Ciberguerra, entorno global y preparación de defensas

Juan Manuel Ruiz González.
Especialización en seguridad Informática.
Universidad Piloto de Colombia
Mgmanolo23@gmail.com

***Resumen*- Este documento exhibe diferentes aspectos y características acerca del panorama internacional de la Ciberguerra, definiendo términos informáticos, usados en amenazas y sus posibles métodos de ejecución, también las posibles medidas en las que se pueden prevenir estos ataques por parte de organizaciones nacionales e internacionales este nuevo tópico de delito y guerra del siglo XXI.**

Abstract: this paper show different aspects and features about the international scope of Ciber warfare, defining informatics terms, used threats and possible methods of execution, also the possible measure that can prevent these attacks by national and international organizations in this new topic of crime and warfare of the XXI century.

***Palabras Clave*- ciberguerra, Ciberataque, malware, virus informático, seguridad nacional, Ciberterrorismo, hacker.**

Keywords – cyberwar, cyberattack, malware, IT, national security, cyber terrorism, hacker.

I. INTRODUCCIÓN

Este artículo contiene parámetros acerca del crecimiento exponencial y la importancia que ha tenido la tecnología a través de los años, ingresando en el diario de toda sociedad, haciéndose participe de todas las actividades que se desempeñan en las culturas mundiales, evidenciando, que existe una guerra silenciosa donde el ataque primordial se ejecuta sobre el activo más preciado en toda organización ya sea pública o privada, de carácter militar, estrategia comercial, o un objetivo individual perpetuado por uno o más hacker o hactivistas, con el hecho de conseguir la preciada información.

Cyberwar. The thread from the Internet, la portada y *Cyberwar* el título de la editorial del primer número del mes de julio de 2010[1] de la prestigiosa revista británica ***The Economist,*** en la que hace énfasis en su escritura al informar que es momento en que los países comiencen a dialogar sobre el control de las armas cibernéticas en Internet.[2]

Teniendo como su principal arma el malware o los diferentes virus informáticos, son uso, con herramientas especializadas en la penetración de la seguridad de diferentes sistemas de información, los expertos en informática desarrollan de manera propia, formas lógicas de vulnerar una infraestructura tecnológica. Por otra parte, las organizaciones gubernamentales y/o militares conformadas para combatir el Cibercrimen, Ciberterrorismo, etc. Desarrollan técnicas de contingencia con un único fin de preservar la integridad de la información ya sea de una organización o de un país, preservando su seguridad nacional, mostrándonos que estos ataques están en considerable aumento y proporción al daño causado por quienes lo ejecutan.

De esta manera nos enfrentamos a una evolución incompleta por parte de la humanidad, el gran peligro que a diario se expone al estar interactuando con un aparato tecnológico compartiendo información, donde no se es consciente de la integridad en la que está expuesta toda la soledad en la red, un abanico grande que permite distintas actividades que van desde situaciones decentes y educativas hasta situaciones perversas donde dejan en tela de juicio de forma denigrante cualquier intimidad. Así se explota un coeficiente para causar daño a un congénito bien sea su patrimonio o su ser. Sin darse cuenta que la manera más fácil de seguir avanzando es ayudando a los demás.

II. ¿QUÉ ES CIBERWAFARE Y A QUIÉN VA DIRIGIDO?

Si intentáramos encontrar una definición cuando nos referimos a una guerra cibernética o guerra informática, diría que es un conjunto bélico establecido en un cuadro de operaciones, donde el campo de batalla cambia radicalmente ya que no es necesario la perdida humana y destrucción masiva para lograr un objetivo, esta se traslada al ciberespacio generando una amplia gama de vectores de ataque con su propósito de inhabilitar un sistema de información de un adversario o competencia ya sea con fin de la anulación del enemigo o la sustracción de información que al final de cuentas se convierte en el botín más preciado de todo ataque.

Existen aspectos que van ligados al enfrentamiento silencioso que ocurre a lo largo de la historia de la guerra cibernética como lo son los delitos informáticos, como su nombre lo indica se trata de toda acción que va en contra de los principios morales y éticos perpetuados en la red sin importar su objetivo. Existe el Ciberterrorismo, cuya mayor característica enfoca un ataque premeditado, políticamente en ejecuciones contra países o de carácter comercial como lo publica el diario el país el 25 de nov de 2014 “Un ataque informático paraliza a Sony Pictures”. Aunque no solo se

[1] The Economist, Volumen 396, number 8689, July 3rd-9th 2010.
[2] Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio, edición febrero de 201.

trata de daños a gran escala ya que dentro de los muchos aspecto que abarca se encuentran temas de extorsión, intimidación y demás tópicos de esta índole comprometiendo la integridad de una persona u organización en la cual se vea afectada con algún acto delictivo en la red.

Ahora pues, multitudinarios ejércitos conformados por hackers de tipo civil y militar conforman los diferentes equipos de ataque y defensa en diferentes países a nivel mundial de forma clandestina ejecutan pruebas, realizan inserciones a conveniencia, accediendo a lugares donde pudieran encontrar información confidencial de empresas, información sensible de usuarios que utilizan la red, secretos empresariales, temas ultra secretos de seguridad nacional. Toda esta información usada en contra de una nación, puede dar una clara ventaja en el momento de un ataque a gran escala ya que el factor sorpresa en caso de reacción, no será posible porque se conoce de antemano el actuar conforme a la ganancia del atacante.

Aunque existe alguna comunicación y cooperación entre diferentes agencias de diferentes naciones con fines de conservación de la integridad ante el Ciberterrorismo, estas a su vez son las primeras líneas de control ante una amenaza crítica a una infraestructura sistemática, velando con cada una de sus lecciones aprendidas la reducción del riego al que se expone todo el tiempo. Aún falta mucho trabajo para lograr prevalecer intacta la información dentro de algún sistema de información ya que las amenazas se han convertido en una importancia primordial que obligan a estar alertas ante un riesgo de Ciberguerra que no se puede seguir mitificando con el hecho de que todos los días los gobiernos gastan importantes sumas de dinero en inversiones que buscan acordonar sus bienes digitales.

Existe demasiado patrimonio en juego de cada país como lo son entidades financieras que en muchos casos soportan la economía del mismo, empresas, multinacionales, entidades estatales que hacen una sola gran cantidad de información y en el peor de los casos la fuga, infiltración, robo, Publicación y demás aspectos pueden desencadenar una serie de altibajos culturales, para un país que podría llegar a su anulación de estado. No es exagerado hacer una apreciación de semejante magnitud, solo basta con ver la nueva guerra fría. Así es llamada a las diferentes interceptaciones de comunicaciones por parte de los Estados Unidos y la Republica de china, si bien es cierto que: ante la percepción mundial de una persona del común dice que son potencias comerciales ya que sus economías son muy sólidas, también se evidencian actos de Ciberterrorismo silencioso como lo expone en su web gitsinformatica enunciando temas de esta índole: "*Un informe elaborado por Team Cymru y al que ha tenido acceso exclusivo The Verge, ha descubierto Ciberataques masivos que tienen como consecuencia el robo de hasta un terabyte de información diaria. Un robo a escala industrial, dice un ex detective de Scotland Yard*[3].

Ahora con el tamaño de información sustraída como lo dice el anterior texto. La cantidad de información es alarmante si en cuanto a temas de seguridad se refiere o fuga de información, su objetivo es y seguirá siendo, reducirlo a 0.

Así pues la ciberguerra no solo está dirigida, a una persona que no tiene actualizado su software de antivirus en casa, oh a personas que usan sistemas operativos no convencionales, tal vez a personas involucradas de una u otra manera en un entorno tecnológico, además de todo esto también existen focos en la industria cualquiera que sea, instalaciones militares, investigaciones de cualquier índole tecnológica, fabricantes de armas de destrucción masiva, avances biotecnológicos, plantas nucleares, y en el peor de los casos a toda la población, donde un ataque terrorista destinado a desestabilizar, desanimar o destruir. Esta nueva guerra que se libra detrás de cables y computadoras que no excluye civiles de militares organizaciones de naciones ONG'S de hactivistas, ella estamos todos y lo importante es el que hacer para contenerlo.

III. ARMAMENTO DE GUERRA

Como existe la inversión en avances para la sociedad, también lo hay para la creación de armamento tecnológico interesado en causar el mayor daño posible en el momento de su uso, virus, en su mayoría, son algoritmos desarrollados por expertos, diseñados para penetrar, dañar, alterar, sustraer, destruir. Diferentes sistemas informáticos que son su principal fuente de ataque, aunque son incalculables los ataques más comunes a toda población la cual les realizan constantemente, a través de estafas por técnicas como phishing identificado como suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta[4].

De esta manera evidencio que existe una gran cantidad de formas o modelos para adquirir información tanto como para una sola persona, como también existen los ataques diseñados a gran escala que han sido propuestas en los últimos años como lo informa el diario el mundo de España "guerra informática en serbia"[5]. En el cual dice que expertos informáticos durante el año 1999 combaten de manera electrónica, el ejército serbio al mando del reconocido capitán Dragan, considerado héroe nacional por ataques perpetuados durante la guerra que libro este país contra su homologo croata 8 años antes, Dragan poseía 40 ordenadores con los cuales contrarrestaba ataques por parte de la OTAN[6]. Realizaron penetraciones a equipamiento sistemático de la

[3] Ciberguerra, Ciberespionaje, Ciberterrorismo y Ciberdefensa. . www.gitsinformatica.com/ciberguerra.html,copyright 2003

[4] Definición de phishing, https://es.wikipedia.org/wiki/phishing, última fecha de modificación 1 de junio de 2015.

[5] Guerra informática en serbia, www.elmundo.es/navegante/99/abril/16/hackers.html. Viernes 16 de abril de 1999.

[6] Acrónimo para dar significado a la organización del tratado del atlántico norte, denominada alianza del atlántico firmado en Washington 4 de febrero del 1949.

OTAN y el portaaviones norteamericano Nimitz, el ataque deja una negación de permisos sobre el portaaviones con imagines obscenas del presidente de turno de los Estados Unidos durante todo un fin de semana, además de la modificación de las noticias que según los serbios la OTAN manipuló, información que en su momento daba al mundo, también páginas web de la casa blanca fueron bloqueadas como resultado del contraataque serbio.

En otro lapso de tiempo con una mayor intensidad China ejecuta ataques informáticos sobre Taiwán, de una década en su duración, ejecutada entre el 2003 y el 2013, introduciendo un virus de tipo troyano en cerca de 30 entidades del estado y consiguiente a más de 50 empresas privadas con el objetivo de sustraer información y provocar una parálisis en la isla como lo informa el ministro de ciencia y tecnología Simón Chang en una entrevista. Además de ello informa que su equipo de trabajo es relativamente nuevo y pequeño en comparación al equipo que contiene la república de China y que son constantes y de gran envergadura los ataques informáticos.[7]

Tal vez uno de los ataques más majestuosos debido a que ningún grupo se dio atribuido el hecho y que fue especulativo hacia los rusos, fue la penetración a instalaciones estatales y de importancia para los negocios de Estonia en el 2007 donde inicialmente sustraen una importante suma de dinero de una entidad bancaria, pese a la gran estructura informática que tiene este país con avances en temas de votación, control de registro electrónico, almacenamiento de datos de sus residentes. Poco o nada pudo hacer para evitar el ataque desarrollado. A causa por el traslado de una estatua de bronce en agradecimiento a pueblo soviético en defesa de retaliación bélica por parte de los nazis. Los rusos al sentir que el traslado de dicha estatua se sintió como una ofensa en retaliación destruyen una gran parte de la infraestructura digital de la nación interrumpiendo medios de comunicación, bancos, entidades del estado promoviendo caos en el país[8].

"Stuxnet: el virus capaz de crear el caos absoluto"[9]. En el 2010 un virus que se propago por el mundo con el único fin de llegar a plantas nucleares de Irán, crea un nuevo concepto de ataque y la evolución en el desarrollo de los virus informáticos, pues esté, ataco plantas industriales como lo fue en caso específico que cambio los parámetro de las centrifugadoras para enriquecer uranio, este ataque pudo haber sido devastador donde en alguna parte de la infraestructura del centro nuclear Iraní Natanz, hubiese hecho explosión, se estima que el retraso en el estudio nuclear de irán estará de 10 a 20 años en reposo debido a que estas centrifugadoras no podrán usarse por su radiación. Ahora personas referentes al tema hablan sobre la preocupación de posibles mutaciones del virus o diversos puntos de ataque hablan de lo que sería capaz. ¿Que podría hacer en un sistema similar si atacase a un aeropuerto?, ¿de qué magnitud seria el caos?, o ¿si atacara un hospital?, tal vez modificar fichas cambiar los sistemas de suministro de medicamento, ¿que podría hacer dentro de los sistemas de generación de electricidad de ciertos países en caso de que logre acceder a sus infraestructuras y sus telecomunicaciones?[10] Según expertos, Stuxnet es un programa en concreto de la marca siemens que utiliza el control de oleoductos, plataformas petroleras, centrales eléctricas y otras entidades industriales con el fin de hacer modificaciones.[11]

También para este año, en el 2010 miles de internautas lanzaron desde sus máquinas, millones de ataques contra las webs de la Sociedad General de Autores y Editores (SGAE), el Ministerio de Cultura y la patronal discográfica Promusicae. Los convocantes, que protestaban contra el canon digital y la ley que perseguirá a las páginas de descargas no autorizadas, consiguieron su objetivo de tirar abajo durante horas las webs atacadas y una repercusión mediática que pocas manifestaciones callejeras.[12]

Pese a que el equipo informático de la institución intento evitar el ataque que fue anunciado por el grupo de Ciberactivistas Anonymous no pudieron hacer mucho ante más de 300 millones de peticiones registradas por el servidor durante 3 días que duro el ataque, dando como fin dejar sin el servicio de la webs de las organización. Con este ataque nos enseña que la guerra cibernética no solo es basada de nación a nación si no que nos muestra un vector de ataque totalmente distinto al ideal que habíamos enunciado anteriormente.

Otro vector importante es ejecutado desde alguna nación en específico hacia una entidad de algún otro país como lo informa el diario el universal de México: "New york times denuncia ataque de hackers chinos"[13] donde informan que hubo una infiltración a los equipos de diferentes periodistas que en su momento trabajaron o aún continúan en el diario, con fines de sustracción de información acerca de las riquezas de la familia del primer ministro chino. El times, contrata expertos en seguridad con el fin de bloquear las penetraciones hechas por parte del gobierno chino, ya que en su rastreo identifican varias entidades militares como responsables de los actos, también relatan que la información contenida acerca de la familia no fue comprometida en ningún aspecto. Así

---

[7] Taiwán confirma los ataques informáticos de china continental. www.spanish.rti.org.tw/new/?recordId=9462. 13 de agosto de 2014

[8] Estonia, primera víctima de los hackers. www.elpais.com/diario/2009/05/30/internacional/1243634402_850215.html, sábado 30 de mayo de 2009.

[9] Stuxnet: el virus capaz de crear el caos absoluto. www.actualidad.rt.com/actualidad/view/111953-stuxnet-virus-iran. 25 de Noviembre de 2013

[10] Stuxnet: el virus capaz de crear el caos absoluto. www.actualidad.rt.com/actualidad/view/111953-stuxnet-virus-iran. 25 de Noviembre de 2013

[11] Irán sufre un ataque informático contra sus instalaciones nucleares. www.elpais.com/diario/2010/09/28/internacional/1285624808_850215.html. 28 de septiembre de 2010

[12] Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Ministerio de defensa española. Instituto español de estudios estratégicos. febrero de 2011

[13] Diario mexicano informa sobre el ataque de china a un periódico de los Estados Unidos www.eluniversal.com.mx/notas/899692.html,

pues se acusa a china de promover una gran campaña de ciberespionaje amplia y agresiva como también el caso de la operación aurora el cual china como responsable de los actos en contra los servidores de google, juniper, adobe. Y varias empresas que aún no se dieron a conocer dan como hecho el robo de información a la propiedad intelectual de estas organizaciones diseñado con un malware como su principal arma de ataque ejecutando un exploit de tipo 0 Day embebido en archivos PDF.[14]

Otro de los más grandes ataques, esta vez contra Internet lo promovieron dos compañías como lo es Spamhaus, organización encargada de rastrear proveedores de correo no deseado y por otra parte Cyberbunker organización especialista en generar correo no deseado o Spam. El ataque se originó en una trasmisión de paquetes de 300 Gb por segundo le atribuyen la responsabilidad a Cyberbunker luego de la compañía de lucha contra el Spam la haya declarado paraíso para el Cibercrimen y el correo indeseado o Spam.[15]

Se reconoció que este ataque de denegación de servicio generado mediante el método spoofiing pudo afectar la velocidad del internet en todo el mundo aunque no se estableció la responsabilidad de los hechos Spamhaus acusa a dicha entidad la promotora de los actos delictivos, días después el portal gizmodo publica que evidentemente existió un ataque a gran escala pero no lo suficiente para tumbar Internet ya que muestra gráficos donde no hay una colisión de este estilo solo un pico de tráfico.

FIGURA 1

Habría caídas masivas y los picos de los gráficos si la guerra se está librando a través de la red.

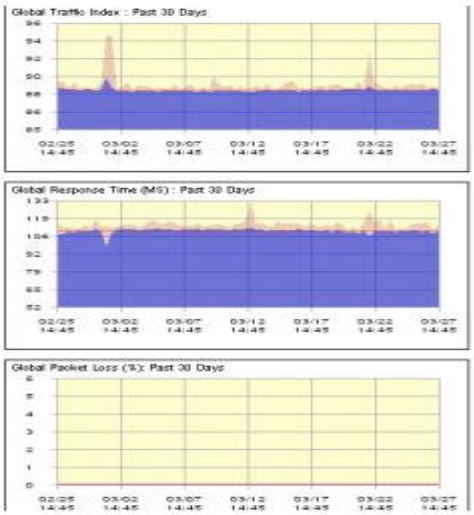

Fig. 1. Picos de tráfico de internet [16]

Uno de los ataques que empiezan a tomar forma ya que por hechos confusos no se atribuyen a nadie en específico y que en la actualidad es el ataque ejecutado hacia el servicio de Play Station Network de Sony, en donde a mediados del año anterior el servicio fue afectado por un ataque de negación de servicios a los usuarios, el cual satura el sistema con la cantidad de trafico suministrada pero que en ningún momento pudo acceder a la información de sus cerca de 53 millones de clientes. Pese a la atribución del hecho se da a un usuario de twitter de seudónimo @LizardSquad el cual en su cuenta se pronuncia en lo siguiente "Sony, otra gran compañía, pero están gastando las olas de dinero que obtienen en el servicio a sus clientes (de PlayStation Network). Pongan fin a la codicia"[17].

Aunque el mensaje no quedo del todo convencido que fue desarrollado por un hacker, al tener un segundo ataque, esta vez a sus estudios cinematográficos Sony Pictures, en los que tuvieron que aplazar el lanzamiento de una cinta en relación al régimen de corea del Norte, mediante amenazas de igual envergadura a las del 11 de Septiembre donde diferentes casas de cine cancelaron su apertura y por su parte Sony cancela su lanzamiento sin fecha de estreno por temor a los diferentes chantajes terroristas. El país asiático declaro que no tenía conocimiento acerca de este delito pero el FBI informa de manera clara en la columna del diario el país que: "tenemos información para concluir que el gobierno norcoreano es el responsable".[18]

Paradójicamente tres días después de la promesa del presidente de los Estados Unidos al decir que se tomaran medidas con el anterior caso, Corea del norte sufre un apagón de internet hecho que lo dejo sin operatividad cerca de 10 horas a este país, de la mano, con la respuesta no muy agradable por parte de los Estados Unidos a la colaboración ofrecida por corea en la búsqueda de esclarecer los hechos que arremetieron contra Sony no solo se sostuvo el apagón si no que luego de ello su conexión fue bastante lenta en comparación a la anterior, aunque existen varias teorías nadie ha hablado públicamente sobre la responsabilidad de los hechos, pero este mismo día a través de un comunicado Pyongyang Primer ministro coreano advierte ataques sin especificar el tipo, hacia la casa blanca, el Pentágono, y todo el territorio de los Estados Unidos. "El ejército de corea del norte están completamente listos para la confrontación con los Estados Unidos en todos los espacios de guerra, incluyendo el espacio guerra cibernética"[19].

[14] que es operación aurora. www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora. 21 de enero de 2010.

[15] Empresas detrás del hackeo que freno internet www.radiosantafe.com/2013/03/28/spamhaus-y-cyberbunker-las-empresas-detras-del-hacker-que-freno-a-internet. Marzo 28 de 2013.

[16] evidencia de tráfico de red www.gizmodo.com/5992652/that-internet-war-apocalyse-is-a-lie. 27 de marzo de 2013.

[17] Hackean servicio de PlayStation Network de Sony www.forbes.com.mx/hackean-servicio-de-PlayStation-Network-de-Sony/ junio 17 de 2014.

[18] FBI acusa a corea del norte formalmente del Ciberataque a Sony www.internacional.elpais.com/2014/12/19/actualidad/1419009199_719868.html. 19 de Diciembre de 2014.

[19] corea amenaza a Estados Unidos a raíz del hackeo de Sony www.lanacion.com.ar/1754717-corea-del-norte-amenaza-con-atacar-a-eeuu-a-raiz-del-hackeo-a-sony. Lunes 22 de Diciembre 2014.

IV. METODOLOGÍA DE DEFENSA

Así como existe la estructuración de técnicas y métodos para el desarrollo de armas cibernéticas, también existen estructuras o guías para la implementación de seguridad en lo que respecta a un sistema de información cuyo principal objetivo es el aseguramiento del éxito de una empresa que cuente con requisitos de seguridad ante el negocio, teniendo claro su política de seguridad, esta es la que da valor agregado a sus activos intangibles como lo es su información, hay que tener en cuenta que a medida que va creciendo una empresa y que abarca un mayor espacio de mercado existe mayor riesgo de ataque ya que sus campañas publicitarias hacen que esta sea más visible, y por ende sea más factible el cambio de nuevas tecnologías aplicadas a la reestructuración del negocio.

Pero antes de implementar una guía de seguridad, hay realizar un diseño sobre el grupo de trabajo donde se establezcan, funciones dentro de un marco operativo que vaya acorde al core del negocio o entidad estatal, dentro de ellos, realizar la conformación de grupos que definan aspectos legales de desarrollo y solución, que involucren como prioridad la seguridad informática. Así tener un gobierno establecido para la implementación de herramientas como esquema de seguridad ya sea la conformación de las ISO 9000 para los temas de calidad, ISO 27000 para el esquema de seguridad y la ISO 20000 de la mano de Itil, para llevar todos los temas que tiene que ver con gobierno, así se puede establecer un buen conjunto de guías o servicios aplicables a la estructura general de una empresa. Ahora, no solo existe este posible esquema, hay otras dos buenas propuestas dentro de las muchas posibilidades que rigen a un buen esquema de seguridad en una organización, CobiT se proyecta en un marco de gobierno de tecnologías, planteando un contenido sobre procesos de regulatorio cumplimiento y es adaptable a cualquier modelo de negocio con el que se desee implementar.

En su última versión, Cobit 5 implementa seguridad en su esquema de gobierno IT, que en su mayor énfasis se da en garantizar la seguridad de los sistemas donde se enfoca en otro modelo relacional de nombre BMIS donde incorpora una visión integra a esta versión de Cobit, con sus mayores características, establece un lenguaje para el uso exclusivo de la protección de la información, plantea un modelo no convencional de la inversión en seguridad de una empresa y explica en detalle toda la estructura del modelo gestionando para la seguridad con el negocio, que en proporción se rige bajo una perspectiva sistémica.

Muchas de las características base del modelo BMIS han sido implementados en el modelo Cobit versión 5, es de aclarar que aunque se compartan aspectos de implementación en cuanto a su seguridad son modelos por separado que enfocan a la seguridad interactuando directamente con el negocio dando respaldo a su continuidad, alcanzando los objetivos de crecimiento y valor el cual propone, una visión de gobierno y gestión en la seguridad de la información hacen parte de su modelo que en verdad son sugerencias en detalle como parte de un refuerzo en las políticas, procesos, estructuras y demás implementaciones que acarree cada empresa.

De acuerdo con ISACA el modelo BMIS es adaptable a cualquier circunstancia de negocio de acuerdo con la implementación suministrada previo a la administración sobre la información y la seguridad física, este modelo identifica cuatro pilares los cuales son base fundamental para su funcionamiento que son: la organización, los procesos, las personas y la tecnología. Son elementos que participan en relación de las partes por medio de la cultura empleada al factor humano que rige la organización, teniendo una arquitectura sólida que esta soportada en la tecnología ejecutando procesos de mejora continua dando soporte en el conjunto de gobierno de la seguridad de la información.[20]

V. CIBERGUERRA EN COLOMBIA

En Colombia desde el año 2005, han creado programas de defensa para velar por la seguridad cibernética, el ministerio de relaciones exteriores crea un equipo con el fin de analizar temas que conciernen a la problemática global del ciberespacio, junto con el ministerio de las TICs mediante consultorías donde identifican brechas de seguridad con todas las posibles mejoras que se deben tener para velas por la nación en cuanto temas referentes de la seguridad en la información, este grupo en el 2009 entra a hacer parte del ministerio de defensa nacional conformado como el colCERT cuyo objetivo principal es la coordinación de acciones necesarias que ayuden a la protección de las diferentes infraestructuras del estado haciendo frente a un posible ataque que comprometa la seguridad nacional[21].

Otra medida de defensa para combatir ataques cibernéticos también existe el Comando Conjunto Cibernético (CCOC), el Centro Cibernético de la Policía Nacional (CCP) , los cuales además de sus portales web donde contienen información en materias de seguridad de la información y seguridad al ciudadano, por su parte la CCOC adelanta investigaciones y avances de la mano con el pueblo israelita el cual es uno de los países vanguardistas en temas de Ciberdefensa y Ciberseguridad, los cuales contemplan temas de seguridad sobre servicios financieros, educativos, mercantiles y demás en lo que avaluaron principalmente aspectos de protección.

Claro está, que según datos suministrados por los portales anteriores, existe una cantidad alarmante de victimas que por alguna modalidad de fraude en la internet les han dejado perdidas sumamente costosas para ellos y para el país, sin contar los sin números de robos de información, nombres de cuentas de usuarios y contraseñas, estos son algunos de los delitos más comunes en la sociedad colombiana en materia de ciberespacio, incluyendo la sustracción de cuentas de correo en la casa de Nariño, de esta manera vemos que aunque no somos capaces de controlar la delincuencia local por llamarlo de alguna manera. Ante la preocupante oleada de desfalcos en

---

[20] Resumen modelo BMIS elaborado por Ing. Juan Carlos Alarcón S, PMP, CISM, 2010

[21] Ciberseguridad y Ciberdefensa: una aproximación. www.mindefensa.gov.co/irj/go/km/mindefensa/documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20Ciberdefensa.pdf. Octubre 2009

el internet el gobierno desarrolla un nuevo plan de Ciberseguridad y Ciberdefensa, donde destacan organismos de control digital bajo la regulación de la agencia nacional de seguridad cibernética, con el fin de fortalecer las diferentes oficinas de seguridad civil, policía, militar, publico, privada. En otro aspecto también conforma convenios internacionales para la capacitación de sus fuerzas en defensa creando en conjunto una línea extensa que abarque personal desde las universidades, en colaboración con las organizaciones especializadas en seguridad que son las que conformarían dicha agencia.

La función de esta agencia estará destinado al continuo monitoreo de todas y cada una de las entidades del estado si estimar si su procedencia sector con el fin de identificar brechas de seguridad, virus, hackeos, etc. Para ello tendrán la colaboración plena de los operadores de internet con el fin de generar reportes de tráfico sin extralimitar su alcance prevaleciendo la información sensible y confidencial de los demás, de esta manera se realizarían inspecciones de carácter preventivo a las redes nacionales con el fin de lograr el ingreso al convenio firmado en Budapest, conformado por los Estados Unidos la Unión Europea Japón y Canadá que lo que buscan es unificar la penalización de los delitos cometidos en la red.

El señor presidente de Colombia Juan Manuel Santos ha sido enfático en la creación de la agencia nacional de seguridad cibernética inmediatamente después de haberse enterado de las interceptaciones de comunicación comprometiendo información de los diálogos de paz que se adelantan en la Habana, esta información la dio después de la reunión de la comisión digital realizada el presente año, se espera que lleve consigo la legislación que debe tener el país no para evitar si no para mitigar o reducir un impacto ante un ataque cibernético, es de aclarar que por mayor defensa que se implemente en materia de seguridad informática no es posible dar un cien por ciento de plenitud en su esquema, "desde Agosto de 2011 el Conpes había aprobado $16.428 millones para creación de organismos de defensa y seguridad cibernética"[22].

En la siguiente imagen se muestra algunas iniciativas de diferentes países en temas de regulación para los temas de Ciberseguridad y Ciberterrorismo.

FIGURA 2
Ciberseguridad y Ciberdefensa: Desafíos emergentes para los profesionales de Gobierno TI.

PAÍS	INICIATIVA GUBERNAMENTAL
ALEMANIA	En febrero de 2011, el gobierno alemán lanzó su Estrategia de Seguridad Cibernética. En abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa.
AUSTRALIA	Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.
CANADÁ	El Departamento de Seguridad Pública implementó el Centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.
ESTADOS UNIDOS	Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: National Cyber Security Division, US-CERT: United States Computer Emergency Readiness Team y la oficina de Seguridad Cibernética de la Casa Blanca. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciber amenazas. En este mismo año es adoptada una Estrategia de Seguridad Cibernética.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 fue adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información.
COLOMBIA	Se publica el 14 de julio de 2011 oficialmente el documento del Consejo Nacional de Política Económica y Social relacionado con ciberseguridad y ciberdefensa.

Fig. 2. Ciberseguridad y ciberdefensa: Iniciativas internacionales.[23]

VI. CONCLUSIONES

1. Hay que promover y/o incentivar a la personas para que realicen y participen de capacitaciones para poder estar preparados y reducir cualquier tipo de agresión que incluya una infraestructura tecnológica que se esté salvaguardando y a que para todos y cada uno sean conscientes de que un ataque cibernético por incapacidad o desconocimiento puede ocasionar desastres irreparables.

2. Incentivar la adquisición de carácter físico y humano para la defensa en contra de ataques que comprometan la seguridad con impactos sumamente altos, en comparación con ataques nucleares con el fin de neutralizar el origen de dicha perpetuación.

3. Los actos que van en contra de la moral y la ética dentro de un entorno cibernético que afecten cualquier infraestructura legal de un país debe ser considerada un acto reprochable por ende debe ser tratado con rigurosidad de Defensa Nacional.

4. En el mundo actual nos enfrentamos a una guerra cibernética a diario la cual es asimétrica teniendo en cuenta el desarrollo de las naciones se debe conformar un excelente equipo con conocimientos de elite las cuales también puedan desestabilizar un estado o nación en pro de la defensa aún más poderoso.

5. El no contar con recursos aptos para la participación de la guerra no asegura que nadie no ejecute algún tipo de

[22] Icontec. Gobierno creará la Agencia Nacional de Seguridad Cibernética. http://icontec.org/index.php/ho/noticias-destacadas/1419-gobierno-creara-la-agencia-nacional-de-seguridad-cibernetica

[23] Ciberdefensa y Ciberseguridad desafíos emergentes para los profesionales de gobierno IT, jeimy J Cano JMC10/11 reglamento isaca. http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/243.pdf. Página 27.

ataque, por el contrario el riesgo es aún mayor ya que no cuenta con ningún mecanismo de defensa.

6. Se deben estipular de la manera más clara posible las reglas que involucren algún uso de los recursos estipulados para la guerra, evaluar un nivel jerárquico establecer políticas y responsabilidades y definirlas sobre los directos responsables o primer respondiente, los cuales determinan y toman decisiones trascendentales en alguna situación real.

7. Concientizar a la comunidad dándole a conocer la verdad y que este tema es más delicado que una película de ciencia ficción.

8. Ejecutar una alianza estratégica en tema de seguridad con la región (latino América) es un excelente programa ya que existen varios países que llevan un poco más lejos sus programas de Ciberdefensa como lo es el caso de Argentina y Brasil.

REFERENCIAS

[1] The Economist, Volumen 396, number 8689, July 3rd - 9th 2010.

[2] Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio, edición febrero de 2011.

[3] Ciberguerra, ciberespionaje, Ciberterrorismo y Ciberdefensa www.gitsinformatica.com/ciberguerra.html,copyright 2003.

[4] Definición de phishing, https://es.wikipedia.org/wiki/phishing, última fecha de modificación 1 de junio de 2015.

[5] Guerra informática en serbia, www.elmundo.es/navegante/99/abril/16/hackers.html. Viernes 16 de abril de 1999.

[6] Acrónimo para dar significado a la organización del tratado del atlántico norte, denominada alianza del atlántico firmado en Washington 4 de febrero del 1949.

[7] Taiwán confirma los ataques informáticos de china continental. www.spanish.rti.org.tw/new/?recordId=9462. 13 de agosto de 2014.

[8] Estonia, primera víctima de los hackers. www.elpais.com/diario/2009/05/30/internacional/1243634402_850215.html, sábado 30 de mayo de 2009.

[9] Stuxnet: el virus capaz de crear el caos absoluto. www.actualidad.rt.com/actualidad/view/111953-stuxnet-virus-iran. 25 de Noviembre de 2013.

[10] Stuxnet: el virus capaz de crear el caos absoluto. www.actualidad.rt.com/actualidad/view/111953-stuxnet-virus-iran. 25 de Noviembre de 2013.

[11] Irán sufre un ataque informático contra sus instalaciones nucleares. www.elpais.com/diario/2010/09/28/internacional/1285624808_850215.html. 28 de septiembre de 2010.

[12] Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Ministerio de defensa española. Instituto español de estudios estratégicos. Febrero de 2011.

[13] Diario mexicano informa sobre el ataque de china a un periódico de los Estados Unidos www.eluniversal.com.mx/notas/899692.html.

[14] Que es operación aurora. www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora. 21 de enero de 2010.

[15] Empresas detrás del hackeo que freno internet www.radiosantafe.com/2013/03/28/spamhaus-y-cyberbunker-las-empresas-detras-del-hacker-que-freno-a-internet. Marzo 28 de 2013.

[16] Evidencia de tráfico de red www.gizmodo.com/5992652/that-internet-war-apocalyse-is-a-lie. Marzo 27 de 2013.

[17] Hackean servicio de PlayStation Network de Sony www.forbes.com.mx/hackean-servicio-de-PlayStation-Network-de-Sony/ junio 17 de 2014.

[18] FBI acusa a corea del norte formalmente del Ciberataque a Sony www.internacional.elpais.com/2014/12/19/actualidad/1419009199_719868.html. 19 de Diciembre de 2014.

[19] Corea amenaza a Estados Unidos a raíz del hackeo de Sony www.lanacion.com.ar/1754717-corea-del-norte-amenaza-con-atacar-a-eeuu-a-raiz-del-hackeo-a-sony. Lunes 22 de Diciembre 2014.

[20] Resumen modelo BMIS elaborado por Ing. Juan Carlos Alarcón S, PMP, CISM, 2010.

[21] Ciberseguridad y Ciberdefensa: una aproximación. www.mindefensa.gov.co/irj/go/km/mindefensa/documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20Ciberdefensa.pdf. Octubre 2009.

[22] ISACA Emite un Nuevo Modelo de Negocio Comprensivo para la Seguridad de Información. http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx.

[23] Seguridad integrada como respuesta al Negocio. https://mail.google.com/_/scs/mail-static/_/js/k=gmail.main.es.-ON4d-uxktg.O/m=m_i,t,it/am=PiOaxvzf-4MYZ5Bd-kDF_v33u0uKnX0e_t2bAJKdAPi_2f8D-D-wj76Q/rt=h/d=1/t=zcms/rs=AHGWq9CDmQgzgozaNAqzVVpcxtRj-sBjKA.

[24] Implementaciones de Cobit.https://mail.google.com/_/scs/mail-static/_/js/k=gmail.main.es.-ON4d-uxktg.O/m=m_i,t,it/am=PiOaxvzf-4MYZ5Bd-kDF_v33u0uKnX0e_t2bAJKdAPi_2f8D-D-wj76Q/rt=h/d=1/t=zcms/rs=AHGWq9CDmQgzgozaNAqzVVpcxtRj-sBjKA.

[25] Ciberguerras las batallas del futuro hoy. http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/.

[26] Icontec**.** Gobierno creará la Agencia Nacional de Seguridad Cibernética. http://icontec.org/index.php/ho/noticias-destacadas/1419-gobierno-creara-la-agencia-nacional-de-seguridad-cibernetica.

[27] Ciberdefensa y Ciberseguridad desafíos emergentes para los profesionales de gobierno IT, jeimy J Cano JMC10/11 reglamento isaca.

[28] Colombia es el tercer país de A. Latina que sufre más Ciberataques. http://www.elespectador.com/tecnologia/colombia-el-tercer-pais-de-latina-sufre-mas-ciberataque-articulo-345008.

[29] Los países mejor preparados para resistir un Ciberataque... y los peores. http://www.bbc.com/mundo/noticias/2012/01/120131_ciberataques_paises_mejor_peor_preparados_adz.

Juan Manuel Ruiz González, Ingeniero de sistemas Corporación Unificada Nacional CUN. Soy Aspirante a otorgar el grado de Especialista en seguridad Informática de la Universidad Piloto de Colombia.