Control del ciberespacio desde el sector Defensa: un reto a la Seguridad Nacional

Blanco Castillo Mauricio
blancoblanco115@gmail.com
Universidad Piloto de Colombia

Resumen - La presente reflexión atiende a la necesidad de examinar las capacidades del sector defensa en Colombia, para encarar los retos que le imponen las tecnologías de la información y el acceso al ciberespacio, principalmente ahora que la seguridad nacional incorpora cada vez más a sus sistemas de gestión, dispositivos para amparar información clasificada, confidencial y de estado, obedeciendo al mandato legal de preservar la vigilancia y el estricto cumplimiento de los protocolos de protección de datos. Por tanto, se aborda la importancia que la seguridad de la información tiene para este sector estratégico del gobierno colombiano en materia de soberanía integral.

Abstract - This discussion examines the capabilities of the defense area of Colombia regarding the challenges that information technology and access to cyberspace require at this time where the national security increasingly incorporates management systems, devices to protect classified information confidential and of the State, subject to the legal mandate to preserve monitoring and strict enforcement of data protection protocols. Therefore, the information security and its impact to this strategic sector of the Colombian Government's sovereignty is studied.

Índice de Términos: Ciberguerra, escenarios estratégicos, políticas de seguridad del ciberespacio, navegación blindada, seguridad cibernética, seguridad nacional, delito informático, instrumentos de seguridad informática, infraestructuras críticas.

I. PREÁMBULO

Actualmente, las Tecnologías de la Información y las Comunicaciones son protagonistas y operan estratégicamente en los sistemas de defensa y seguridad, de manera paralela al cometido de las fuerzas constitucionalmente delegadas para preservar el orden, proteger a la sociedad y velar por la soberanía territorial.

La preocupación constante por evolucionar valiéndose de la tecnología, siempre ha estado presente en el ámbito militar. Por esto, previamente a ahondar en las capacidades del sector defensa, con el fin de encarar los desafíos del control del ciberespacio, conviene acotar, cómo el proyecto *ARPANET* (Advanced Research Projects Agency Network) [1], "desarrolló los protocolos de comunicación que permitieron que todas las computadoras de la red se mantuvieran al mismo nivel, evitando que un punto central tuviera a su cargo la administración de la información… lo que impide que una transmisión monopolice los servicios de la red" [1], esto se realizó, en el seno de la seguridad estadounidense a través de la agencia para los proyectos de investigación avanzada DARPA, con la creación del protocolo TCP/IP. También en el ámbito militar se cifró el escenario precursor de la informática moderna, cuando en la segunda guerra mundial se desencintaron los códigos alemanes gracias a la máquina de Turing[2]. [2]

Cabe subrayar que la tecnología del ciberespacio no solo es un lugar común para el sector defensa, también es un aliado estratégico; de ahí que dimensionar los modelos de un Sistema de Gestión de Seguridad de la Información – SGSI – en las Fuerzas Armadas de Colombia, resulte imprescindible en los niveles tácticos, operacionales y estratégicos. Desde esta premisa, es que puede entenderse esta reflexión porque cada vez se exige mayor precisión en el planeamiento de la inteligencia de estado, optimizando las capacidades militares para la detección temprana de amenazas a la red de comunicaciones y proveyendo validaciones seguras a los servidores, a la plataforma digital y al *software* y el *hardware* que conforman la codificación integral de blindaje ciberespacial del sector defensa.

Por su parte, un lineamiento básico es la navegación blindada para las tareas que competen a la seguridad de la nación y a la vigilancia de su soberanía, las cuáles no se omiten en las actuales exigencias de los campos estratégicos, especialmente si se trata de ciberdefensa desde lo militar. Justamente por el hecho de que lo militar conlleva a asumir la protección de la seguridad nacional, toda la información sistematizada amerita garantizar que el blindaje de la misma, cuente con los dispositivos indispensables para amparar el sigilo y la custodia de la información y de todos los datos que conforman la plataforma instrumental del ciberespacio.

II. ANTECEDENTES LEGALES

El antecedente común de las entidades públicas en materia jurídica frente a la obligación que tienen de implementar un SGSI, es la *directiva presidencial 02 del 28 de agosto del 2000* que hace emerger la *ley 790 de 2002*, *capítulo III – artículo 14* sobre la que posteriormente se deriva el *decreto 1151 de 2008* y luego el *decreto 2693 de 2012*, respecto a sus estrategias. En este, se ahonda igualmente en su *artículo 7*, no solo en los componentes del modelo de gobierno en línea –institucionalización de la estrategia, el usuario en sí mismo, implementación de un Sistema de Gestión de Tecnologías de Información y del SGSI- sino también, en los plazos de las entidades públicas para la implementación.

De igual manera, para el sector defensa rige un marco legal específico con el *Conpes 370*[1] *de 2011*, el cual designa entidades para la prevención y control del delito cibernético, que afecte la seguridad de la información de los internautas del ente privado.[3]

Los grupos de blindaje designados en estas disposiciones, se canalizan en:

- Grupo de respuestas de emergencias cibernéticas a nivel nacional.
- Comando conjunto cibernético de las Fuerzas Militares.
- Centro Cibernético Policial, con unidades investigativas en ocho ciudades y proyectado al 2016 con 25 ciudades más.

En esta regulación se cobijan cinco componentes para la estrategia de ciberdefensa: procesos, tecnología, cooperación, operaciones y fundamento legal. Adicionalmente, dentro de los estándares internacionales de blindaje internáutico para navegación de las instituciones gubernamentales, las recomendaciones para la normatividad exigen tomar en cuenta estos lineamientos:

- Proyecciones de blindaje digital.
- Fortalecimiento de las capacidades institucionales para detectar amenazas.
- Empleo efectivo de los medios.
- Fortalecimiento a la Inteligencia.
- Fortalecimiento de los mecanismos de cooperación interinstitucional.
- Implementación y aplicación de nuevas tecnologías anti espionaje y anti infiltración.

El marco legal nacional tendrá que evolucionar hacia estos resultados. En esa dirección, se debe consolidar jurídicamente para el sector defensa, el análisis informático para la recuperación de información contenida en dispositivos de almacenamiento masivo, así como promover la capacidad de generar ambientes informáticos simulados bajo disposiciones que la amparen. Es de anotar, que se trabaja en una normativa que se basará en las directrices de un nuevo Conpes que se prevé esté listo antes del cierre del año.

III.POLÍTICAS RECTORAS DE LA CIBERSEGURIDAD

La inserción de la fotogrametría digital[3] para el análisis de imágenes del espectro electromagnético, forman parte de la nueva concepción de lineamientos de la política de ciberseguridad. [4]

Los nuevos ejes se sintetizan en:

- Gobernanza.
- Fortalecimiento de capacidades en seguridad.
- Marco jurídico.
- Infraestructuras críticas (redes de telecomunicaciones, redes de energía, sistema financiero).
- Cultura de ciberseguridad.
- Cooperación internacional.
- Diplomacia cibernética y evaluación constante de la política.

Esta política tiene que contar con un esquema de interarticulación institucional como lo plasma, *figura 1*, que explica cómo el gobierno debe velar por la implementación de una estructura que admita el trabajo conjunto, para combatir el asalto digital y la perpetración ilegal del universo navegable y de la red institucional, debilitando así la ciberdelincuencia.

Figura 1. Lineamiento de ciberseguridad de las Fuerzas Armadas de Colombia.

Fuente: elaboración propia con base en Ministerio de Defensa.

Ahora bien, la misión de asistencia técnica de la Organización de Estados Americanos (OEA), insta en su última sesión, a que los estados democráticos avancen hacia una política rectora de la ciberseguridad. Para lograrlo, Colombia asume que el desarrollo del nuevo blindaje debe comulgar con tareas pendientes asignadas a un jefe nacional para la ciberseguridad, quien dependa directamente del presidente de la república.

Este indicativo sugiere la creación de una agencia nacional de seguridad cibernética. La pregunta lógica es, ¿Por qué y para qué?, precisamente porque del escenario informático y del uso de la tecnología en general, se desprenden riesgos no solo para las entidades estatales sino para la gente del común. Se hace necesario, tomar acciones frente a estas amenazas por medio de "la modernización de los sistemas de las entidades para blindarlas contra la corrupción y los hackers". [5], es un deber del Estado garantizar a través de su estructura institucional y de todos los medios y recursos que considere necesarios, la preservación de la soberanía y seguridad del país.

Paralelo a esto y en aras de lograr este cometido, se requiere activar toda una plataforma de acciones concretas y puntuales que en adelante se describen.

A. Mesas de trabajo

En las políticas del sector defensa, se deben establecer mesas de trabajo con el sector de las TIC, se hacen necesarias "acciones concretas como cambios en el Código Penal, para que sea 'moderno y tenga en cuenta diferentes formas de combatir los delitos dentro del territorio nacional pero que se provocan fuera'. Para hacer frente a crímenes que no conocen fronteras físicas" [6], así mismo el sistema implantado debe integrarse con el de otras naciones para garantizar respuesta internacional.

Cada día se mueve más información a nivel mundial y a medida que esta se digitaliza, las amenazas se hacen mayores y la red se vuelve aún más vulnerable a los llamados hackers, lo cual es un problema de gran magnitud especialmente si el ataque tiene como objetivo infraestructuras críticas y/o equipamientos militares.

Cabe anotar, que un factor importante y prioritario en la agenda de esta agencia de seguridad cibernética debe ser la identificación de estas amenazas para establecer las estrategias correctas para cada delito informático. De igual manera se debería hablar de un ente de control ya que no es desconocido el hecho de que, quien posee la información posee el poder. Se debe controlar la manera de gestionar la información ya que quien la posee, tiene la facultad de ayudar o de perjudicar a otros y más si se trata de instituciones que por su naturaleza blindada pueden encubrir casos de corrupción o beneficiarse de su estatus.

B. Convenio Budapest

El convenio contra el cibercrimen pretende que los gobiernos adscritos a la OEA, suscriban el compromiso de adoptar en su normativa un marco

legal para la guerra de la invasión a la información de la red.

Se empieza a visualizar el camino por el cual el Estado mantiene su *statu quo* dentro del campo informático, aludiendo al principio fundamental de supervivencia y mantenimiento de los intereses nacionales. Es decir, acá se perfecciona el ejercicio de concepción, manejo, maniobra y proyección en la red y en el universo digital de lo que se entiende como información reservada e información clasificada, por lo que el organismo internacional entiende que es imperativo blindar a los estados de todo tipo de amenazas cibernéticas.

De ahí, que el reto a la seguridad nacional, se adscriba a la cooperación intergubernamental, la cual determina que los estados trabajen conjuntamente en pro de unos objetivos previamente establecidos, y hagan de la organización de cooperación un organismo al servicio de los propios estados, mediante sus respectivas entidades encargadas de preservar el orden y procurar seguridad en el universo informático que sus servidores y plataformas administren.

Por su parte, las organizaciones de cooperación para la seguridad cibernética, se enmarcan dentro de la causa de las relaciones internacionales, ya que existen únicamente por la simple voluntad de los estados, con el fin de coordinar políticas nacionales en aras de la discreción del uso de los datos.

A este respecto, el sector defensa específicamente estaría enhebrando sobre las bases jurídicas internacionales, un frente específico de acción donde se enarbolen concretamente las acciones, que para las capacidades militares validen las respuestas puntuales de cada sector a sus amenazas particulares.

C. Monitoreo entorno digital

¿Cuál es la importancia de este elemento? La gran cantidad de información que se mueve a nivel global hace que cada país implemente diferentes acciones para monitorear y analizar la información que absorba cada agencia de seguridad, en este caso la agencia nacional de seguridad cibernética de Colombia. No obstante, se debe explorar si cada país está dispuesto a revisar las políticas de monitoreo que rigen sus prácticas ya que el derecho a la privacidad en el entorno digital como en cualquier gestión, tiene sus alcances y limitaciones; se debe revisar la legislación con detenimiento y alinear cada acción a tomar, con los estándares de derechos humanos (establecer mecanismos de respeto en el entorno digital).

Por otra parte, en este monitoreo entran en juego los ejercicios tácticos, para enfrentar amenazas cibernéticas y neutralizar las incursiones de piratas informáticos a la infraestructuras del Ministerio de Defensa. Es un esfuerzo más con miras al fortalecimiento de las Fuerzas Armadas y de Policía, para asumir la optimización de las nuevas capacidades sobre ciberseguridad y ciberdefensa.

Los delitos cibernéticos requieren que las fuerzas de la defensa preparen ingenieros electrónicos e informáticos, que atiendan el monitoreo del entorno digital con base en estas capacidades, para que los entrenamientos respondan en forma proactiva y veraz a estos asaltos del ciberespacio.

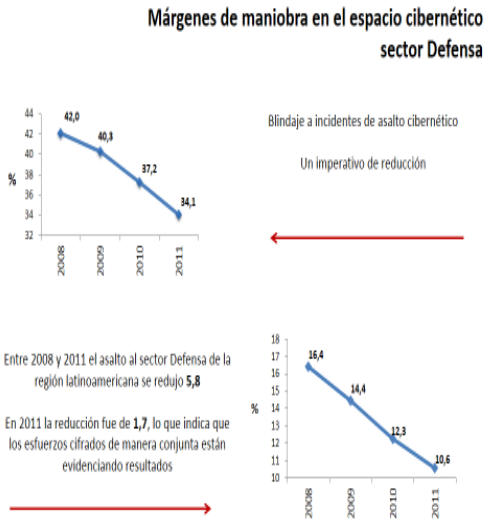

Figura 3. Mecanismos extrapolados sector defensa.

Fuente: Elaboración propia con base en cálculos de la OEA (2015).

Este monitoreo debe abstenerse de publicidad alguna, para evitar ofrecer a los ciberdelincuentes pistas de acción y rutas susceptibles de exploración. [7] De acuerdo con las *figuras 3* y *4* los mecanismos

tienen que extrapolar los escenarios previstos y mapear espacios inesperados, porque anticiparse al enemigo, es una agresiva y efectiva estrategia de seguridad cibernética. La *figura 4* nos muestra la posición del país en el escenario global, tanto en el sector público como en el sector privado.

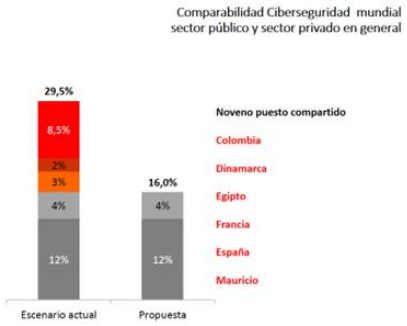

Figura 4. Colombia y el escalonamiento de la ciberseguridad mundial.

Fuente: Elaboración propia con base en cálculos de la Unión Internacional de Telecomunicaciones, ONU (2015).

Hoy Colombia ocupa el noveno lugar en el índice mundial de ciberseguridad de la unión internacional de telecomunicaciones, el brazo de las Naciones Unidas para las TIC y las telecomunicaciones, el cual mide el "compromiso" de los países, sus capacidades técnicas y su disposición de cooperación internacional entre otros aspectos. Comparte ese puesto con Dinamarca, Egipto, Francia, España y la Isla Mauricio en la lista que encabezan Estados Unidos, Canadá y Australia. [8]

La sofisticación de los delitos, es una preocupación a nivel mundial, por tanto, una parte del presupuesto gubernamental de cada nación debe ser destinado para blindar las estrategias de sus entidades contra el cibercriminal.

IV. BLINDAJE ESTRATÉGICO

Toda estrategia de ciberdefensa en el sector defensa, debe procurar la prevención de ataques en un escenario de antelación. Esta estrategia de blindaje, debe contar con sub-proyectos de capacitación y de investigación, en aras de que el sector defensa desarrolle mecanismos de ciberdefensa, con la ayuda de herramientas de seguridad que fortalezcan el universo extrapolar del segmento digital.

Se deben contrarrestar las vulnerabilidades de los sistemas de información y tecnología de las comunicaciones, ya que este tratamiento aportará al fortalecimiento de la ciberdefensa y permitirá frenar el avance de intromisión y asalto digital.

A. Parámetros esenciales

Los ataques contra el sistema militar conectado, están ligados a delitos de fraude al marco identitario de las Fuerzas Militares y de la Policía, como cuerpo constitucionalmente designado para la defensa.

Para neutralizarlos, es de suma importancia contar con la idoneidad de los miembros de las fuerzas de defensa, principalmente en detección, anticipación, acción, coordinación y ejercicio estratégico.[9]

En el mejoramiento de las herramientas, entran en juego factores que ayudan a medir el campo de desempeño con antelación, donde se activan diversos entes (centros de gravedad) del entorno complejo, tal como describe el *esquema 1*. Todo esto, con el propósito de que en el proceso de mejora continua, el desarrollo de herramientas sobre escenarios específicos y rutas de navegación blindada, cobijen las áreas críticas de enfoque para la defensa nacional; estas herramientas sujetas a proyectos estratégicos, se diseñan en aras de minimizar las amenazas y ponderar las posibilidades de control.

Esquema 1. Articulación de centros de gravedad para la defensa cibernética.

Fuente: Elaboración propia con base en documentación.

B. Desarrollos angulares

La protección virtual de estructuras estratégicas, comprende el desarrollo de herramientas que garanticen la seguridad del cuerpo de información del estado colombiano. Ante un conflicto como el que vive Colombia, los delitos cibernéticos hacia el sector defensa dejan en alto grado de vulnerabilidad la estabilidad nacional, de manera que se requiere de acciones especializadas, para no solo controlar los más corrientes, sino, lograr encarar el terrorismo cibernético. [10]

El trabajo debe concentrarse desde el sector defensa, para habilitar de manera efectiva la plataforma de blindaje, prevención, control, monitoreo y anticipación, con el fin de enfrentar y contrarrestar los ataques destructivos y sistemáticos de las fuerzas oscuras, que buscan violar información reservada y clasificada, para uso ilegal o ventajoso respecto a secretos de estado.

Los procesos que conforman el conjunto de ejercicios y entrenamientos anti infiltración y anti vulneración, no deben ser ajenos a la estrategia de política de ciberdefensa, dichos procesos deben contemplar todos sus lineamientos. De igual forma se debe velar por una completa comprensión de las responsabilidades involucradas en el manejo de la información sensible, con el fin de aumentar el grado de seguridad de la información manejada. No se debe hablar exclusivamente de la información amparada desde la legislación, se debe considerar un plan de contingencia elaborado y sancionado por un comité que sea el encargado de generar las pautas del tema y guie la canalización de situaciones no contempladas en dicha reglamentación.

C. Instrumentos soporte

Lo ideal es que una dependencia, integre todos los proyectos estratégicos de blindaje ante la ofensiva dirigida al sector defensa. Esta dependencia debe encargarse de contrarrestar las acciones que vulneren la seguridad y la soberanía del sector y amparar las directrices de la inteligencia y contrainteligencia, propias de los ejes de seguridad del Estado.

Es preferible que sobre la investigación se construyan los instrumentos, para que los intercambios de información sobre operaciones militares de ciberdefensa den resultado. En este cometido, el Estado Mayor Conjunto cumple un papel substancial, en tanto su coordinación con las máximas autoridades del sector defensa, se erija como imperativo para el blindaje.

El insumo que alimenta la cadena del ciberdelito, es la incapacidad del blanco, en este caso el sector defensa, de reaccionar y anticiparse ante los factores que imposibilitan y vulneran a la institución. Por tal razón, es imprescindible la capacitación y el entrenamiento especializado, para neutralizar las acciones violatorias a la plataforma de información del ente público encargado de la seguridad nacional.

También debe subrayarse que, “hay más evidencias de que los estados avanzados invierten recursos en desarrollar y comprar virus informáticos, programas espías ('spyware'), vulnerabilidades en sistemas y 'software' intrusivo, como una estrategia para reforzar la 'ciberseguridad', la capacidad de respuesta a un 'ciberataque' y lo que parece más importante, la capacidad de 'ciber atacar' primero**.** Lógicamente, la opacidad con la que operan los servicios de defensa y de inteligencia (SIC), dificulta un diagnóstico real: sólo hay pistas que descubren empresas y expertos en seguridad”. [11]

Para salvaguardar la soberanía y el ciberespacio del sector defensa, se hace necesaria la implementación de tecnologías que ayuden a la monitorización continua de los sistemas, a la protección de datos, a la detección de intrusos y a la recuperación del sistema después de un ataque, es decir, un sistema integrado de vigilancia electromagnética que reafirme el blindaje efectivo del Estado y sus instituciones.

Desde ese centro de mando y control de actividad magnética y del ciberespacio, los altos mandos de las Fuerzas Armadas y de la Policía Nacional, a través del Estado Mayor de la Defensa Nacional, pueden centralizar el monitoreo de la red, porque para su análisis y coordinación de las operaciones militares o de interdicción, se requiere de un sigilo que debe resguardarse para no desestabilizar y poner en riesgo la seguridad nacional.

Esa solidez se cifra entonces en:

- Incrementar las capacidades del sector defensa, para fortalecer la vigilancia, el control y la seguridad de su ciberespacio.

- Reforzar el combate al delito informático con el empleo de los recursos tecnológicos y las capacidades humanas, para reafirmar la cooperación conjunta contra la vulnerabilidad del ciberespacio.
- Consolidar el compromiso para combatir el flagelo de la violación del espacio electromagnético y del delito informático.
- Disponer de la capacidad para detectar y dar seguimiento a irrupciones ilícitas en el territorio informático del sector defensa.

V. CONCLUSIONES

El grado de seguridad de las aplicaciones de información del sector defensa, avanza hacia la identificación eficiente y oportuna de vulnerabilidades, con miras al mejoramiento de las tareas que debiliten y reduzcan las amenazas.

El imperativo es, fortalecer las capacidades del sector para garantizar la soberanía y seguridad de la plataforma informática, salvaguardar la documentación de alta reserva, los escenarios de contenido confidencial y el espacio cibernético de su competencia, en aras de un espectro seguro, donde enfrentar con eficiencia las amenazas, ya sea producto de inteligencia y/o de la acción anticipada, gracias a la intervención oportuna de los recursos humanos y tecnológicos de ineludible articulación.

De manera adicional, al incrementar las capacidades militares frente a la ciberguerra y el terrorismo cibernético, se contribuye a que desde el sector defensa, se canalicen las potencialidades del país inmersas en toda política de estado que preserve y garantice los intereses nacionales.

Finalmente, el utilizar la capacidad operativa y administrativa para cumplir eficientemente con las misiones anti infiltración, la observancia de los instrumentos jurídicos internacionales y la cooperación de los sectores de defensa de otros gobiernos, es un ejercicio de gran importancia, al momento de enfrentar las vulnerabilidades cibernéticas y las violaciones a la información de estado.

REFERENCIAS

[1] Buitrón, Nachyelli (2003) Entre la Virtualidad y la Ética. Número 35. Recuperado el 9 de septiembre de 2015. Disponible en http://www.razonypalabra.org.mx/anteriores/n35/nbuitron.html

[2] Andrades, Fran. "Cinco escenarios de ciberguerra en el nuevo orden mundial". Diario Turing, (7 de mayo de 2013 [citado 4 de mayo de 2014]: disponible en. http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html

[3] Departamento Nacional de Planeación (2011). Documento Conpes 3701, Lineamientos de política para ciberseguridad y ciberdefensa Bogotá.

[4] Caracol radio. (2014) Colombia contaría con una Agencia Nacional de Seguridad Cibernética. Recuperado el 10 de septiembre de 2015 de http://caracol.com.co/radio/2014/07/09/nacional/1404929760_313921.html

[5] Medina, Alejandra (2015). El Espectador. La hoja de ruta para la ciberseguridad. Entrevista a Samuel Yohai, presidente ejecutivo de la CCIT[4]. Recuperado el 10 de septiembre de 2015 de http://www.elespectador.com/noticias/economia/hoja-de-ruta-ciberseguridad-articulo-576914

[6] Segura y F. Gordo (coords). (2013).Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio. Granada: Universidad de Granada.

[7] Gestión de riesgo en la era digital. Recuperado el 28 de julio de 2015 en el sitio Web: blicación comprar Gestión http://www.riskgroup.com.ar/cobertura/gestion-de-iesgo-en-la-era-digital.

[8]CCN-CERT IA-03/10 Ciberamenazas (2009) y Tendencias 2010, Informe de amenazas del CCN-CERT, 15 de marzo de 2010, [disponible en www.ccn-cert-cni.es (parte privada del portal)].

[9]Pérez Martínez, V. M. (2009). El ciberespacio: la nueva ágora. Tenerife: Ediciones IDEA.

Universidad Piloto de Colombia. Blanco. Control del ciberespacio desde el sector defensa.

[10] Acissi, M., Baudru, N. et. al. Seguridad informática, conocer el ataque para una mejor defensa. Barcelona: Ediciones Eni.

[11] La Inteligencia, factor clave frente al terrorismo internacional (2009). Cuadernos de Estrategia nº 141, Ministerio de Defensa.

---

[1] Traduce Red de la Agencia de Proyectos de Investigación Avanzados. Es una red precursora de la actual Internet. Fue desarrollada en la década de 1960 por el departamento de defensa de Estados Unidos, fundada por DARPA, una agencia de investigación del gobierno norteamericano. ARPANET sirvió como banco de pruebas para las nuevas tecnologías de red, inicialmente uniendo varias universidades y centros de investigación. Tomado de http://www.cavsi.com/preguntasrespuestas/arpanet-red-de-la-agencia-de-proyectos-de-investigacion-avanzados/.

[2] Es un dispositivo que manipula símbolos sobre una tira de cinta de acuerdo a una tabla de reglas. Puede ser adaptada para simular la lógica de cualquier algoritmo de computador y es particularmente útil en la explicación de las funciones de un CPU dentro de un computador. Tomado de http://es.slideshare.net/lourdesnbv/definicion-y-funcionamiento-de-maquina-de-turing.

[3] Es una tecnología basada en la medición sobre imágenes digitales, para conseguir geometrías, radiometría e información semántica de áreas u objetos en 2D y/o 3D. Tomado de http://www.topoequipos.com/topoequipos2.0/fotogrametraa-digital/fotogrametria-digital.

[4] Cámara Colombiana de Informática y Telecomunicaciones.