CIBERDEFENSA Y CIBERSGURIDA: UNA NUEVA PRIORIDAD PARA LAS NACIONES

Autor

Sandra Camila Valencia Rojas

Tutor

Juan Pablo Gómez Azuero

Universidad Militar Nueva Granada
Faculta de Relaciones Internacionales, Estrategia y seguridad
Programa Relaciones Internacionales y Estudios Políticos
2014

CIBERDEFENSA Y CIBERSGURIDA: UNA NUEVA PRIORIDAD PARA LAS NACIONES

Sandra Camila Valencia Rojas
Relaciones Internacionales y Estudios Políticos
Estudiante Universidad Militar Nueva Granada

Resumen

Grandes hombres como Hertz con sus experimentos confirmativos, Maxwell con sus bases matemáticas, y Marconi con la invención de la Telegrafía sin hilos, dieron al mundo la posibilidad de la comunicación a través de la distancia y sus obstáculos, el trabajo de estos hombres logró demostrar el aprovechamiento de las propiedades de la programación de la energía electromagnética.

Para los Estados la energía electromagnética principalmente se utilizó en el campo de la comunicación en el ámbito militar, lo cual hacia más fácil el cumplimiento de las operaciones militares, sin embargo, tras la utilización continua de transmisores, se pudo demostrar que con la manipulación de la llave telegráfica, no solo se podían trasmitir mensajes, sino que también se podía producir un ruido, que generaba una perturbación en las frecuencias, dificultando así la organización y la acción de combate del enemigo. Esto fue el inicio de lo que hoy se conoce como la guerra electrónica.

A partir del uso de la energía electromagnética en el ámbito militar, la guerra electrónica conocida por sus siglas en inglés como (EW) Electronic Warfare, se entiende como cualquier acción militar que se ejerce sobre el espectro electromagnético, el cual hace uso en su mayoría de ataques electrónicos dirigidos a la extracción de información así como el bloqueo de la misma entre otras. (Guerra electrónica. Cátedra in-nova. Universidad Politécnica de Madrid. 2014). Se comenzó a utilizar en el campo de la estrategia y la táctica militar, es así como se entendieron todas las ventajas operativas que ésta traía implícita, logrando crear situaciones falsas y trasmisiones ficticias que desorientaban al enemigo y encubrían sus verdaderas intenciones.

Desde la segunda guerra mundial, la guerra electrónica se ha desarrollado exponencialmente, hasta la actualidad durante la cual se ha convertido en un elemento imprescindible, en los escenarios de conflicto presentes en el mundo. (Guerra electrónica. Cátedra in-nova. Universidad Politécnica de Madrid 2014). Mediante el uso de los medios electrónicos presentes durante la segunda guerra mundial, se presume que se dio inicio a la conocida actualmente guerra electrónica, pero enfocada más hacia el uso de equipos electrónicos, los cuales poseían válvulas electrónicas delicadas y complejas, así como también diversos cables y placas de circuito, los cuales eran imprescindibles ya que del debido uso y funcionamiento dependía en su mayoría el fracaso o éxito, lo cual se traducía en vivir o morir. (Guerra electrónica. Sf. U- historia. S.f)

Ya en 1919, con el invento del radiogoniómetro, la intersección e interferencia de las ondas electromagnéticas lograron evolucionar, ya que por medio del radiogoniómetro se podía determinar la dirección de procedencia de las señales interceptadas del enemigo, dando la posibilidad de ubicar los centros de comunicación, y conjunto a éstos los cuarteles generales del mismo.

El siguiente paso en la guerra electrónica, fue la aparición del radar en 1935, por medio de éste se logró medir el paso de energía trasmitida, la cual se refleja en un blanco. Estas ondas no se emplean para trasmitir información con contenido de comunicación, si no que se centran en el desarrollo de funciones de detección y vigilancia.

Por todo lo anteriormente descrito se puede afirmar, que el creciente desarrollo tecnológico iniciado en el siglo XX, dio inicio a la guerra electrónica, que aún hoy no vislumbra su fin.

Palabras claves:

Ciberguerra, ciberseguridad, ciberdefensa, ciberespacio, ciberataques, seguridad, Estado.

Abstract

Great men like Hertz with confirmatory experiments, Maxwell with mathematical foundations, and Marconi with the invention of Wireless Telegraphy, gave the world the possibility of communication over distance and obstacles, the work of these men failed to show exploiting the properties of the electromagnetic energy programming.

For States electromagnetic energy is mainly used in the field of communication in the military, which made it easier to comply with military operations, however, after the continuous use of transmitters, it could be demonstrated that manipulating the telegraph key, not only could transmit messages, but could also produce a sound that generated a disturbance frequencies, thus hindering the organization and combat action of the enemy. This was the beginning of what is now known as electronic warfare.

Through the use of electromagnetic energy in the military, electronic warfare known by its acronym in English (EW) Electronic Warfare, is understood as any military action exerted on the electromagnetic spectrum, which uses mostly electronic attacks on information extraction and blocking it from others. (Electronic Warfare. Professorship in-nova. Polytechnic University of Madrid. 2014). It began to be used in the field of military strategy and tactics, so as all operational advantages it brought implied, even creating false and fictitious situations that disorient the enemy transmissions and concealed his true intentions are understood.

Since World War II, electronic warfare has evolved exponentially, to the present during which it has become an essential element in conflict scenarios present in the world. (Electronic Warfare. Professorship in-nova. Polytechnic University of Madrid 2014). By using electronic media present during the second world war, presumably initiated the currently known electronic warfare occurred, but focused more towards the use of electronic equipment, which had delicate and complex electronic valves, as well as various wires and circuit boards, which were

essential as the proper use and operation depended mostly failure or success, which resulted in live or die. (Electronic Warfare. Sf. U-history. Sf)

Already in 1919, with the invention of the finder, the intersection and interference of electromagnetic waves managed to evolve, and that through the finder could determine the direction of origin of intercepted enemy signals, giving the possibility of locating communication centers and set them the same headquarters.

The next step in electronic warfare, radar was the appearance in 1935, through this we were able to measure the passage of transmitted energy, which is reflected on a white. These waves are not used to transmit information content of communication, but will focus on the development of detection and surveillance functions.

For the above described we can say that the increasing technological development begun in the twentieth century ushered in the electronic war which still sees no end.

Keywords:

Cyberwar, Cybersecurity, cyber defense, cyber, cyber, security, rule.

La Guerra

Tradicionalmente las guerras se han desarrollado en tierra, aire y mar, sin embargo, al trascurrir de los años y de los grandes avances tecnológicos ha surgido una nueva forma de combatir ligada al fenómeno de la internet, mejor conocido como el ciberespacio, el cual encierra un sin fin de interrogantes, muchos de éstos sin resolver aún.

> El ciberespacio está formado por todas las redes de computación y todo lo que conecta y controla, incluyendo el internet, más otras redes que no son abiertas; es el espacio en que la información digitalizada se comunica

> por medio de computadoras. Ahora si tuviéramos que dar una definición militar, diría que es el dominio caracterizado por el uso de medio electrónicos y espectro electromagnético para guardar, modificar e intercambiar información vía sistemas en red. (Morelli. A, SF)

Ésta circulación de información por cables, satélites y ordenadores, ha dado origen a un ambiente peligroso con nuevas y complejas amenazas, en donde los individuos pueden realizar diferentes actividades, las cuales en ocasiones se pueden realizar de forma menos compleja, lo cual posibilita, ocasionalmente el acceso a la información contenida en el espacio virtual, logrando una nueva versión bélica que pone en riesgo los campos de poder nacional, representado en este caso por las entidades legítimas del Estado, gubernamentales, privadas, públicas, así como también ONG, alertando además a los Estados a actuar eficaz y efectivamente frente al tema de ciberseguridad y ciberdefensa.

Por tal motivo la Ciberguerra es entendida como:

> La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde “la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento” (G.Sanchez.2012)

En otras palabras son acciones realizadas por un Estado para penetrar las redes de otra nación, con el fin de generar daño o interrupción en las mismas, dejando ver que los ciber-ataques, se han convertido en una amenaza para cualquier nación, no solo porque son ataques conectados entre sí, sino que son diversos y aún más importante, son demasiado variables, manejando un nivel de destrucción invisible, latente y progresivo.

Son ataques que pueden generarse desde cualquier lugar del planeta o incluso desde diferentes lugares simultáneamente, de manera que cualquiera puede dejar por ejemplo, sin electricidad o sin comunicación a una ciudad, así como también penetrar los sistemas informáticos de un país para controlar la internet, los móviles y los sistemas de seguridad dejando como resultado, un enorme caos en el país, así como también pánico entre la población, sin riesgo de ser detectado ni detenido, pues éste riesgo es prácticamente invisible gracias al modo de acción de los ataques.

En el mundo se realizan alrededor de 362.600.000 ciberataques en el año (BBC mundo. 15 de Marzo 2013), en el caso Colombiano según la revista dinero, las computadoras de un 35% de usuarios en la región fueron atacadas por lo menos una vez mientras navega por la web. (Dinero, 2012)

Conjunto a esto durante los últimos 10 años se han escuchado continuos comentarios por parte de gobiernos que hacen referencia a la violación de sus derechos soberanos por ataques informáticos y en algunos casos entre estos gobiernos se acusan de ciberespionaje tal es el caso de la vigilancia silenciosa de los Estados Unidos, mediante el programa llamado PRISM, el cual se encarga de la vigilancia electrónica y que se encuentra a cargo de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos aproximadamente desde el año 2007, es así como PRISM se formó debido a los atentados terroristas ocurridos el 11 de septiembre, hacia el final del gobierno del ex presidente Bush, de tal manera que gracias a PRISM, el gobierno de los Estados Unidos podría tener acceso a los correos electrónicos extranjeros. (Coordinación de Seguridad de la Información, 2013)

De esta manera permitía la vigilancia por parte de funcionarios norteamericanos hacia cualquier ciudadano tanto dentro como fuera de los Estados Unidos, en el renombrado caso Snowden, en donde éste último permitiera que diarios mundiales, conocieran los movimientos y las filtraciones que al interior de entidades gubernamentales se realizaban, tanto a ciudadanos estadounidenses

como a ciudadanos externos, protegidos legalmente bajo legislaciones diferentes como lógicamente sucede en el ámbito internacional. (Bejerano, P. 2013)

Normalmente, hay actos de ataque que de forma directa o indirecta, pueden afectar a una persona de forma particular, pero hay mucho más detrás de estos ataques. Hay un fenómeno de escala mundial que ya no afecta una persona en particular si no a un Estado o varios en específico, por lo que éstos se han visto en la obligación de tomar medidas frente a la ciberdefensa y ciberseguridad, dadas las implicaciones que éste tipo de ataques implican tanto a la seguridad nacional, como a la internacional, pues es importante destacar, que se encuentran al alcance de cualquier individuo, a lo cual se suma que pueden ser utilizados por los terroristas, que ya sea de índole social, cultural, religioso o económico, ponen en riesgo la seguridad tanto de la ciudadanía como del Estado en pleno.

Con base en lo anterior, es importante establecer que la definición del término es compleja, a esto se suma que actualmente el terrorismo también actúa, igualmente en otro espacio complejo como lo es el del ciberespacio. Es así como se puede determinar, como un fenómeno social que presenta diversos y variables aspectos, en la Convención de 1937, se define que son actos de terrorismo, los actos criminales que tengan como fin establecer e infundir terror, a todo tipo de individuo, que haga parte, de una comunidad, un grupo y al público en general. (Gasser. H. 2002.)[1]

La ciberdefensa hace relación a:

> Una nueva connotación sistémica y sistemática que deben desarrollar los gobiernos para comprender ahora sus responsabilidades de Estado, en el contexto ciudadano y de fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la compresión de variables, entre otras, las vulnerabilidades en la infraestructura critica de una nación, las garantías y los derechos de los ciudadanos en el mundo en línea, la renovación de la administración de justicia en el entorno digital y la evolución de la inseguridad de la información en el contexto tecnológico y operacional (Cano. J, 2013.)

[1] El termino Terrorismo también hace referencia a: los actos que además de terror causan también daños físicos y materiales, tanto a individuos como a bienes materiales, públicos y privados causando perjuicios daños económicos, ambientales, estructurales entre otros. (Gasser. H, 2002)

Y la ciberseguridad se entiende como:

> La realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital en un conjunto de variables claves, acertadamente definidas por la International Telecommunication Union (ITU), en las cuales se hace necesario el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación en el contexto de una realidad digital y de información instantánea (Cano .J, 2013).

Por ende para lograr entender la importancia de la ciberguerra, es necesario tener en cuenta que ésta no es una guerra que tiene un desarrollo tradicional y que a través de la observación de los estudios de casos de ciber ataques realizados en el mundo en la última década, se pueden tomar medidas y acciones para contrarrestar estos tipo de ataques, los cuales han demostrado un alcance sin precedentes gracias a la acción silenciosa de los mismos, pero letal a la hora de arrojar resultados.

En el caso Colombiano, donde la organización encargada de velar por la ciberseguridad y ciberdefensa de la nación, está hasta ahora comenzado, es necesario cuestionarse ¿Qué están haciendo en Colombia para combatir éstos ciberataques y qué se debería hacer para reforzar seguridad nacional frente a la ciberguerra o posibles ataques cibernéticos que colapsen las instituciones del Estado?

Éste y otros cuestionamientos, causan especial atención, si se tiene en cuenta que en el país, las normas y restricciones hasta hace escasos días, eran no solo escasas, sino también débiles en cuanto a la acción de respuesta para contrarrestar, las acciones que pusiesen en peligro la seguridad nacional, más aún cuando éstos ataques se revelan por parte de ciudadanos del común, que no cuentan constitucionalmente con el permiso ni con el deber de realizar éste tipo de acciones, que supuestamente justificadas o no, vulneren los derechos y deberes de los ciudadanos Colombianos.

A nivel mundial, muchas naciones se encuentran trabajando desde sus Fuerzas Armadas en la implementación de métodos, que permitan combatir, los ciberataques que reciben diariamente y que comienzan a ser parte de su

escenario de guerra, o como una precaución para el aseguramiento de la paz, empezando a lanzar políticas en materia de ciberseguridad y ciberdefensa, las cuales incorporan nuevas capacidades tecnológicas, las cuales permiten activar nuevos organismos encargados de esta área, tales como:

Brasil: tras los hechos presentados con el mencionado caso PRISM, anteriormente mencionado, los gobiernos de Brasil y Argentina han adoptado una serie de decisiones en pro de la protección de la información entre las dos naciones, es así como firmaron un acuerdo en ciberdefensa, el cual se basa en la creación de un sistema que permita proteger tanto las actividades que realizan los dos países así como la información manejada, ésta por medios técnicos los cuales se estima que se implementaron en un término de dos meses. (Bejerano, P. 2013)

Todo esto en respuesta a los hechos de filtraciones realizados por los Estados Unidos en Latinoamérica, especialmente sobre Brasil. Mediante el acuerdo presentado, se establecen el entrenamiento por parte de técnicos brasileros a unidades argentinas, así como también el desarrollo de sistemas de contrainteligencia en cuanto a la información y el manejo digital. (Bejerano, P. 2013)

Colombia: con base en a las necesidades de fortalecimiento en cuanto a ciberseguridad y ciberdefensa, los Ministerios de Justicia, Defensa y las TIC de Colombia, se reunieron con expertos nacionales para realizar una evaluación de la situación nacional, pues en éstos campos no son muchas las medidas implementadas y desarrolladas actualmente, es por ello que gracias a un documento que se elaborara con base a las recomendaciones que de éstas reuniones se difieran, se elaborará un documento el cual será evaluado por expertos de 10 países líderes en el tema a nivel mundial, los cuales conformaran, la denominada: "Misión de Asistencia Técnica en Seguridad Cibernética en Colombia" convocada por la OEA. (Ministerio de Tecnologías de la Información y las Comunicaciones. 2014)

“Representantes de los gobiernos de Canadá, España, Estados Unidos, Estonia, Corea del Sur, Israel, Reino Unido, República Dominicana y Uruguay, han sido invitados a formar parte de esta comisión internacional. De igual forma, se espera la participación de

organismos internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Consejo de Europa, el Centro Global de Seguridad Cibernética de la Universidad de Oxford, el Foro Económico Mundial y las Naciones Unidas". (Ministerio de Tecnologías de la Información y las Comunicaciones. 2014)

Así mismo es importante destacar, que la situación que se presenta en el país, ya vislumbra los modos de operar que a nivel mundial, la sociedad ya conoce, tal es así, que ciudadanos del común, según los resultados de los análisis realizados por parte de las autoridades competentes, extraen información que se puede considerar como importante, para ser posiblemente negociada, dentro de un peligroso juego invisible, pues si bien se pueden conocer detalles relacionados con la vida personal de algún ciudadano, de la misma manera se puede llegar a conocer detalles e información, que ponen en peligro tanto la seguridad nacional, como la internacional, los cuales sólo pueden ser administrados por las autoridades competentes.

Con base en lo anterior es necesario aclarar, que el concepto de seguridad nacional hace referencia a la capacidad y a los medios que tiene un gobierno defensivamente, es decir en la parte militar, en cuanto a la defensa tanto del Estado como a la de la legitimidad del mismo, frente a amenazas tanto internas como externas, que puedan amenazar, la seguridad nacional.

Por otra parte, es necesario aclarar que éstas medidas han sido implementadas a través de las experiencias vividas en los últimos años, entre las que se encuentran:

Estonia 2007: Las instituciones se vieron paralizadas por una avalancha de ciberataques realizados por hackers rusos, su objetivo, numerosas instituciones públicas, bancos, partidos políticos y medios de comunicación, esto luego de un incidente diplomático generado por el gobierno estonio, al reubicar la estatua del Soldado de Bronce de Tallin, un símbolo Ruso importante (BBC, 2007). Por tal motivo se decidió crear Centro Internacional de Análisis de Ciberamenazas. En este centro trabajan personal técnico y administrativo. (Ministerio de defensa, 2010).

Australia: En múltiples ocasiones, lograron establecer ciberataques lanzados desde el extranjero contra algunas de las mayores empresas de materias primas y otros negocios. Hackers (El termino hacker designa a una persona con cualidades, como la inteligencia, conocimiento y talento, generalmente relacionado con el manejo de computadoras, y redes informáticas, electrónicas, de seguridad, etc. (Seguridadpc.net. Sf) han ingresado y bloqueado páginas web del Gobierno. En una oportunidad lograron infiltrarse al sitio del Primer Ministro el cual fue desconectado completamente por dos días (CNN expansión, 2013). Así que crearon el Centro de Operaciones Cibernéticas que coordina las acciones estatales.

Por otra parte el termino hacker ético, designa la labor de buscar las distintas vulnerabilidades existentes en los sistemas de las organizaciones para mitigarlas a fin de evitar las fugas de la información sensible. (Seguridad. Prevención para ti. Hacking ético mitos y realidades. 2012).

Alemania: diariamente reciben de 3 a 6 ataques a estructuras gubernamentales y federales por hackers, los cuales en su mayoría provienen del territorio chino, y que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas, además de esto, constantemente recibe ataques por parte de hackers rusos a su red eléctrica y ferroviaria (Von Hein M Y Papaleo. C, 2010). Por lo que se estableció su primera unidad exclusivamente dedicada a la guerra cibernética conformada por oficiales y suboficiales de todas las fuerzas. (Ministerio de defensa.2009)

Estados Unidos: recibe miles de ciber ataques, que han afectado y robado información secreta de vital importancia como lo fue el caso de Joint Stike Fighter F-35, (NTD Spanish. 15 de marzo 2013). Además de esto han logrado ingresar a páginas de instituciones de gran valor para la nación como el Departamento del Tesoro y de Estado, el Pentágono y de la Casa Blanca. Solución, creó un Centro de Ciber Comando Unificado. (Ministerio de defensa.2009)

Por otra parte, los países de América del sur cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), entre los que se encuentran:

Argentina (Ar CERT): Se crea la oficina nacional de tecnologías de información para evaluar y poner en marcha un sistema de modernización y uso eficiente de los recursos digitales. En el año 2005 a través de esta oficina se da el nacimiento del Equipo de Respuesta ante Emergencias Informáticas.

Ya para el 2012 Argentina crea el Programa Nacional de Infraestructura Criticas de Información y Ciberseguridad, el cual se encarga específicamente de la protección de la infraestructura critica del país. De igual manera está estructurado el borrador del Plan Nacional de ciberseguridad y protección de infraestructura critica 2013-2015. (Jefatura de gabinete de ministros presidencia de la nación, sf).

México: cuenta con la Unidad de Secretaria Pública, que está encargada del manejo de las respuestas a las amenazas cibernéticas, la investigación de delitos electrónicos, el análisis de pruebas electrónicas y la protección de estructuras críticas, de la mano creó el Equipo Nacional Especializado de Respuesta a Incidentes Cibernéticos, para así aumentar la capacidad de respuesta gubernamental .(OEA. Sf).

Panamá: en marzo de 2013 adopto una Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Ésta estrategia se basa en; asegurar la privacidad y la confianza en el uso de las tecnologías de la información y las comunicaciones; eliminar el uso ilícito de las tecnologías de la información y las comunicaciones; asegurar la continuidad de la infraestructura crítica; desarrollar normas de seguridad cibernética benévolas para la industria; promover una cultura de seguridad cibernética y proteger las redes estatales (OEA. Sf).

Sumado a todo lo anterior, los países desarrollados y los organismos encargados de la seguridad cibernética, con tecnología de punta y una gran capacidad de capital humano, han podido implementar unos sistemas de espionaje y de control que facilitan la protección de la soberanía.

Entre los sistemas más relevantes se encuentran:

Sistema Echelon: Es una red de espionaje global, por medio de ésta red, se realizan interceptación de trasmisiones, se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar trampas terroristas y planes de narcotráfico, inteligencia política y diplomática. Este programa es capaz de vigilar, a través de satélites espías y estaciones de escucha. El sistema de satélites Echelon es una inmensa red de espionaje que, utiliza satélites para capturar las comunicaciones establecidas por radio, satélite, teléfonos móviles y fibra óptica y gigantescas redes de computadoras, intercepta millones de llamadas telefónicas, emails y faxes en todo el mundo, esto incluye a Latino América. Aunque, este sistema no sólo intercepta, sino que filtra, examina y codifica esta información (Sanchez.G.2013.).

El sistema Enfopol: Es una creación de los gobiernos europeos, que junto a los servicios secretos y de policía de la Unión Europea, tienen como objeto coordinar una fórmula que les permita realizar interceptaciones a las comunicaciones por Internet y el teléfono sin ningún tipo de control y sin que les acarree problemas judiciales, ya que las agencias de telefonía fija y móvil están bajo la normatividad de éste sistema al igual que los proveedores de internet. (Captación y uso de datos personales. 2001)

Además de estos dos, existen otros sistemas implantados en Europa. Por ejemplo:

> ..el Ministerio de Defensa español, junto con Italia y Francia, han puesto en marcha el proyecto Infraestructura Semántica Operacional, Donde por medio de ordenadores, que no sólo puedan identificar frases o palabras concretas en cintas de grabación o en textos escritos, sino que sean capaces de entenderlas…(Sánchez. G, 2013).

Caso Colombia

En el caso de Colombia la guerra electrónica, cumple funciones de monitoreo del espectro electromagnético, donde se realizan labores de rastreo de

forma aleatoria e indiscriminada, captando de manera incidental imágenes, datos, señales, información, comunicaciones tecnologías que permitan velar por la soberanía nacional, y logrando mantener la integridad territorial, estas actividades no implican seguimiento individual o determinado sobre sujetos concretamente considerados, ni interceptación o registro de comunicaciones privadas..

¿Pero qué ha sucedido en Colombia puntualmente?, la respuesta a esta pregunta se puede observar desde el año de 1999, ya que desde dicho año, se han reportado números ataques hacia infraestructura critica nacional, entre las que se encuentran las vías nacionales, oleoductos petroleros, antenas de comunicación, para el año 2002 se reportaron alrededor de 50 ataques en el año, en 2009 se dio un aumento considerable, con un reporte de 20 ataques mensuales.

Ante esta reveladora respuesta, nace una pregunta, tal vez más perturbadora, si se tiene en cuenta que en general la población nacional desconoce en su mayoría, sobre éste tipo de hechos, por lo cual es necesario cuestionarse, ¿Cuál ha sido uno de los ataques más sofisticados que ha sufrido Colombia? fue a mediados del 2009, cuando el sistema financiero vio comprometidos alrededor de 50 millones de dólares que desaparecieron de cuentas bancarias. (Ministerio de defensa. 2009) Sin contar con los ataques más frecuentes que según la Policía Nacional van desde, el robo de identidad, hurtos electrónicos, hasta el accesos abusivos a sistemas informáticos.

A pesar de que hace cuatro años, se empezaron a tomar medidas eficaces y eficientes para combatir la guerra electrónica, Colombia ya participó en una de las operaciones más efectivas para la captura de una banda de ciber delincuentes, el 28 de febrero del 2013, en donde se llevó a cabo la operación Unmask, operación que se desplegó y conformó en respuesta a los ataques persistentes contra la infraestructura crítica de Colombia y Chile.

Esta operación contó con la colaboración de inter equipos de respuestas incidentes y cuerpos policiales de Argentina, Chile, Colombia y España donde se realizaron varias redadas simultáneamente en 40 lugares de 15 ciudades distintas.

Logrando así el arresto de 25 delincuentes y logrando el decomiso de 250 dispositivos informáticos utilizados para estas actividades criminales. (INTERPOL. 28 de febrero de 2012)

En el año 2011, Colombia adoptó una estrategia de ciberdefensa y ciberseguridad a partir del documento CONPES 3701, el cual determino que se encontraría a cargo de 3 instituciones:

- El ColCERT, entidad encargada de coordinar y supervisar a nivel nacional todos los aspectos de la ciberdefensa y ciberseguridad. (DEPARTAMENTO NACIONAL DE PLANEACIÓN) Prestará su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC.

- El Centro Cibernético Policial (CCP), encargado de asegurar la integridad de las redes policiales y la sociedad civil con una vigorosa capacidad de investigación (DEPARTAMENTO NACIONAL DE PLANEACIÓN). Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el ColCERT.

- El Comando Conjunto Cibernético (CCOC), unidad militar encargada de responder ataques contra los bienes militares de la nación e infraestructura crítica (DEPARTAMENTO NACIONAL DE PLANEACIÓN). El CCOC deberá seguir los lineamientos nacionales en ciberdefensa y trabajará de manera coordinada con el ColCERT.

Para ilustrar de forma concreta el operar de las entidades anteriormente descritas, se presenta a continuación, gráficamente, el operacional del ColCERT, en la interacción simultánea entra las Fuerzas Armadas de Colombia y la Policía Nacional del país:

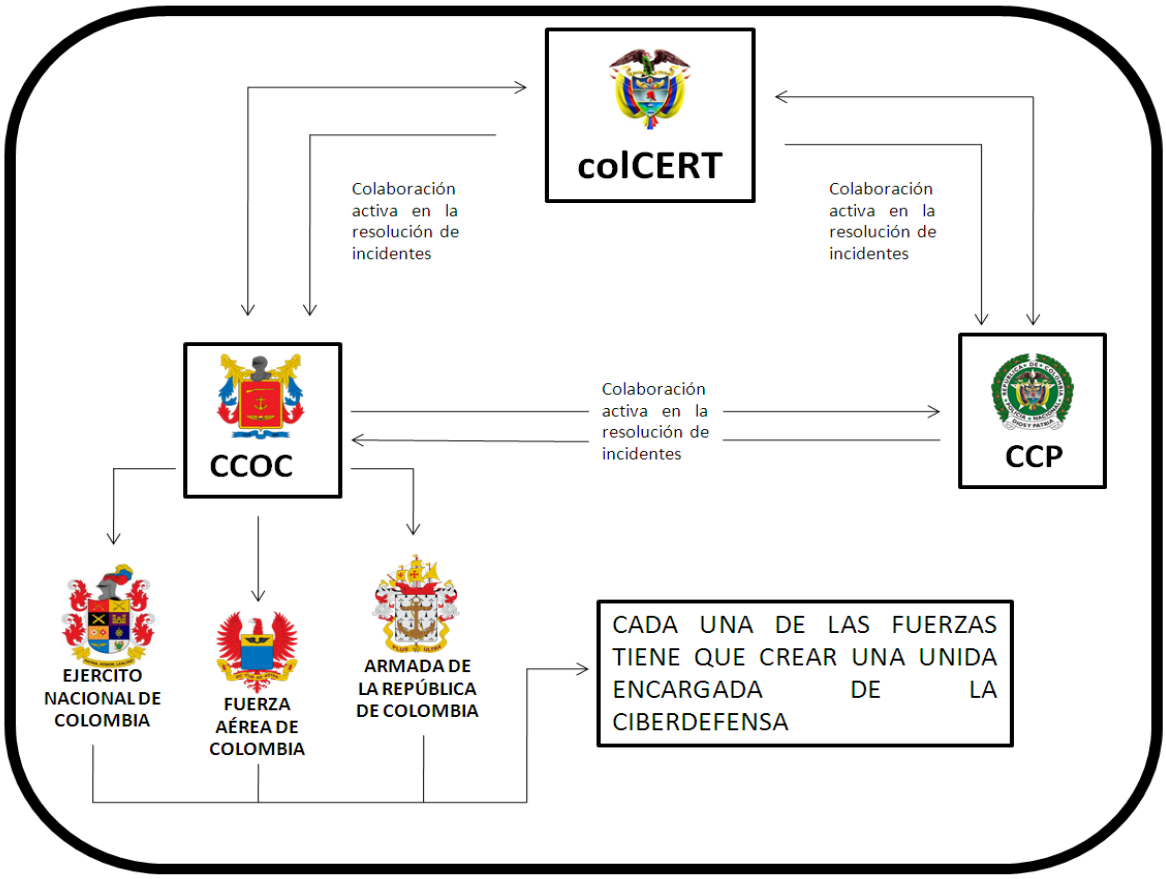

Figura 3. Estructura del organismo de Colombia de control en ciberdefensa y ciberseguridad

Fuente: Propia

Ya para el 2012, el Ministerio de Defensa crea un equipo élite de 150 miembros de la Policía y de las Fuerzas Militares para vigilar durante las 24 horas la plataforma informática del Estado, para evitar que sea blanco de ataques cibernéticos. Éste proyecto busca también reforzar los grupos de cibernética de la Policía y el Comando Conjunto Cibernético de las Fuerzas Militares. (El Tiempo. 2012)

Es así, como frente a los sistemas de control y de inteligencia de la ciberguerra de los países latinoamericanos, se puede observar, que en su mayoría no cuentan con tecnología de punta y el suficiente presupuesto económico, para

implementar sistemas similares a los que se encuentran en el Estados Unidos y Europa, como los ya mencionados.

Con todo lo anteriormente descrito, se puede concluir que hoy en día el internet es un elemento esencial en todas las sociedades, por que conecta millones de redes, las cuales hacen funcionar estructuras y sistemas indispensables de un país, de ahí que el tema de ciberdefensa y ciberseguridad ha empezado a ser un tema primordial en las agendas políticas de los gobiernos del mundo.

Desafortunadamente, para que la seguridad cibernética sea efectiva, se tendría que desconectar cada computador del mundo, lo difícil de esto, es que el mundo ya no quiere vivir sin la tecnología, a lo cual se suma que gracias a la globalización ya no puede vivir sin ella, haciendo casi imposible la implementación de esta acción. Sin embargo los países han optado por implementar otras medidas con el fin de contrarrestar este tipo de ataques y sus consecuencias

En el caso Colombiano tan solo hace unos 4 años se empezaron a implementar medidas contra los ataques cibernéticos, haciendo a Colombia demasiado vulnerable frente a otros países, por esto es necesario no solo tomar medidas que contrarresten los ataques al instante, sino que se deben plantear líneas de acción más profundas tales como:

- Crear una conciencia frente a los hábitos cibernéticos y la generación de la sensibilidad hacia la seguridad cibernética entre los usuarios, siendo ésta una de las medidas más económicas y eficaces para contrarrestar cualquier ataque cibernético así como también es importante reforzar la ciberseguridad.

- Dotarse de medios de seguridad especializados en ciberdefensa, para reducir la vulnerabilidad a la que se está expuesto, sin dejar atrás el hecho de que en cualquier momento estos medios pueden ser vulnerados, por eso es importante, que al lado de la implementación de estas medidas, se integren también contramedidas, (contramedida: disposición que se adopta para neutralizar una acción) (The free dictionary. 2013), y contra-contra medidas (contra-contra

medidas electrónicas: “DEF. Medidas tomadas para asegurar la utilización eficaz de las radiaciones del espectro electromagnético por las fuerzas propias a pesar de las medidas de guerra electrónica enemigas” (BTB de Termium Plus. Gobierno de Canadá. 2014) para tener un resultado más eficiente ya que es necesario contar con la planeación necesaria que asegure en lo posible, que los ataques se controlen en un 98% o 99%, así como sus consecuencias.

- Promover en las instituciones de educación privada y pública la creación y el refuerzo de programas de formación técnica y profesional en todo lo competente a manejos electrónicos y digitales, y en consecuencia la ciberguerra. Con esto se lograría tener un gran acervo de candidatos calificados para suplir el personal requerido por las organizaciones encargados de ciberguerra en el país, lo cual ofrece además, la visión del ciudadano del común y lo que de ello se difiere, alertando sobre otras posiciones de interés, frente a la posición de un militar o policía, de acuerdo tanto a la formación, como al deber, que desde las dos posiciones un Colombiano vive.

- Endurecer la legislación ya existente, en términos de delitos cibernéticos, ya que los casos presentados, por parte de hackers realizados más recientemente dentro de campañas políticas, han evidenciado la importancia de mejorar los vacíos judiciales presentes en el país, mediante, normas, leyes y condenas, que castiguen los delitos cometidos, por parte de personas que de manera ilegal extraen información y la utilizan con fines, poco éticos a fin de favorecer diversos intereses.

- Fortalecer todos los mecanismos de política, promoción de medidas y de futuras leyes, para asignar funciones y responsabilidades gubernamentales, relacionadas con la seguridad cibernética y establecer el intercambio de información y cooperación.

- El estudio y la aplicación de mayores contramedidas electrónicas para neutralizar cualquier intento de ciberataque, utilizados por las grandes potencias, con el fin de salvaguardar la soberanía nacional.

- Considerar la posibilidad de lanzar un satélite propio de la órbita geoestratégica. Para poder implementar sistemas de espionaje y de control sobre el espacio nacional, para lograr un mayor control de la información así como el uso de la misma.

- Implementar capacitaciones permanentes para los miembros de las fuerzas armadas encargados del ámbito del ciberespacio.

- Incentivar la investigación en lo relacionado con la seguridad cibernética para generar grandes avances en este campo y así los proteger la seguridad del Estado.

- Crear una unidad de contrainteligencia especializada en el ámbito del ciberinteligencia, con el fin de que se puedan identificar vulnerabilidades e individualizar los peligros potenciales que dichas debilidades permiten.

De la misma manera como un Estado tiene que proporcionar ciberseguridad y ciberdefensa, también tiene que adquirir responsabilidades de las actividades que se cometen adrede a través de sus agentes, organismos, funcionarios o terceros que maniobran por cuenta del Estado, ya que todo lo que implica el ejercicio de trabajar en el ámbito de defensa y en este caso cibernético, debe contar, con todas las medidas tanto de control como de capacitación, ya que exigir es fácil cuando no se conoce de la manipulación de una labor, pero es difícil ejercer de manera eficaz medidas que resulten, tanto apropiadas como seguras dentro del ejercicio de la vigilancia y el control.

Es decir, como en todo proceso y al igual que en toda organización se requiere, tanto de la formación constante y de calidad, con los medios que aseguren la excelencia dentro del operar, pues solo cuando se conocen de estos casos, las entidades gubernamentales y los gobiernos, discuten entre sí, y ponen en entredicho las capacidades y responsabilidades de tal manera que se pretenda hacer ver que no hay responsables manifiestos, dejando de lado la parte más importante que requiere de formación con excelencia, equipos de mejor calidad, espacios exclusivos de trabajo.

Así mismo es importante contar, con más visión, frente a la capacitación de las amenazas que superen la incidencia nacional, para lograr contrarrestar y eliminar cualquier intención negativa, ya que además de los problemas internos del país, en el mundo a cada segundo se conocen y se crean nuevos medios de invasión, que amenazan tanto la seguridad nacional como la seguridad internacional.

De esta manera, es importante humanizar el tema, pues es importante analizar la importancia que desde éste punto ofrece el principio de humanidad, establecido bajo el derecho internacional, el cual parte de la importancia que se debe tener frente a los derechos humanos a nivel mundial, ¿pero, cual es la relación entre derechos humanos, y ciberseguridad?

La respuesta es tan sencilla como poco analizada dentro de la problemática presentada, ya que dentro de la cadena de hechos que entrelazan las redes electrónicas y digitales del mundo, se encuentran los seres humanos, los cuales manipulan los mismos en favor de los intereses anteriormente descritos, con total y completo olvido, de vulnerar ese derecho fundamental que cobija tanto a víctimas como a victimarios, pues todos son seres humanos, y tanto la seguridad, como la paz, la dignidad y la privacidad, son derechos fundamentales de todo individuo, los cuales se rigen por el respeto, el mismo que cada vez es más vulnerado y olvidado, pues dentro del mundo globalizado, cada vez son más los seguidores de la vida digital y las facilidades que de ésta se difieren, quedando en manos de cualquier individuo, que con buenas o malas intenciones, tiene el total y libre acceso a la manipulación de las mismas, las cuales se escapan en ocasiones del interés de un gobierno, frente a otras problemáticas que se presentan al interior de un Estado.

Por todo lo anterior, es importante resaltar y cuestionar el papel que tanto gobiernos como autoridades están desempeñando frente a este tipo de hechos que vulneran la seguridad nacional, puesto que el manejo de la información, el acceso a la misma y los medios de recepción y de vigilancia, deben ser ejercidos solo por parte del personal idóneo y legalmente habilitado para hacerlo, lo cual si

bien supone de manera desafortunada un posible riesgo en cuanto a la posible fuga de información, como en todo ejercicio laboral, en su mayoría propone mayor seguridad.

Para esto es importante resaltar que no solo es necesario incrementar la responsabilidad por parte tanto de los gobiernos como de las autoridades, sino también incrementar las medidas de selección de personal en base a la ética, moral y los valores que los funcionarios presenten como característica personal y profesional, en base a desempeñar con los mismos, funciones enmarcadas dentro del ejercicio responsable y ético, disminuyendo tanto las posibilidades de perder información vital, como de proporcionar de manera segura, los medios y manejo de restricción de la información sensible.

Referencias

- BBC mundo. 15 de Marzo (2013). El mapa global de ciber ataques en tiempo real. Recuperado el 16 de julio de 2013. En: http://www.bbc.co.uk/mundo/noticias/2013/03/130315_tecnologia_ciberataques_mapa_aa.shtml

- BBC mundo. 17 de mayo (2007). La guerra fría cibernética. Recuperado el 27 de febrero de 2014. En: http://news.bbc.co.uk/hi/spanish/international/newsid_6665000/6665367.stm

- Bejarano. G, Pablo. 17 de septiembre (2013). Cómo preocupa a gobiernos y empresas el ciberespionaje de EEUU. Diario. Turing. Extraído el 10 de mayo de 2014. En: http://www.eldiario.es/turing/reaccion-ciberespionaje-prism_0_176383033.html

- Biblioteca virtual universal. (1909). Julio César (William Shakespeare). Extraído el 9 de julio de 2014. En: http://www.biblioteca.org.ar/libros/130807.pdf

- BTB de Termium Plus. Gobierno de Canadá 5. (2014). Recuperado el 2 de julio de 2014. En: http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-spa.html?lang=spa&i=1&index=alt&srchtxt=contra%20contramedidas%20electronicas

- Cano. J. (2013). Inseguridad de la información una visión estratégica. Pág. 151. Colombia: Alfa omega Colombiana S.A.

- Captación y uso de datos personales. (2001) ¡World. La revista de internet. Extraído el 9 de julio de 2014. En: http://users.dsic.upv.es/asignaturas/fade/oade/articulos/pdf/articulo9.pdf

- CNN expansión. 27 de mayo de (2013). Australia, ¿víctima de 'hackers' chinos? Extraído el 27 de febrero de 2014. En: http://www.cnnexpansion.com/tecnologia/2013/05/27/hackers-se-adentran-en-australia
- Coordinación de Seguridad de la Información. (2013) Conoce más sobre el PRISM. Extraído el 9 de julio de 2014. En: http://www.seguridad.unam.mx/noticia/?noti=1158
- Dinero. 12 de Septiembre. Colombia, segundo país más sensible a ciberataques. Recuperado el 24 de febrero 2014. En: http://www.dinero.com/empresas/articulo/colombia-segundo-pais-mas-sensible-ciberataques/159739
- El Tiempo. (2012) Ministerio de Defensa blinda al país contra la ciberguerra. Recuperado el 27 de febrero de 2014. En: http://www.eltiempo.com/justicia/ARTICULO-WEB-NEW_NOTA_INTERIOR-12243886.html
- Gasser. H. (2002). CICR. Terrorismo. (2002) Actos de terror "terrorismo" y derecho internacional humanitario. Extraído el 9 de julio de 2014. En: http://www.icrc.org/spa/resources/documents/misc/5ted8g.htm
- G. Sánchez. (2012) La ciberguerra: los casos de Stuxnet y Anonymous. DERECOM. No. 11. Nueva Época.p.124, 133.
- INTERPOL. 28 de febrero de (2012). Los hackers presuntamente vinculados con el grupo 'Anonymous' dirigido en operación global con el apoyo de INTERPOL. Extraído el 27 de febrero de 2014. En: http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
- Jefatura de gabinete de ministros presidencia de la nación. (sf).Oficina Nacional de Tecnología de Información. Extraído el 27 de

febrero de 2014. En: http://www.jgm.gov.ar/sgp/paginas.dhtml?pagina=27

- Julio César (William Shakespeare). 2012. Extraído el 5 de julio de 2014. En: http://www.acanomas.com/Libros-Clasicos/9286/Julio-Cesar-(William-Shakespeare).htm

- Ministerio de Defensa Nacional. (2009).Ciberseguridad y Ciberdefensa: Una primera aproximación. Recuperado el 26 de febrero de 2014. En: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

- Ministerio de Defensa. (2009). Cambio Climático en los desastres Naturales Ciberseguridad y Ciberdefensa: Recuperado el 27 de febrero de 2014. En: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

- Ministerio de Defensa. (2010). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Recuperado el 27 de febrero de 2104. En: http://www.bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

- Ministerio de Tecnologías de la Información y las Comunicaciones. 30 de marzo de (2014). Sin autor. Gobierno Nacional avanza en la construcción de una nueva política nacional de ciberseguridad y ciberdefensa. Extraído el 9 de mayo de 2014. En: http://www.mintic.gov.co/portal/604/w3-article-5851.html

- Morelli. A. (SF). Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio. Recuperado el 17 de marzo

de 2014. En: http://wwww.cari.org.ar/pdf/conflicto_internacional_ciberespacio.pdf

- OEA. (Sf). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Extraído el 27 de febrero de 2014. En: http://www.oas.org/es/ssm/cyber/documents/OASTrendMicroLAC_SmA.pdf
- Qué es un hacker. Seguridadpc.net concepto de hackers. Sf. Extraído el 9 de mayo de 2014. En: http://www.seguridadpc.net/hackers.htm
- Sánchez. G. Marzo-Mayo (2013). La ciberseguridad de Europa. Extraído el 27 de febrero de 2014. En: http://www.derecom.com/numeros/pdf/medero.pdf
- Seguridad. Prevención para ti. Hacking ético mitos y realidades. (2012). Anaid Guevara Soriano. Extraído el 2 de julio de 2014. En: http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades
- The Free Dictionary. Contramedida. (2013). Extraído el 2 de julio de 2014. En: http://es.thefreedictionary.com/contramedida
- Guerra electrónica. Cátedra in-nova. Universidad Politécnica de Madrid. Extraído el 3 de julio de 2014. En: http://catedrain-nova.etsit.upm.es/index.php/formacion-continua/presencial/15-tdf/52-guerra-electronica
- U – Historia. (sf) Guerra Electrónica. Extraído el 2 de julio de 2014. En: http://www.u-historia.com/uhistoria/tecnico/electronica/electronica.htm
- Von Hein. M Y Papaleo. C. 30 de marzo de (2010). Inicia tareas Central alemana de Defensa contra Ciberataques. Extraído el 27 de

febrero de 2014. En: http://www.dw.de/inicia-tareas-central-alemana-de-defensa-contra-ciberataques/a-14954034

Sandra Camila Valencia Rojas