que comprometen gravemente la estabilidad política, social y económica de las naciones, además de su soberanía territorial, se ponen en juego todos los medios disponibles y utilizables, militares y no militares, lo que complica la tipificación de las agresiones contra una nación o un gobierno, dando por descartada cualquier consideración de índole moral y ética. Como lo revelara hace siglos el general y estratega militar chino Sun Tzu en su obra "El Arte de la Guerra", «no existen en la guerra condiciones permanentes... en el arte de la guerra no existen reglas fijas. Las reglas se establecen conforme con las circunstancias».

GENERAL ANÍBAL LUIS INTINI: “RECIBIMOS UNA IMPORTANTE CANTIDAD DE CIBERATAQUES POR MES”

Los ciberataques crecen a velocidades aceleradas, mientras los Estados buscan fortalecer sus estructuras y organismos para evitar una catástrofe. ¿Cuál es el rol de las Fuerzas Armadas?



Un ciudadano intenta ingresar en la web de su banco para consultar su saldo y realizar pagos, pero la operación no puede realizarse. En ese mismo instante, en una oficina estatal, un empleado quiere enviar un correo con datos sensibles y tampoco puede. En simultáneo, un grupo de periodistas cubre una protesta con disturbios, pero, al igual que el empleado y el usuario, no pueden subir sus trabajos a la web.

Todo esto, que parece el guion de una película de cine catástrofe, ocurrió de verdad. Fue el 26 de abril de 2007 y afectó a más de un millón de personas: ese día, Estonia protagonizó uno de los primeros ciberataques de la historia y quedó paralizado, y así dejó al descubierto las vulnerabilidades de un Estado frente a los posibles ataques a su estructura digital.

Los conflictos del futuro, en materia de defensa, ya están entre nosotros y avanzan con la misma velocidad con la que lo hace la tecnología.

¿Cómo se preparan las Fuerzas Armadas locales para enfrentar estos desafíos?

DEF dialogó con el general Anibal Luis Intini, quien está a cargo del Comando de Ciberdefensa del Estado Mayor Conjunto, un organismo creado en el año 2014 que debió evolucionar y equiparse ante el avance de los ciberataques.

- ¿Cuál es el terreno sobre el que opera este Comando?

-El ciberespacio es un dominio, tanto físico como virtual, muy complejo. Allí se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de información usando software y hardware interconectado. Lo constituyen tanto la Internet como todas aquellas redes aisladas que se utilizan con finalidades particulares.

A diferencia de los dominios terrestre, aeroespacial y marítimo -donde se pueden desarrollar operaciones militares- el ciberespacio, es de características artificiales. Por ejemplo, en los espacios tradicionales, aún si se interrumpiera el suministro de energía eléctrica o nadie estuviera en esos lugares, ese ambiente seguiría existiendo.

-Ante este fenómeno, ¿por qué hablamos de ciberdefensa?

-Básicamente, el ciberespacio es un ambiente en el que las personas desarrollan actividades de distinto tipo, con una injerencia cada vez mayor en la sociedad. Como tal, se convierte en un escenario de conflictos de múltiples características, desde incidentes relacionados con ciberdelitos hasta aquellos que afectan objetivos nacionales de valor estratégico. En este último caso, es donde se sustenta la necesidad de establecer un sistema que permita proteger, y si es necesario responder, ante amenazas que atenten contra la soberanía nacional, como parte integral de la defensa nacional y del Instrumento militar.

En ese sentido, el control digital de movimientos y accionamiento a través de redes de datos, resulta una gran herramienta de automatismo industrial. Pero, a su vez, presenta un escenario de nuevas vulnerabilidades, que en algún caso pueden alcanzar riesgo de vida. Por ejemplo, tomando el control de la apertura de las compuertas de un dique, se podría inundar un valle con las graves consecuencias que eso acarrearía.

-Estos ataques pueden dañar a una población entera...

-En la historia hay ejemplos: como el sabotaje al sistema digital de control de las instalaciones nucleares iraníes, en 2010, mediante un arma cibernética conocida como Stuxnet, que destruyó las centrifugadoras que purificaban el uranio. Si esa destrucción hubiese sido lo suficientemente violenta, podría haber habido riesgo de vida.

De hecho, a raíz del concepto de Internet de las cosas, hoy existen en el mercado electrodomésticos que pueden ser conectados a la red. Si un atacante tomara el control de alguno de ellos podría generar acciones mecánicas que provoquen daños como roturas o incendios.

En otro orden de magnitud, se puede pensar en ataques, con consecuencias impensadas, contra centrales hidroeléctricas o plantas potabilizadoras de agua corriente o centrales nucleares. -En este contexto, ¿existen objetivos nacionales que se tengan que proteger más que otros?

-Sí, y es necesario proteger los objetivos de valor estratégico del ataque de una fuerza externa que, además, es difícil de identificar. Por lo general, nadie se hace responsable de los ciberataques. Por ejemplo, el que recibió Estonia produjo un caos importante y, si bien se presume que fue Rusia, la atribución nunca se ha podido probar de manera fehaciente.

- ¿Quiénes definen estos objetivos?

-Estamos en un proceso de definición de la nueva Directiva Política de Defensa Nacional, de la que derivará la Política de Ciberdefensa para la jurisdicción. Asimismo, permitirá establecer nuevas responsabilidades para este Comando, además de definir el marco de actuación dentro de la estrategia multicapa, actualmente, en estudio en el Estado Mayor Conjunto de las Fuerzas Armadas. De acuerdo con las leyes de Defensa y Seguridad Interior vigentes, nuestra misión está apuntada a asegurar el adecuado funcionamiento del instrumento militar.

A nivel nacional, la definición de las infraestructuras críticas a proteger corresponde a la determinación que realicen los más altos niveles de la conducción política.

Estas definiciones, y las cuestiones relacionadas con el marco legal asociado, son desafíos que también enfrenta el resto del mundo, dada la reciente aparición de esta problemática.

UN FENÓMENO QUE CAMBIÓ TODO

- ¿Cuáles son las operaciones que llevan adelante?

-Llevamos adelante operaciones de protección de las infraestructuras críticas del Instrumento Militar, junto con las Direcciones de Ciberdefensa de cada una de las Fuerzas. Controlamos permanentemente los sistemas de comando y control, detectando amenazas, determinando posibles ciberataques y evitando que ocurran. Nos preparamos, de ser necesario, para generar una respuesta.

Uno de los objetivos de nuestro trabajo diario es el de dar una alerta temprana ante ciberataques. Esta tarea puede resultar compleja dada la dificultad para establecer límites en el ciberespacio, tal como se definen en los otros dominios, y la determinación de la atribución del ataque.

- ¿Ustedes son atacados?

-Recibimos una importante cantidad de ciberataques por mes. Nuestros sistemas registran incidentes en todo momento. De su análisis se determina cuáles corresponden a ataques y se trabaja sobre ellos para mitigar los efectos que puedan producir. Las amenazas crecen día a día y tienen múltiples orígenes. De hecho, algunos son bastante repetitivos, pero, al conocerlos, ya sabemos cómo proceder. Hay aplicaciones que se encargan de buscar permanentemente vulnerabilidades en las redes y hay otras que realizan un intento dirigido a blancos determinados.

También en el ciberespacio existen diferentes tipos de atacantes con distintas capacidades técnicas: desde aficionados que buscan el desafío de hacer algún daño, hasta países que aplican todo su poder estatal para realizar ciberoperaciones.

-Antes, el ataque se caracterizaba por la invasión de fuerzas extranjeras sobre un territorio y, hoy, eso es muy incierto...

-Además, este tipo de cuestiones ocurren a gran velocidad. Pensando en un conflicto tradicional, se podrían generar acciones que interrumpen el sistema de comando y control del enemigo y asegure el sistema propio para apoyar las operaciones del instrumento militar. Por eso la ciberdefensa es transversal al resto de los dominios.

Es un tema conflictivo porque nadie se hace cargo, incluso hay países que tercerizan los ataques. Un claro ejemplo: desde el exterior alguien puede tomar como rehén una computadora que está en determinado territorio y disparar desde ahí un ataque. Entonces surge la pregunta: ¿quién es el responsable, es un tema de seguridad interior, o se trata de un enemigo externo?

- ¿Qué ocurre después de un ataque?

-Hoy se busca trabajar sobre la ciberresiliencia, que implica tener los medios adecuadamente preparados para que, en caso de ataque, la restitución de los servicios que provee la red sea lo más rápido posible y se produzca la menor pérdida posible.

DESAFÍOS CONSTANTES

- ¿Cómo se capacita al personal?

-Nuestro personal proviene de las tres Fuerzas Armadas. Ellos se capacitan en instituciones civiles y en las Maestrías en Ciberdefensa que hoy dictan la Facultad de Ingeniería del Ejército en Buenos Aires y el Instituto Universitario Aeronáutico en Córdoba (en el marco de la UNDEF). En este momento, estamos avanzando sobre un proyecto para crear el Instituto de Ciberdefensa de las FF.AA. Creemos que va a ser un avance importante ya que la formación de nuestros especialistas y técnicos se realizará de acuerdo con las necesidades concretas de la ciberdefensa y del instrumento militar. Además, realizamos actividades de adiestramiento con plataformas que nos permiten entrenar a nuestro personal en las distintas destrezas requeridas por la organización.

- ¿Es un área costosa?

-Menos que los sistemas clásicos de otros dominios, como un tanque, un avión de combate o un buque de guerra. Por ejemplo, si yo quisiera interferir o engañar un radar utilizando equipamiento requeriría el uso de un sistema electrónico avanzado y costoso. Pero, ingresando maliciosamente al sistema informático que controla el radar, puedo borrar, modificar o incrementar los ecos, distorsionando la observación del operador y, además, con menor inversión y a distancias que no comprometen al atacante. Ahí es donde todo esto toma relevancia. El proceso de concientización en las organizaciones debe estar siempre presente para minimizar la probabilidad de ocurrencia de estos hechos, considerando que, en estos casos, el hombre es el eslabón más débil de la cadena.

- ¿Qué representa el Fondo Nacional de Defensa en este contexto?

-Abre posibilidades importantes. Sobre todo, para la adquisición de material que incremente las capacidades, en cantidad y en calidad. Eso puede traducirse en el aumento de la superficie de protección y en la renovación de licencias e incorporación de tecnología de última generación.

Además, puede representar un interesante salto tecnológico al implementar nuevas herramientas y favorecer, paralelamente, el desarrollo de una infraestructura de generación de conocimientos científicos y tecnológicos vinculados a la defensa y a un aparato industrial capaz de producir equipamiento y sistemas. El FONDEF cumple un rol complementario que oxigena con una clara finalidad: equipar a las Fuerzas Armadas.

- ¿Se pretende crear un sistema nacional de protección del ciberespacio?

-Sí, esto es lo que mencionaba en relación con la protección de los objetivos de valores estratégicos nacionales. A mediano plazo, la proyección es proteger a esos sistemas con el concepto de Sistema Nacional de Protección del Ciberespacio (SINPROCIBER). En ese contexto, los responsables de darles seguridad a esos objetivos podrían estar coordinados de manera de poder prevenir los ataques y mitigar aquellos que se reciban con mayor eficacia.

-Usted egresó en 1983 del Colegio Militar. ¿Cuándo fue que esto se convirtió en un asunto de Estado?

-Cuando egresé ni siquiera se hablaba de este fenómeno. Y, si bien mi capacitación siempre estuvo orientada al área de las comunicaciones y redes de datos, era muy difícil imaginar que uno iba a comandar operaciones virtuales dentro de un ciberespacio. De hecho, en el mundo, los primeros comandos con estas características se crearon a partir de 2010.

(Fuente Infobae por Patricia Fernández Mainardi)

La ciberdefensa es un tema clave a nivel mundial y la red de redes es una fuente de amenazas. En nuestro país cada vez adquiere mayor relevancia el entorno virtual de información e interacciones, es decir, un dominio global y dinámico compuesto la infraestructura de las Tecnologías de la Información (TICs, incluida Internet), con sus redes, sistemas de información y telecomunicaciones.

Frente a esta situación, la responsabilidad primaria de los Estados, es adoptar los recaudos para defender los sistemas de información y sus accesos. Además, hace falta mayor cooperación internacional, ya que a pesar que las potencias mundiales son fuertes bélicamente y poseen ejércitos de vanguardia, las asimetrías de poder se hacen menos notorias en el mundo cibernético y se convierten en igual de vulnerables.

El interés por la ciberdefensa está expandiéndose rápidamente y Argentina produjo un aumento significativo de las normativas específicas en torno al ministerio de Defensa, que mediante el accionar de la Subsecretaría de Ciberdefensa, es responsable de las políticas de seguridad de la cartera y de la definición de estrategias y mecanismos para la protección de la información y los servicios, el despliegue de elementos de ciberseguridad, evaluaciones de intrusión, monitoreo de infraestructuras críticas y transferencia de conocimientos. Este organismo, además, ejecuta la adecuación de procedimientos, la adquisición e implementación de nuevas tecnologías y, la concientización y capacitación de los recursos humanos.

A lo largo de este tiempo (años 2020/21), se llevó adelante un plan de fortalecimiento tecnológico que incluyó la incorporación de nuevas tecnologías de la información y la comunicación para mantener sus funciones esenciales en el contexto de pandemia. Parte de esa estrategia adaptativa, se centró en la habilitación de más de 350 puestos de trabajo a distancia para que el personal del Instituto pueda continuar desarrollando sus tareas desde su casa. En ese marco fue que se aceleró también la renovación de un convenio con ARSAT y se trabajó arduamente en la actualización de la infraestructura de Seguridad Informática, con el fin de elevar los niveles de protección de los activos críticos tecnológicos y mejorar tanto su gestión como su operación.

ARGENTINA: LOS RETOS Y DESAFÍOS QUE PLANTEA LA CIBERDEFENSA



En este nuevo escenario, como ya se hizo referencia en este artículo, tomamos parte del ideario del general de brigada Anibal Luis Intini, comandante conjunto de Ciberdefensa, que sostiene que "los conflictos son variados y su evolución exponencial obliga a las organizaciones a estar permanente actualizados en el conocimiento necesario para realizar las acciones que demandan el acompañamiento de las operaciones del instrumento militar, como así también aquellas operaciones de protección de los Objetivos de Valor Estratégico que sean asignados al Instrumento Militar. Esta circunstancia impone avanzar sobre la investigación, desarrollo e innovación nacionales, tendientes a evitar la dependencia externa y lograr soberanía tecnológica en esta área. El FONDEF, sostienen las autoridades, constituirá un aporte decisivo para materializarlo, y contribuirá al mejor aprovechamiento del talento tecnológico con que cuenta nuestro país.

Otro aspecto que plantea la evolución de la ciberdefensa es la adecuación del marco legal, ya que el actual plexo normativo tiene definidas las cuestiones vinculadas a la defensa y la seguridad, pero no contempla cuestiones relativas a las particularidades de las operaciones en el ciberespacio. Una adecuada normativa al respecto debería derivar entre otras cosas en la definición clara de reglas de empuñamiento en la ejecución de operaciones en el ciberespacio. Por lo tanto, la conducción de las organizaciones de ciberdefensa, en todos sus niveles, también representa un desafío particular porque ubica al conductor en dos dimensiones paralelas: la virtual, donde se desarrollan las acciones, y la real, donde impactan esas acciones. Esta dualidad impide visualizar –porque no existen– los conceptos tradicionales que se manejan en cualquier teatro de operaciones como son el frente, flanco o retaguardia y todas las características convencionales que se quieran referir. En el ciberespacio, las cosas tienden a ser difusas, multidimensionales e intermitentes. El proceso de toma de decisiones convencional debe ser complementado o adaptado en función de la velocidad de ocurrencia de las acciones, y en este difícil entorno el sistema de defensa nacional continúa desarrollando capacidades para contribuir a garantizar la soberanía nacional".

Fuentes consultadas: para la elaboración de la presente consigna, se consultó telefónicamente al Dr. Roberto Uzal y a partir de allí se hizo lo propio con los elementos que se detallan:

Material disponible en la UNDEF

Sergio G. Eissa / Sol Gastaldi / Iván Poczynok / Elina Zacarías Di Tullio El ciberespacio y sus implicancias para la defensa nacional Aproximaciones al caso argentino

Entrevista al general Intini, "El enfoque argentino sobre Ciberseguridad y Ciberdefensa" de Edgardo Aimar Gago.

Bulcourn, Pablo (2004) "Continuidad, cambio y re conceptualizaciones en torno de las nuevas amenazas", en Ernesto López y Marcelo Saín (comps.) Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil. Bernal: Universidad Nacional de Quilmes.

Castells, Manuel (2006) La era de la información. Buenos Aires: Siglo XXI

La guerra irrestricta o el nuevo reino de las armas de Homar Garcés

J. Marcelo Ramírez (2019). La Sociedad como blanco de los nuevos tipos de Guerras. XIII Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires, Buenos Aires.

LOS CIEGOS Y EL ELEFANTE: EL AMBIENTE OPERACIONAL HÍBRIDO Por CL (R) Gustavo Adolfo Trama, GB (R) Gabriel Jorge Guerrero y GD (R) Evergisto de Vergara

GEOPOLITICA: ¿QUÉ ES LA "GUERRA SIN RESTRICCIONES"? del General de División de la Fuerza Armada Nacional Bolivariana: Barrios Quintero

Ballesteros Miguel Ángel, Hacia una Estrategia de Seguridad Nacional, Instituto de Estudios Estratégicos de España,

Feliú, Ortega Luis, El espacio cibernético nuevo escenario de confrontación

"Los Nuevos Conflictos y la Supervivencia como Nación", por Patricio Trejo publicado en "Zona Militar"

Documental (Netflix) "Nada es privado" (dirigida por Karim Amer y Jehane Noujaim), cuya temática es la violación de la privacidad en la era de Internet y las redes sociales y la manipulación de datos. La producción, pone el foco en ese problema.

Clarín: Informe internacional
Argentina es uno de los países que más ataques cibernéticos recibe en la región. La modalidad más repetida es el phishing, una técnica que utiliza links y formularios falsos para robar información.

INFOBAE: sí se preparan las FF. AA. argentinas para hacer frente a la guerra electrónica

OPERACIONES MILITARES CIBERNÉTICAS General de División (RE) Evergisto de Vergara Contraalmirante (RE) Gustavo Adolfo Trama

Lectura de material de los científicos Rain Ottis y Peeter Lorents

Dr. Uzal Roberto, Ciberdefensa-Ciberseguridad: Riesgos y Amenazas.

Flores, Héctor, "Los ámbitos no terrestres en la guerra futura: espacio cibernético y aeroespacio, Estado Mayor Conjunto de las Fuerzas Armadas-

Material del Gabinete de Estrategia Militar - Centro de ESTUDIOS PARA LA DEFENSA NACIONAL UNIVERSIDAD DE BELGRANO

"La defensa cibernética, alcances estratégicos, proyecciones doctrinarias y educativas" por Javier Ulises Ortiz, Claudia Fonseca, Miguel Ansorena Gratarcos y Luz Ivone Perdomo.

Ciberdefensa y ciberseguridad, más allá del mundo virtual, por Robert Vargas Borbúa, Luis Recalde Herrera y Rolando P. Reyes

CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL? UNIVERSIDAD MILITAR NUEVA GRANADA FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD ESPECIALIZACIÓN EN ALTA GERENCIA DE LA DEFENSA NACIONAL

08.02.2021
AÑO 2021

NOTICIAS

Nº **157**

Desde 1988

LO QUE NECESITAS SABER. INFORMACION A TODA HORA

www.noticias.com.ar

Universidad de la Defensa Nacional

Diplomatura Internacional en Comunicación y Defensa Nacional (2020-2021)

Alumno: Osvaldo Jorge Palacio

Trabajo Práctico Final

15 de febrero de 2021



Ministerio de Defensa Argentina

**Diplomatura Internacional en
Comunicación y Defensa Nacional**

UNDEF Universidad de la
Defensa Nacional



Ministerio de Defensa
Argentina

- 2020 - "Año del General Manuel Belgrano" -

Anexo 2:

Fuentes: para la elaboración de la presente consigna, se consultó telefónicamente al Dr. Roberto Uzal y a partir de allí se hizo lo propio con los elementos que se detallan:

Material disponible en la UNDEF

Sergio G. Eissa / Sol Gastaldi / Iván Poczynok / Elina Zacarías Di Tullio El ciberespacio y sus implicancias para la defensa nacional Aproximaciones al caso argentino

Entrevista al general Intini,

“El enfoque argentino sobre Ciberseguridad y Ciberdefensa” de Edgardo Aimar Gago.

Bulcourf, Pablo (2004) “Continuidad, cambio y re conceptualizaciones en torno de las nuevas amenazas”, en Ernesto López y Marcelo Saín (comps.) Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil. Bernal: Universidad Nacional de Quilmes.

Castells, Manuel (2006) La era de la información. Buenos Aires: Siglo XXI

La guerra irrestricta o el nuevo reino de las armas de Homar Garcés

J. Marcelo Ramírez (2019). La Sociedad como blanco de los nuevos tipos de Guerras. XIII Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires, Buenos Aires.

LOS CIEGOS Y EL ELEFANTE: EL AMBIENTE OPERACIONAL HÍBRIDO Por CL (R) Gustavo Adolfo Trama, GB (R) Gabriel Jorge Guerrero y GD (R) Evergisto de Vergara

GEOPOLITICA: ¿QUÉ ES LA “GUERRA SIN RESTRICCIONES”? del General de División de la Fuerza Armada Nacional Bolivariana: Barrios Quintero

Ballesteros Miguel Ángel, Hacia una Estrategia de Seguridad Nacional, Instituto de Estudios Estratégicos de España,

Feliú, Ortega Luis, El espacio cibernético nuevo escenario de confrontación

“Los Nuevos Conflictos y la Supervivencia como Nación”, por Patricio Trejo publicado en “Zona Militar”

Documental (Netflix) “Nada es privado” (dirigida por Karim Amer y Jehane Noujaim), cuya temática es la violación de la privacidad en la era de Internet y las redes sociales y la manipulación de datos. La producción, pone el foco en ese problema.

Clarín: Informe internacional

Argentina es uno de los países que más ataques cibernéticos recibe en la región. La modalidad más repetida es el phishing, una técnica que utiliza links y formularios falsos para robar información.

INFOBAE: Así se preparan las FF. AA. argentinas para hacer frente a la guerra electrónica

OPERACIONES MILITARES CIBERNÉTICAS General de División (RE) Evergisto de Vergara Contraalmirante (RE) Gustavo Adolfo Trama

Lectura de material de los científicos Rain Ottis y Peeter Lorents

Dr. Uzal Roberto, Ciberdefensa-Ciberseguridad: Riesgos y Amenazas.

Flores, Héctor, “Los ámbitos no terrestres en la guerra futura: espacio cibernético y aeroespacio, Estado Mayor Conjunto de las Fuerzas Armadas-

Material del Gabinete de Estrategia Militar - Centro de ESTUDIOS PARA LA DEFENSA NACIONAL UNIVERSIDAD DE BELGRANO

“La defensa cibernética, alcances estratégicos, proyecciones doctrinarias y educativas” por Javier Ulises Ortíz, Claudia Fonseca, Miguel Ansorena Gratarcos y Luz Ivone Perdomo.

Ciberdefensa y ciberseguridad, más allá del mundo virtual, por Robert Vargas Borbúa, Luis Recalde Herrera y Rolando P. Reyes

CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL? UNIVERSIDAD MILITAR NUEVA GRANADA FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD ESPECIALIZACIÓN EN ALTA GERENCIA DE LA DEFENSA NACIONAL



Ministerio de Defensa Argentina

**Diplomatura Internacional en
Comunicación y Defensa Nacional**

UNDEF Universidad de la
Defensa Nacional |  **Ministerio de Defensa
Argentina**
- 2020 - "Año del General Manuel Belgrano" -

Anexo 3:

Entrevistas.

Telefónica al especialista en ciberdefensa, Dr. Roberto Uzal

Reproducción de un reportaje realizado por la periodista Patricia Fernández Mainardi, para el diario Infobae, al titular del Comando Conjunto de Ciberdefensa, general de brigada Aníbal Luis Intini.