AÑO 2 - Nº 13 DICIEMBRE 2015

cedef

CENTRO DE ESTUDIOS
PARA LA DEFENSA NACIONAL
UNIVERSIDAD DE BELGRANO

CIBERDEFENSA

En la era donde la revolución de la información permite a los individuos y a los estados cometer sabotaje, espionaje y otras acciones a una velocidad y escala sin precedentes, la amenaza cibernética se constituye en un factor de vulnerabilidad y pérdida del control en la sociedad moderna que exige rápidas y contundentes medidas para evitar una catástrofe

Año 2 - Nº13

Diciembre de 2015

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 interno 5075
cedef@ub.edu.ar

TOMAR CONCIENCIA

La modernidad introdujo un nuevo espacio y forma de conflicto que, si bien no está plenamente asumido, siempre está activo y nadie puede escapar de él.

El ciberespacio constituye una nueva dimensión creada por el hombre en la que es difícil atribuir una agresión y que genera una nueva preocupación para los estados.

Se trata de un ámbito común y global, semejante al mar internacional pero virtual, donde existe una seria dificultad para definir fronteras y soberanía, lo que impacta en el orden mundial.

Su violación afecta la seguridad individual y colectiva al dañar el funcionamiento del estado, por ello este debe protegerse, informar y educar a la población para prevenir sus efectos.

La ciberguerra no solo se trata de una guerra sin ruido ni armas, sino también de un delito rentable y, por ello, la ciberdefensa constituye un reto que impone equilibrar el anhelo de la apertura y la libertad, con los reparos frente a las amenazas crecientemente sofisticadas.

Cualquier proyecto debería considerar el desarrollo de un marco legal y protocolos, el diseño y aplicación de una estrategia organizacional y, especialmente, la generación de una cultura nacional ciudadana, similar a lo que fue la "Nación en armas" en el siglo XIX.

"Aquí el más fuerte es el más débil"

Doctor Horacio Jaunarena
Director del CEDEF

CIBERSEGURIDAD Y CIBERDEFENSA

En la actualidad, los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. La demanda de Internet y de conectividad digital exige una integración cada vez mayor de las Tecnologías de la Información y la Comunicación (TIC) en productos que anteriormente funcionaban sin estas tecnologías, por ejemplo automóviles, edificios e, incluso, sistemas de control para las redes de distribución eléctrica y de transporte. Prácticamente todos los servicios modernos dependen de la utilización de las TIC.

A medida que fue aumentando la dependencia con respecto a las TIC en el plano mundial, también se incrementó la vulnerabilidad ante los ataques a las infraestructuras críticas[1] a través del ciberespacio. Ello se debió y se debe a que el ciberespacio carece de fronteras geográficas, es artificial y cambiante y la tecnología que en él se puede llegar a emplear no es muy costosa y se encuentra al alcance de cualquiera.

Por otra parte, es difícil atribuir una agresión en este ámbito, lo que genera una complicación para los estados, pues la mayoría de las acciones son anónimas y sus autores pueden variar desde adolescentes con intenciones simples hasta organizaciones criminales, en ciertos casos utilizadas por algunos gobiernos.

Es así como el Consejo de Seguridad de las Naciones Unidas, mediante la resolución 1113 del 2011, definiera a 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.

[1] **“Aquellas 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 las Administraciones Públicas“. Esta definición fue establecida por la Directiva europea: 2008/114/CE del 8 de diciembre de 2008.**

> -la producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna.

Por su parte, la Unión Internacional de Telecomunicaciones, en su resolución 181, recomendación UIT-TX 1205 de noviembre de 2010, definió “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. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad.

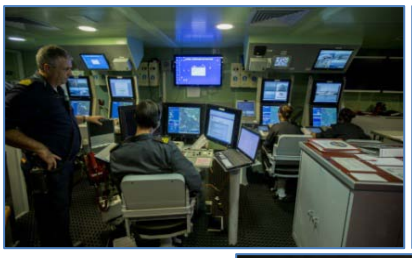
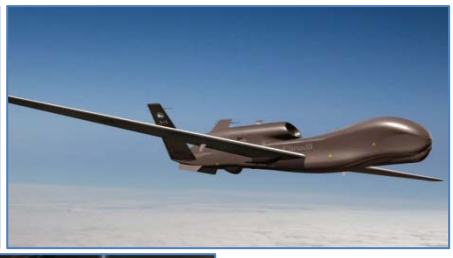
Pese a ello, aún no existen acuerdos sobre ciertas definiciones básicas y mucho menos sobre cómo debe aplicarse el derecho internacional en el ciberespacio en tiempos de guerra, una vez que el umbral de conflicto armado se haya cruzado. Lo que es delito o un ataque para unos, no lo es para otros.

Estas discrepancias, en muchos casos atribuidas a diferencias idiomáticas, hace que se produzcan discusiones respecto de la gobernanza de Internet y las tensiones entre seguridad y privacidad han ido aumentado con el tiempo y en la medida en que se producen más incidentes.

Lo concreto es que los actores en el ciberespacio (incluyendo estados, empresas, organizaciones, grupos e individuos) compiten por el control del mismo, lo cual lleva a la inevitabilidad de los conflictos en él, que afectan tanto a civiles como a militares y perturban en mayor medida a los países más desarrollados en el tema que a los que no lo son. Así, muchos han encontrado un arma barata para dañar a los más poderosos.

Desde la óptica de la seguridad, la multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las administraciones públicas, las infraestructuras críticas o las actividades de las empresas y ciudadanos.

Desde el punto de vista de la defensa, estas nuevas tecnologías han producido un cambio trascendental. Si en el pasado era suficiente con aprovecharse de las nuevas capacidades de los sistemas de información y del ciberespacio para mejorar la eficacia operacional de las fuerzas armadas, ahora es necesario poder combatir y ganar en el ciberespacio.


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 solo contemplara la organización, sino también los recursos humanos, el material, la infraestructura, la logística, la información, el adiestramiento y la doctrina.

Varios países, como por ejemplo España, elaboraron sus estrategias de ciberseguridad nacional alineadas con las respectivas estrategias de seguridad nacional por entender que la defensa nacional es parte y contribuye con sus medios, recursos y acciones a lograr la seguridad del Estado y por concebirla en los términos establecidos por la Asamblea General de la Organización de las Naciones Unidas (documento A 40/553 de 1986), que la definió como “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”.

Como principal objetivo, estas estrategias muestran la ciberseguridad y la ciberdefensa como materias prioritarias en la agenda de los respectivos gobiernos y procuran establecer un liderazgo único para coordinar las acciones y los actores involucrados en la lucha contra los riesgos derivados del ciberespacio.

Por lo general, ponen de manifiesto la gravedad y complejidad de las ciberamenazas, así como el grado de organización alcanzado por los grupos delincuentes o terroristas que están detrás de ellas. También identifican la necesidad de coordinación entre los organismos públicos dedicados a la ciberseguridad, los dedicados a la ciberdefensa, y la de estos con los actores técnicos, académicos, juristas y privados, y destacan la necesidad de la cooperación internacional, dado que la amenaza es de carácter global.

En consonancia con dichas estrategias, y ante evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la seguridad nacional, países como Brasil produjeron su correspondiente Doctrina Militar de Defesa Cibernética con la finalidad de “establecer los fundamentos de la doctrina militar de ciberdefensa, proporcionando unidad de pensamiento sobre el tema, en el ámbito del Ministerio de Defensa y contribuir a las actividades conjuntas de las fuerzas armadas en defensa de Brasil en el ciberespacio”.

Para 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.

Estos ejemplos muestran que existe una tendencia generalizada hacia el desarrollo de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la estrategia de ciberseguridad nacional y que, tanto ciberseguridad y ciberdefensa forman parte de un mismo abanico de herramientas y procedimientos del que las naciones tienen que disponer para garantizar su libertad.

Entendida así la ciberseguridad como un objetivo y la ciberdefensa como un medio para alcanzarla, esta última en las fuerzas armadas debe, entre otras: garantizar la libertad de acción de las operaciones militares en el ciberespacio y apoyar la respuesta coordinada entre los diferentes actores, tanto nacionales como internacionales, ante un ciberataque que pueda afectar a la defensa nacional.

Por lo tanto, resulta necesario, además de informar y educar sobre la materia, comenzar a elaborar una estrategia de ciberdefensa que sirva para desarrollar las previsiones de la estrategia de seguridad nacional y la correspondiente de ciberseguridad, que deberían considerar el desarrollo de un marco legal dentro de una visión compartida internacionalmente.

LA CIBERDEFENSA EN ARGENTINA

En palabras del actual Ministro de Defensa, la política de seguridad de la información, la protección de infraestructuras críticas y los estándares tecnológicos vinculados a la cuestión cibernética es competencia de la Jefatura de Gabinete de Ministros.

En ese marco, durante 2006 se constituyó el primer comité de seguridad de la información en el Ministerio de Defensa, por indicaciones de la Oficina Nacional de Tecnologías de la Información (ONTI). Allí se abrió la reflexión sobre el ciberespacio como ámbito u objetivo militar, a fin de definir y relevar los activos críticos o infraestructuras del Estado que podrían ser amenazadas y debían ser objeto de protección.

Hace dos años, la organización de la Unidad de Coordinación de Ciberdefensa en el Ministerio de Defensa permitió recoger las iniciativas y esfuerzos desarrollados por las tres fuerzas armadas y el área civil de esa cartera, donde se elaboró la propuesta orgánica que devino en la creación del Comando Conjunto de Ciberdefensa y la instrucción para desarrollar la capacidad de ciberdefensa en cada una de las fuerzas armadas y en el Estado Mayor Conjunto.

Hace apenas ocho meses el gobierno nacional normalizó la situación y, en consideración de que la defensa nacional es una obligación esencial e indelegable del Estado, que el desarrollo actual y el empleo de las tecnologías de la información generan un desafío constante para resguardar redes, sistemas informáticos y activos de la defensa y de las capacidades de su instrumento militar; le asignó responsabilidades orgánicas y funcionales en la materia a la Dirección General de Ciberdefensa del Ministerio de Defensa, para intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de esas políticas.

Entre las acciones asignadas se destacan:

1. La asistencia en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.

2. La coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.

3. La intervención en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por el nivel estratégico militar y la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la doctrina básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.

4. El control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.

5. La intervención en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.

6. El fomento de políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa, a fin de mantener un plantel adecuado.

7. La promoción de vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.

8. El impulso de acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.

9. La asistencia en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad a los lineamientos del Ciclo de Planeamiento de la Defensa Nacional.

CIBERATAQUE Y DERECHO HUMANITARIO

Suele afirmarse que el ciberataque en el conflicto entre naciones, sea bélico o prebélico, es el uso de las llamadas “armas bondadosas” y que no encuadraría en el “ius in bello” (derecho que regula las prácticas de la guerra, hoy llamado Derecho Humanitario Internacional que encuentra su fuente en los Convenios de La Haya y las Convenciones de Ginebra). Lo que se traduce en que una agresión mediante instrumentos informáticos a redes informáticas no encuentra regulación concreta por parte del derecho humanitario por ausencia de una *lex scripta* específica.

Sin embargo, esta ausencia de regulación precisa por parte de las reglas de la guerra no sería tal. La llamada cláusula de Martens (contenida en el IV Convenio de La Haya de 1907) sobre principios ampliamente aceptados del derecho humanitario estipula que, cuando una situación no esté prevista en un acuerdo internacional, “las personas civiles y los combatientes quedan bajo la protección y el imperio de los principios del derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública”. Según esta norma, todo lo que ocurra durante un conflicto armado está sujeto a la aplicación de los principios del derecho humanitario. De esta forma no existe vacío legal alguno. La “costumbre internacional” es fuente de derecho según el artículo 38 del Estatuto de la Corte Internacional de Justicia.

Claro que se suele argüir que las costumbres o derecho de gentes con que se pretende cubrir el uso de “armas informáticas” contra blancos de igual naturaleza son anteriores a esta nueva forma de combatir al enemigo. Pero el derecho internacional tiene como réplica el precedente que constituye la respuesta dada por la Corte Internacional de Justicia en un planteo análogo que llegó a su consideración por el uso de armas nucleares. En tal circunstancia sostuvo que: “...según la opinión de la amplia mayoría de los estados, así como de los tratadistas, no puede haber ninguna duda sobre la aplicabilidad del derecho humanitario a las armas nucleares...”.

También se esgrime como argumento –de bastante peso– que el ataque a redes informáticas de un país por parte de otro, cuando no hay guerra convencional o conflicto armado, torna inaplicable el derecho humanitario, porque para que se active el “ius in bello” justamente se necesita de un estado de guerra o un conflicto armado.

En este contexto cabe preguntarse: ¿qué es un conflicto armado? En los Comentarios de los Convenios de Ginebra de 1949 y de los Protocolos Adicionales de 1977, publicados por el Comité Internacional de la Cruz Roja, se adopta un punto de vista muy amplio acerca del significado de ese término. En los primeros se define un conflicto armado como "toda diferencia que surja entre dos estados y que dé lugar a la **intervención de fuerzas armadas**…, incluso si una de las partes niega la existencia de un estado de guerra y sin importar la duración o el carácter más o menos mortífero del conflicto". Del mismo modo, en el Comentario del Protocolo Adicional I, se especifica que "el derecho humanitario cubre también todo litigio entre dos estados que dé lugar a la **intervención de sus fuerzas armadas**. Ni la duración del conflicto ni su carácter más o menos mortífero desempeñan papel alguno…". En el Protocolo Adicional II, se describe un conflicto armado como "la existencia de **hostilidades abiertas entre fuerzas armadas** dotadas de cierta organización". La condición *sine qua non* en los tres casos es la intervención de fuerzas armadas.

Pero al parecer, el criterio de que una disputa o un litigio que da lugar a la intervención de las fuerzas armadas es lo que llevaría a la aplicación del derecho humanitario ha resultado un poco exagerado según la sana doctrina. Las fuerzas militares se emplean con regularidad contra adversarios, sin que se produzca necesariamente un estado de conflicto armado (valga el ejemplo de las operaciones de reconocimiento o de control aéreo). Además, en la actualidad se acepta generalmente que incidentes aislados, como enfrentamientos en la frontera o ataques en pequeña escala, no alcanzan el nivel de un conflicto armado en el sentido en que esta expresión se emplea en derecho humanitario, pero lo tornarían aplicable.

Más todavía, si el derecho humanitario rige el "conflicto armado", este cobraría vigencia cuando un grupo toma medidas que causan muertos, heridos, daños o destrucción. La expresión también abarca las acciones destinadas a causar tales resultados o que los tendrán como consecuencia previsible. Dado que la cuestión pertenece más al *jus in bello* que al *jus ad bellum*, la motivación de esas acciones no hace al caso, al igual que su licitud o ilicitud. Así por ejemplo, la parte que inicia el conflicto armado cometiendo esos actos puede estar actuando, de forma anticipada o interceptiva, en legítima defensa; de todos modos, si esas acciones tienen la intención de herir, matar, dañar o destruir, están regidas por el derecho humanitario. Cabe señalar que, según la opinión predominante actual, acciones esporádicas o aisladas no serían suficientes para constituir un conflicto armado. Además, dado que la cuestión planteada es el derecho aplicable a los conflictos armados internacionales, las acciones de que se trata deben ser atribuibles a un Estado.

Dentro de este marco jurídico internacional, y en relación a los ciberataques, los principios del derecho humanitario se aplicarían siempre que los ataques a través de redes informáticas puedan ser atribuidos a un Estado, que sean más que meros incidentes aislados y esporádicos, que tengan por objeto causar heridos, muertos, daños o destrucción y efectos análogos, o que se pueda prever que tendrían esas consecuencias. Esto es válido aunque no se empleen fuerzas armadas clásicas en el ataque.

De esta forma, un ataque contra la red informática del sistema de control del tráfico de un gran aeropuerto, perpetrado por agentes de otro Estado, implicaría la aplicación del derecho humanitario. Lo mismo ocurriría en el caso de un ataque cuyo objetivo fuera destruir oleoductos, aumentar el flujo del petróleo, tras hacerse con el control de los ordenadores que lo regulan, causar la fusión de un reactor nuclear mediante la manipulación de su centro computarizado o valerse de la red informática para activar la liberación de productos químicos tóxicos de las instalaciones de almacenamiento o producción.

En cambio, el derecho humanitario no se aplicaría al hecho de alterar la red interna de una universidad, descargar informes financieros, interrumpir temporalmente el acceso a Internet o realizar espionaje cibernético, porque, aunque formen parte de una campaña sistemática de actos similares, las consecuencias previsibles no incluirían muertos, heridos, daños o destrucción.