AÑO 8 - Nº 49 OCTUBRE 2021

cedef

CENTRO DE ESTUDIOS
PARA LA DEFENSA NACIONAL
UNIVERSIDAD DE BELGRANO

CIBER

DEFENSA

Año 8 - Nº 49
Octubre de 2021

Universidad de Belgrano

Presidente:
Doctor Avelino Porto

Vicepresidente de Gestión Institucional:
Profesor Aldo J. Pérez

Vicepresidente de Gestión Técnica y Administrativa:
Doctor Eustaquio Castro

Centro de Estudios para la Defensa Nacional (CEDEF)

Director:
Doctor Horacio Jaunarena

Colaboraciones:
Fundación SenD

Contacto:
Zabala 1837 – C1426DQG
4788-5400
cedef@ub.edu.ar

LA DIMENSIÓN SIN FRONTERA

Con el advenimiento y el desarrollo cibernético nos hallamos frente a un fenómeno que producirá cambios tan importantes en nuestras vidas y en las formas que tenemos de proteger muestra seguridad, solamente comparables con los que produjo a su tiempo, la imprenta.

Las concepciones tradicionales acerca de muchos principios entran en crisis: el concepto de soberanía de un Estado, vinculado íntimamente con la territorialidad, aparece insuficiente y ahora se comienza a considerar que pasa fundamentalmente por su capacidad de garantizar la seguridad de sus ciudadanos.

Hoy, no estamos en capacidad de determinar el lugar geográfico desde el cual se produce un ataque, tampoco podemos saber si está perpetrado por un ejército organizado o un simple agrupamiento. Las armas son mucho más baratas, su adquisición es muy sencilla y es imposible garantizar la invulnerabilidad de un objetivo. En el ciberespacio operan Estados y empresas particulares, también delincuentes.

En nuestra patria debemos darle al problema toda la importancia que tiene para el futuro de nuestra defensa. Podremos descubrir entonces que, además de las amenazas que desarrolla, contiene un conjunto de oportunidades a nuestro alcance.

Dr. Horacio Jaunarena
Director del CEDEF

INTRODUCCIÓN

CONCIENTIZAR

Hace más de un quinquenio y con el objeto de concientizar sobre la materia, el Director de este Centro de Estudios prologaba aquel Boletín sobre Ciberdefensa, resaltando que la modernidad había introducido un nuevo espacio y forma de conflicto, que si bien no estaba plenamente asumido, siempre estaría activo y que nadie podría escapar de él.

Asimismo, agregaba que el ciberespacio constituía una nueva dimensión creada por el hombre, en la cual era muy difícil atribuir una agresión, generando una nueva preocupación para los Estados, siempre que su violación afectaba la seguridad individual y colectiva, al dañar el funcionamiento del Estado, exigiendo su protección, así como la información y educación de la población para prevenir sus efectos.

Resaltaba en aquella oportunidad la condición de constituir un ámbito común y global, semejante al mar internacional pero virtual, donde existe una seria dificultad para definir fronteras y soberanía, impactando en el orden mundial.

En dicho marco, la ciberguerra no sólo constituye un conflicto sin ruidos ni armas, sino que es un delito altamente rentable, estableciendo un reto al equilibrio de apertura y libertad.

Habiendo trascurrido casi seis años desde aquellas declaraciones y en virtud de la acelerada evolución generada, retomamos la delicada tarea de contribuir a la necesaria concientización sobre sus amenazas y la exigencia de generar adecuadas respuestas.

En dicho marco, este Centro de Estudios desarrolló durante el pasado setiembre, las Jornadas denominadas **“La seguridad en el ciberespacio, dimensión sin fronteras”**, en las cuales se expusieron los siguientes asuntos al público en general:

1. **“Cibercrimen, una amenaza permanente - Análisis de la situación actual en la Argentina y en el mundo – Ciberataques a cadenas de producción”**, por parte del Lic. (UTN) Cristian Borghello.

2. “**Errores producidos por interferencias electromagnéticas aleatorias o intencionales en la transmisión de datos sobre las redes**” y “**Las consecuencias sociales y tecnológicas como parte del conflicto en el ciberespacio**”, por parte de la Dra. Felicitas Arias (Observatoire de Paris, Université PSL, CNRS Sorbone Université, LNE Presidente de la División A WG Time Metrology Standards de la International Astronomical Union (IAU).

3. “**La seguridad de la información en el ciberespacio y su efecto en la protección del patrimonio del conocimiento**”, por parte del Lic. (UTN) Marcelo Cipriano, Licenciado en Matemáticas, Especialista en Criptografía y Seguridad Teleinformática por la Facultad de Ingeniería del Ejército. Coordinador de la Maestría en Ciberdefensa (FIE-UNDEF)

PARTICULARIDAD

Con el fin de acordar conceptos para el desarrollo de un tema que ha irrumpido recientemente en nuestra realidad y que nos afecta individual, social, políticamente e incluso a nuestra seguridad, convenimos que el "ciberespacio" constituye ***un ámbito de creación humana y temporal, que genera un elemento nuevo y de preocupación para los Estados, que afecta fundamentalmente el patrimonio individual, social, nacional y transnacional***.

En nuestro país, mantenemos un atraso dentro del contexto internacional en general y particularmente en relación con otras naciones de la región. Probablemente sea consecuencia de la falta de adecuadas políticas de Estado en tan sensible área de la defensa.

Sin duda, la ciberseguridad constituye una exigencia para la defensa nacional, especialmente de la concientización en todos los ámbitos, siempre preservando la faz ética y moral en la materia.

En el marco de lo expresado precedentemente y desde la visión de la Seguridad y Defensa de una Nación, destacamos las principales particularidades que afectan este ámbito cada vez más imprescindible y vital para la sociedad:

1. El carácter global, que trasciende al individuo, a la comunidad, a la nación y a toda organización de la sociedad.

2. La dificultad para atribuir el origen de una agresión, constituyendo una complicación para el Estado.

3. Su naturaleza política, en tanto constituye un ámbito donde la persona expresa su voluntad con plena libertad.

4. El perjuicio que genera su afectación al funcionamiento del Estado y especialmente a su seguridad.

EXIGENCIAS

Las precedentes particularidades imponen las siguientes exigencias para un adecuado tratamiento y gestión, especialmente por parte del Estado:

1. Convenir una terminología de entendimiento, la cual aún se encuentra en discusión, dificultando su eficiente tratamiento.

2. Tratar en forma integrada la ciberseguridad y la ciberdefensa para trazar una estrategia eficiente.

3. Fomentar el debate entre todos los sectores de forma integrada, incluyendo gobierno, técnicos, académicos, juristas, privados, etc.

4. Mantener adecuadamente informada a la sociedad.

5. Educar sistemática y asistemáticamente sobre la materia, incluyendo la materia en las currículas de todos los niveles de la educación.

6. Definir una política nacional, que considere:

   a. El marco legal para la prevención y la acción.

   b. El diseño de estrategias y protocolos obligatorios.

   c. La concientización y culturización en los ciudadanos.

   d. La cooperación particularmente en el marco de organizaciones internacionales, en virtud de constituir una amenaza que impacta en el orden internacional.

7. Evaluar los perjuicios y considerar las acciones para salvar los efectos de la diferencia conceptual entre seguridad y defensa, siempre que afectara cualquier estrategia y acción en este ámbito.

CIBERSEGURIDAD Y CIBERDEFENSA

Actualmente, la evolución de la tecnología e infraestructura digital permitieron el enlace permanente en prácticamente todo el planeta, generando una creciente dependencia de los sistemas entrelazados; creando demanda de conectividad mediante una integración cada vez mayor de las Tecnologías de la Información y la Comunicación (TIC).

Junto al avance de las TIC, se fue incrementando la vulnerabilidad de las infraestructuras críticas y el ciberespacio, dominio donde se torna difícil atribuir una agresión, generando una seria complicación para la seguridad de los Estados.

En dicho marco, la ONU definió la "guerra cibernética" como: *el uso de computadoras o medios digitales por un gobierno o con el conocimiento explícito o la aprobación de ese gobierno contra otro Estado, o propiedad privada dentro de otro Estado, incluyendo* el acceso *intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente*.

También, hace casi trece años, la Directiva Europea "2008/114/CE" estableció como "críticas" las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de la Administraciones Pública. Ello fue así, en virtud la producción y distribución de dispositivos que podrían ser usados para subvertir la actividad dentro de su jurisdicción territorial.

En la misma línea, la Unión Internacional de Telecomunicaciones emitió, en 2010, la recomendación UIT-TX 1205 por la cual definió la "ciberseguridad" como "*el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".* Dichos son todos los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimediales, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

Desde el punto de vista de la defensa, estas nuevas tecnologías han producido un cambio trascendental. Hoy, las nuevas capacidades de los sistemas de información y del ciberespacio mejoran la eficacia operacional de las fuerzas armadas, mediante las capacidades para combatir y ganar en el ciberespacio, imponiendo cambios en las organizaciones, doctrina, infraestructura, logística, capacitación y adiestramiento de las fuerzas militares.

Este cambio obligó a modificar los conceptos y doctrinas que se aplicaban a la confrontación clásica, que debieron ser adaptados a las exigencias del nuevo escenario virtual. Este proceso de adaptación constituyó, en muchos países, el punto de partida para la definición y la creación ordenada de una capacidad de ciberdefensa que no sólo contemplara la organización, sino también los recursos humanos, el material, la infraestructura, la logística, la información, el adiestramiento y la doctrina.

Lo natural y lógico es que el gobierno nacional elabore una estrategia de ciberseguridad alineada con las respectivas estrategias de seguridad y considerando que la Defensa Nacional no sólo es parte, sino contribuye sustancialmente con sus medios y acciones en el logro de la seguridad del Estado, en los términos fijados por la Asamblea General de la ONU: "*La condición en que los Estados pueden libremente continuar con su desarrollo y progreso, al no existir peligro de un ataque militar, presión política o coerción económica*".

El principal objetivo de cualquier estrategia de ciberseguridad y ciberdefensa deberá establecer un mando único que coordine las acciones y a los actores involucrados en la lucha contra las amenazas en el ciberespacio. Entre ellos, deberán coordinarse las organizaciones públicas y privadas, los técnicos, académicos, juristas, etc.; resaltando la necesidad de cooperación internacional, en virtud del carácter global de amenaza.

En línea con las estrategias diseñadas, deberá ser definida la Doctrina Militar de Defensa Cibernética con la finalidad de establecer los fundamentos doctrinarios de ciberdefensa para generar unidad de pensamiento, contribuir con las actividades conjuntas y la interoperabilidad en el ámbito regional en términos de capacidades militares y de inteligencia.

Entendiendo la ciberseguridad como un fin y la ciberdefensa como medio para alcanzarla, esta última deberá garantizar la libertad de acción de las operaciones militares en el ciberespacio y apoyar las respuestas coordinadas entre los diferentes actores, tanto nacionales como internacionales, ante un ciberataque que afecte la defensa nacional.

En ese marco, será imprescindible informar, educar y mantener una estrategia de ciberseguridad y ciberdefensa integral e integrada en el ámbito internacional.

Como ejemplo y antecedente, en la República Federativa de Brasil, la seguridad cibernética se encuentra a cargo de la Presidencia de la República, y la defensa cibernética, a cargo del Ministerio de Defensa, por medio de las Fuerzas Armadas.

REFLEXIÓN

¿SE PODRÁ ENFRENTAR LA CIBERGUERRA CON UNA POLÍTICA DE DEFENSA NACIONAL “PSICOTICA” O “DISOCIADA”?

Por Santiago Mario Sinopoli

Dice la Ley de Defensa Nacional N° 23.554 (LDN): “Art. 2° – La Defensa Nacional es la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes”.

Esta norma no hace más que dar los instrumentos jurídicos que requiere uno de los objetivos preambulares, la defensa común, y que también exige el artículo 21 de la Constitución Nacional (CN), cuando instituye el Órgano Castrense, con base democrática, para la defensa de la patria y dicha carta magna.

La defensa común antes mencionada no sólo se refiere al empleo de las fuerzas militares ante ataques externos que afecten la soberanía de la nación, sino que es comprensiva del orden interno del país, en el cual, según manda la CN, llegado el momento, se puede hacer uso de las Fuerzas Armadas para defender el sistema constitucional.

Pero la historia quiso que, a partir de 1988, se redujera la competencia del instrumento militar a enfrentar agresiones de origen externo, guardándose silencio ante la necesidad de emplear los “ejércitos” en el marco interno.

Esto constituyó el inicio de una política “psicótica” o “disociada” de la defensa nacional, ya que se elaboró una defensa común sin conexión con la realidad social o, dicho de otro modo, creando el gobernante de turno su propia realidad, porque respondía a la ideología que sostenía, más que como verdad racional, como dogma de fe.

La “psicosis” es una alteración del campo vivencial y del campo práctico en las personas, que crea una duradera pero variable desadaptación entre los sujetos y el medio ambiente y, en última instancia, destruye pasajera o definitivamente la inestable fórmula de relación entre ambos (sujeto y

medio ambiente). En materia de defensa nacional, desde 1988, se destruyó casi en forma permanente la conexión entre los gobernantes argentinos y el medio ambiente o realidad social.

Este pensamiento disociado de la realidad, que separó la agresión externa del conflicto interno -el enemigo de la patria sólo debería provenir de afuera de sus fronteras-, en cuanto al uso del instrumento militar, tuvo un duro golpe, con el ataque terrorista al Cuartel Militar en La Tablada (enero de 1989) y, debido a ello, la relación de los sujetos, hasta ese momento alejada de la realidad, volvió a tomar cierto contacto con el medio ambiente. Por ende, se emitió la Ley de Seguridad Interior 24.059 (1991) que, con ciertos rodeos, permitió el empleo de las Fuerzas Armadas en materia de defensa común "interior", que es en definitiva cumplir con la parte del artículo 21 antes citado, que pone además como fin de las fuerzas armadas la defensa de la constitución.

Pero como las mentes psicóticas se caracterizan por no tener noción de que padecen una enfermedad mental -en cambio el neurótico, que también tiene un problema de adaptación con la realidad social, tiene conciencia de su problema-, los gobernantes de la Argentina, que viven "inmersos" en su "propio mundo", al " irreal" uso de las fuerzas armadas sólo ante agresiones externas agregó otra limitación más al empleo de las fuerzas armadas ante ataques del exterior, que consiste en que la agresión debe provenir de las fuerzas armadas de otro Estado.

Así las cosas, dice el Decreto Nacional N° 727/ 2006: "Artículo 1º — Las Fuerzas Armadas, instrumento militar de la defensa nacional, serán empleadas ante agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s, sin perjuicio de lo dispuesto en la Ley Nº 24.059 de Seguridad Interior y en la Ley Nº 24.948 de Reestructuración de las Fuerzas Armadas en lo concerniente a los escenarios en los que se prevé el empleo del instrumento militar y a las disposiciones que definen el alcance de dicha intervención en operaciones de apoyo a la seguridad interior. Se entenderá como agresión de origen externo el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas".

En casos de agresiones externas a la patria, deberían estar a cargo de fuerzas militares del Estado que produce el ataque, para usar las fuerzas uniformadas del país. Si no se evidencia esta "equivalencia", el instrumento militar de la Argentina debe permanecer en sus cuarteles.

Esta disociación entre el sujeto y la realidad social en materia de defensa nacional negó la existencia de los atentados del 11 de septiembre del 2001 en los Estados Unidos de Norteamérica, que son una réplica en mayor escala de los actos terroristas sucedidos en la Argentina contra la Embajada de Israel (marzo de 1992) y la AMIA (julio de 1994), hechos que muestran un nuevo paradigma en materia de defensa nacional. El crimen organizado y el terrorismo internacional son capaces de poner en jaque la soberanía de un país, como un ejército profesional.

Así lo entendió el Consejo de Seguridad de las Naciones Unidas al emitir resoluciones referidas a los ataques terroristas del 11-S, reconociendo el derecho inmanente de legítima defensa del Estado frente a los ataques de un grupo terrorista.

A partir de 2018, un nuevo gobierno asumió en el país y la limitación que al uso de las fuerzas armadas en el marco externo imponía el Decreto N° 727 /2006 sufrió una modificación, mediante el Decreto N° 683/2018, quedando la redacción de la norma así: "ARTÍCULO 1°.- Las Fuerzas Armadas, instrumento militar de la defensa nacional, serán empleadas en forma disuasiva o efectiva ante agresiones de origen externo contra la soberanía, la integridad territorial o la independencia política de la REPÚBLICA ARGENTINA; la vida y la libertad de sus habitantes, o ante cualquier otra forma de agresión externa que sea incompatible con la Carta de las Naciones Unidas".

El cumplimiento de esta misión primaria no afecta lo dispuesto en la Ley N° 24.059 de Seguridad Interior y en la Ley Nº 24.948 de Reestructuración de las Fuerzas Armadas, en lo concerniente a los

escenarios en los que se prevé el empleo del instrumento militar y a las disposiciones que definen el alcance de dicha intervención en Operaciones de Apoyo a la Seguridad Interior.

La exigencia de que las fuerzas militares fueran usadas sólo si la agresión externa provenía de fuerzas armadas de otro país se derogó, quedando ajustada la Reglamentación de la Ley de Defensa Nacional a la realidad social y, por supuesto, a dicha ley y lo que manda la Constitución Nacional.

La psicopatía o disociación imperante en el tema de la defensa nacional pareció remitirse (curarse), y se estableció una conexión positiva entre la mente de los sujetos y el medio ambiente.

Pero tal remisión o cura de la patología fue transitoria, porque ante la aparición de un nuevo gobierno nacional, mediante el Decreto N° 571 del 2020, la oscilante política en materia de defensa nacional volvió a instalar el artículo 1 del Decreto 727/ 2006 antes transcripto y, con ello, el principio que rezaría: “Podemos usar nuestras Fuerzas Armadas si el ataque externo es de las fuerzas armadas de otro país”.

La desconexión de la política de defensa con la realidad vuelve a mostrar sus “síntomas”, en la Directiva Política de la Defensa Nacional (DPDN 2021), donde se reitera que: “1) La Misión Principal del INSTRUMENTO MILITAR consiste en disuadir, conjurar y/o repeler agresiones militares externas de origen estatal, lo cual constituye el principio ordenador de su diseño, planificación, organización, despliegue y funcionamiento. Siguiendo el consenso político, institucional y normativo fijado desde la aprobación de la Ley N° 23.554 de Defensa Nacional, en el presente documento debe entenderse la frase ‘agresión de origen externo’ como el uso de la fuerza armada por parte de un Estado en contra de la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier forma que sea incompatible con lo establecido por la CARTA DE LAS NACIONES UNIDAS”.

Ahora bien, la mirada “psicótica” de la defensa nacional argentina tiene una profundización cuando la DPND trata el tema de la ciberguerra o ciberdefensa: “De modo más específico, resulta crucial tomar en consideración las dimensiones de la defensa relacionadas al ciberespacio. Este ámbito ha generado replanteos sobre las tradicionales categorías con las que se abordaba la ‘guerra real’, exigiendo una rápida adaptación por parte de los sistemas de defensa. En las últimas décadas, muchos países han reorientado esfuerzos y recursos para resguardar su ámbito ciberespacial.

Una de sus principales características es que, con medios y reglas propios, no constituye un “espacio en sí mismo”, sino que se trata de una dimensión que atraviesa a todos los espacios tradicionales (tierra, mar, aire y espacio). Si bien las acciones de ciberguerra poseen su origen en el ámbito virtual de los sistemas informáticos y las redes de comunicación, también pueden impactar sobre el mundo físico. Esto es tangible en los recaudos cada vez más expandidos en ámbitos tan variados como el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, las comunicaciones militares y la capacidad de comando y control, entre otros”.

¿Por qué hablamos de aumento en la disociación de la política con la realidad en el tema de la defensa nacional? La respuesta es sencilla. Puede que no se sepa de dónde proviene un ciberataque de poca o gran magnitud y, por ende, si no es factible determinar si la agresión es producto de fuerzas armadas de otro Estado, el instrumento militar de la ciberdefensa no se podría activar, porque los límites legales lo impiden. El ataque informático no lleva “uniforme militar”, sus componentes no tienen a la vista grado o algo que los distinga como miembros de una fuerza armada regular.

Habría que observar la realidad social y las experiencias vividas por otros Estados, para darse cuenta de que la exigencia de que sólo se use el instrumento militar argentino cuando tenga “enfrente” al instrumento militar de otro país, para la ciberbeligerancia no sirve.

Lo que pasa es que el sujeto psicópata vive su “mundo”, sin contacto con el medio ambiente y, si elabora una política de defensa nacional, la va a pensar para ese mundo “irreal” o de fantasía. Este sujeto no va a entender lo que sucedió en Estonia en abril y mayo del 2007, cuando una andanada de ciberataques paralizó las actividades del gobierno y financieras en forma total, mediante programas de ejecución automática desde servidores ubicados en Egipto, Vietnam y Perú.

Los ataques, perfectamente organizados y coordinados, tuvieron características y propósitos bien definidos, circunstancia que indica que los autores formaban parte de una estructura compleja y dotada de recursos para tal fin, capaz de paralizar al Estado de Estonia, y sin que se pudiera identificar a los agresores como otro Estado, y menos que integraban una fuerza armada.

Estonia, durante el ataque informático, se comunicó inmediatamente a sus aliados de la OTAN y de la Unión Europea, quienes comenzaron a colaborar para anular los programas de ejecución automático que tenían en jaque a casi toda una nación.

He aquí un ejemplo de ciberguerra a gran escala contra la infraestructura crítica de un país, en donde el enemigo no vestía uniforme militar de algún Estado agresor, como prevé nuestro régimen jurídico de la defensa nacional, para que puedan actuar las fuerzas armadas en defensa de la patria.

El ataque a Estonia terminó gestando el Manual de Tallin, que lleva justamente el nombre de la capital de dicho país, y que es una consecuencia directa de las preocupaciones compartidas por los Estados miembros de la OTAN respecto de los ciberataques, luego de los incidentes ocurridos en 2007. En este manual se prevé la legítima defensa de un Estado en los términos del artículo 51 de la Carta de las Naciones Unidas. Más aún se habla de la legítima defensa anticipada, ya que más que la represalia ante un ataque, para el trabajo el cibernético, lo que interesa es mantener la indemnidad de la propia estructura estatal.

Si el Estado dejara de actuar, perdería la posibilidad de defenderse de manera efectiva. Por ello, debe tenerse en cuenta la legítima defensa anticipada como una verdadera posibilidad frente a ataques cibernéticos, ya que no sería razonable obligar a un Estado que puede evitar los efectos de un ataque armado cuya realidad conoce (es decir, no es una mera sospecha, sino un ataque en desarrollo, ya desencadenado), a mantenerse a la espera de que se produzca el resultado del ataque armado para actuar después como reacción. Quizá para entonces su poder de reacción defensiva haya sido diezmado.

Terminando con este razonamiento, volvemos a la patología que se sufre al diagramar las políticas de defensa nacional, marcando que el instrumento militar argentino sólo entra en acción con un equivalente de otro Estado, y ante ello nos preguntamos: Con esta postura, ¿quedamos en estado de indefensión, sobre todo en supuestos de agresiones externas?