MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TRABAJO FINAL INTEGRADOR

TEMA:

CIBERGUERRA

TÍTULO:

LA CIBERGUERRA COMO AMENAZA A LOS SISTEMAS DE DEFENSA INTEGRADOS Y BASADOS EN REDES DEL TEATRO DE OPERACIONES

AUTOR: MAYOR (FAA) SERGIO DAVID MIRANDA

PROFESORA: Dra. LUCÍA ALEJANDRA DESTRO

Año 2014

Resumen

Un teatro de operaciones moderno exige que las decisiones tomadas sean rápidas y precisas, con el fin de mantener el ritmo de batalla y así poder conservar la iniciativa en el combate.

Esto llevó al desarrollo de los sistemas integrados en redes, los cuales permiten manejar información precisa y prácticamente en tiempo real, al mismo tiempo coordinar con los sistemas de armas las acciones y supervisar las operaciones realizadas por estos desde el Puesto Comando.

Por un lado, esta integración permite la coordinación de las fuerzas y el accionar conjunto de los medios logrando sinergia en las acciones que realizan.

Por otra parte, la proliferación de los ataques a través del ciberespacio se tornaron más complejos, al punto que lograron penetrar en las redes más seguras y sustraer información o bien modificarla en beneficio del atacante.

Estos hechos llevan a replantear la seguridad de los enlaces y en las redes de estos sistemas por el tenor de la información que transportan y las consecuencias en el caso de que un atacante vulnere las redes y tome los datos que allí circulan además de inferir cuales serían las medidas a tomar para minimizar estos efectos.

En este trabajo se describen las medidas necesarias para incrementar la capacidad de ciberdefensa en estas redes identificando para ello: la organización necesaria, las vulnerabilidades del sistema como también la formación del personal para integrar la organización.

Palabras clave: ciberguerra – ciberdefensa – redes – sistemas de defensa integrados

TABLA DE CONTENIDO

"Al distinguir las ventajas de las armas de los guerreros, descubrimos que, cualquiera que sea el arma, existe un momento y una situación en la que ésta es apropiada".

Del libro "Los cinco anillos" de Miyamoto Musashi.

INTRODUCCIÓN

En la actualidad, el mundo se ha configurado en un ambiente muy complejo, en parte por los avances tecnológicos que han afectado todos los ámbitos donde se desenvuelven comúnmente las sociedades.

Las fuerzas armadas no son ajenas a estos cambios que han influido fuertemente en ellas, a tal punto que hoy día deben actuar efectivamente en un ámbito más, cuya característica es artificial y virtual. Este nuevo ámbito es el ciberespacio.

Desde que los estados comenzaron a resguardar las actividades de su estructura en el ciberespacio, este cobró la importancia de "objetivo a proteger". Ello quedó manifestado en el ciberataque realizado a Estonia en el año 2007, cuando a través de una acción en el ciberespacio se consiguió inhabilitar gran parte de la estructura estatal.

Si bien antes de este ataque hubo otros incidentes de gran importancia, como la pérdida de control de un satélite inglés en 1999[1] o bien durante la operación Allied Force donde una unidad especial penetró las redes de la OTAN e inclusive del portaviones Nimitz[2], el ataque de Estonia tuvo particular relevancia porque afectó seriamente a todo un país a través del ciberespacio[3], configurándose así un nuevo ámbito donde llevar el combate.

---

[1] Rivolta, Augusto S.; "Las organizaciones militares frente a un nuevo escenario, la guerra informática"; Boletín del Centro Naval; Escuela de Guerra Naval; Nº 819; Buenos aires; Enero/marzo 2008; Pág. 21

[2] Huerta, Pablo; "ciberguerras: las batallas del futuro hoy"; Discovery; recuperado de *http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/*

[3] Rauscher, Karl; "Ciberguerra: es hora de escribir sus reglas"; prueba&Error; recuperado de *http://www.pruebayerror.net/2013/12/ciberguerra-es-hora-de-escribir-sus-reglas/*

Este hecho se vio replicado en Georgia en el año 2008[4] y posteriormente se dió paso al desarrollo de las ciberarmas o virus, como Stuxnet, que afectó a todo el programa nuclear iraní en el año 2010, o Flame diseñado para realizar espionaje y que una vez diseminado en los ordenadores de las instalaciones de interés, copia los archivos y los envía a distintos destinatarios. Asimismo, tiene la capacidad de autocopiarse en otros ordenadores e inclusive cambiar su comportamiento para eludir a los sistemas de protección.

Se cree que este virus fue diseñado y desarrollado en el año 2008 como parte del programa secreto de EE.UU. *"Juegos Olímpicos"*, el cual fue descubierto recién en el año 2012 cuando atacó refinerías en Irán, Sudán, Siria, Arabia Saudita, Egipto y otros países de la zona[5].

Dentro de las nuevas ciberarmas, una en especial le permitió a Israel afectar severamente el programa nuclear de Siria[6]. Esta ciberarma penetró en la red de los sistemas integrados de defensa aérea y manipuló la información presentada en las pantallas de radar[7].

De esta forma, el virus inhabilitó el sistema de defensa sirio y permitió que los aviones de ataque israelíes atacaran las instalaciones y retornaran a sus bases con éxito. Puede decirse entonces, que las acciones de las Fuerzas de Defensa Israelíes demuestran que es imperativo preparar y adecuar los sistemas locales para este tipo de acciones.

Este último hecho es especialmente llamativo ya que las Fuerzas Armadas Argentinas, particularmente la Fuerza Aérea, se encuentra trabajando en un sistema integrado de defensa que estará vinculado con sus elementos a través de redes de comunicaciones.

---

[4] Über, Denken; "Georgia y Rusia en escalada de ciberataques", recuperado de: http://www.uberbin.net/archivos/internet/georgia-y-rusia-en-escalada-de-ciberataques.php

[5] Anón; "EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán", recuperado de: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html

[6] Pérez, Jesús; "Cómo Israel destruyó el programa nuclear sirio". En Guerras Posmodernas. Los conflictos armados en el siglo XXI, recuperado de; *http://www.guerrasposmodernas.com/tag/operacion-huerto/*

[7] Anón.; "Report: Israel 'blinded' Syrian radar"; ynetnews; recuperado de *http://www.ynetnews.com/articles/0,7340,L-3456456,00.html*.

Teniendo en cuenta el futuro desarrollo de un sistema integrado y conjunto de defensa aeroespacial cabe preguntarse: ¿qué tipo de medidas son necesarias para repeler o bien minimizar los efectos de la ciberguerra en las redes de este sistema de defensa?

Para responder al interrogante, el objetivo general de este trabajo se concentra en describir las medidas necesarias para incrementar la capacidad de ciberdefensa en estas redes identificando para ello: la organización necesaria, las vulnerabilidades del sistema como también la formación del personal para integrar la organización.

En lo que respecta a la organización del trabajo, este se encuentra estructurado en dos capítulos. En el primer capítulo se desarrolla un breve marco introductorio tomando para ello un ejemplo que ilustra los efectos que ocasiona esta nueva amenaza, se definen conceptos clave sobre la temática y luego se profundiza sobre las fortalezas y debilidades de un sistema de defensa integrado y como esta amenaza puede afectarlo explotando sus vulnerabilidades.

En el segundo capítulo, se exponen los principales factores a tener en cuenta al integrar un sistema de defensa en redes determinando las vulnerabilidades de este sistema, cómo deberían ser fortalecidas y cuál es la organización que puede adoptarse para implementar un sistema de defensa eficiente.

"El arte de la guerra es también el arte del engaño"
Sun Tzu, del libro El arte de la guerra

CAPÍTULO I – CONCEPTOS GENERALES

LOS SISTEMAS DE DEFENSA INTEGRADOS. UN EJEMPLO ILUSTRATIVO SOBRE SU VULNERABILIDAD

En septiembre de 2007, personal calificado sirio trabajaba junto con técnicos norcoreanos en la construcción de la planta nuclear siria, ubicada en la provincia de Dayr az Zawr; toda esta región gozaba de la seguridad y tranquilidad que le brindaban los modernos sistemas integrados de defensa ruso, basado en el sistema de defensa antiaérea TOR-M1, PECHORA-2A y PANTSIR-S1, los cuales conformaban una moderna red de defensa para prevenir ataques aéreos con munición de precisión (Precision Munition Guided – PMG). Estos sistemas recién habían sido incorporados al arsenal sirio, y por su efectividad, también fueron adquiridos por Irán, motivando a que otros países de la región iniciaran tratativas para su adquisición.

Al finalizar la noche del día miércoles 5 de septiembre, una estación de radar ubicada al norte en Tall al-Abuad comenzó a recibir mucha interferencia y unos minutos después fue completamente neutralizada; el moderno sistema de defensa no detectó eco alguno donde apuntar sus armas.

Poco después, el ruido de los motores de los jets de combate quebraron la tranquilidad de la noche sobre la planta en construcción. Los sistemas integrados de defensa no reaccionaron y los primeros misiles aire-tierra comenzaron a hacer estragos en las defensas de las instalaciones; luego fueron las bombas de precisión (PMG) las que terminaron el trabajo de "no dejar nada en pie". Los sistemas de defensa siguieron sin reaccionar, no detectaron a los ocho F-15I "Ra´am" que estaban atacando a la planta nuclear en construcción, ni siquiera a los F-16I "Sufa" que estaban mucho más arriba, brindándoles cobertura aérea.

Sin embargo, estos aviones de combate no son furtivos o invisibles al radar, entonces ¿Porqué no fueron detectados por los sistemas de defensa? Ello puede

explicarse porque en parte esta operación se apoyó básicamente en la cobertura electrónica brindada por una plataforma aérea de guerra electrónica basada en el avión Gulfstream 550 y en la capacidad de autoprotección proporcionada por el sistema ELISRA SPS-2110 instalado en cada avión de combate, que les permitía interferir el único sensor de alerta temprana, cuyos receptores fueron literalmente "quemados" por una combinación de pulsos electrónicos emitidos por el Gulftream 550[8]; pero la penetración de la red de defensa fue realizada por un sistema capaz de introducir un virus informático en la red a través de los sensores o los sistemas de comunicaciones, el cual tiene la capacidad de tomar el control de la información que se maneja en la red, pudiendo introducir/extraer datos como por ejemplo los contactos de radar[9].

Este sistema es similar al sistema SUTER desarrollado por la empresa BAE SYSTEMS, que se estima está en servicio desde el 2006 y que fue usado y probado en Irak y Afganistán[10].

En la actualidad, la mayoría de los sistemas de defensa se encuentran integrados a través de redes de información que vinculan a cada subsistema en unos pocos centros de comando, donde la información colectada por los diversos sensores y sistemas de comunicación es presentada para ilustrar la situación en un área particular donde un comandante debe tomar decisiones.

De esta forma, la integración de sistemas de defensa a través de redes se transforma en un factor multiplicador de fuerzas que reduce tiempos de reacción y a su vez permite obtener información en tiempo real. Esta, que parece ser su fortaleza, se convierte a su vez en su debilidad, ya que el comandante al tener diseminadas sus fuerzas depende sobremanera de estos vínculos que le permiten ordenar movimientos a sus fuerzas y retroalimentar la toma de decisiones para ordenar nuevos movimientos.

---

[8] Anón; "Operación Huerta", recuperado de: http://miblog-shomer.blogspot.com.ar/2006/07/operacin-huerta-destruccin-del-programa.html

[9] Fulghum, David A.; "Why Syria's Air Defenses Failed to Detect Israelis"; Strategy Page; recuperado de: http://www.strategypage.com/militaryforums/512-40367.aspx#startofcomments

[10] Fulghum, David A., Michael A. Dornheim, and William B. Scott.; "Black Surprises". Aviation Week and Space Technology; recuperado de: http://www.aviationnow.com/avnow/noys_story.jsp?id=news/02145p04.xml

Si se tiene en cuenta la velocidad con la que se desarrollan los diferentes eventos en los conflictos actuales, tener la información en tiempo real es una necesidad.

Es en este punto donde actúa esta nueva amenaza que tiene capacidad de penetrar estas redes con variadas intenciones que van desde negar el vínculo de la información, diseminar información falsa o bien tomar la información que ve el oponente sin delatar esta actividad, para inferir sus decisiones y actuar en consecuencia.

A su vez, este nuevo empleo de la tecnología, al igual que una fuerza de submarinos o los medios ofensivos del poder aéreo, es capaz de lograr efectos en todos los niveles (estratégico, operacional y táctico) ya que este tipo de ataques puede afectar la estructura completa de un país (programa nuclear iraní y Estonia en el 2006), monitorear redes de defensa (Kosovo 1999) y penetrar sectores de defensa sin ser descubierto (Operación Huerto 2007, descrita al inicio del Capítulo).

DEFINICIONES CONCEPTUALES REFERIDOS A LOS SISTEMAS DE DEFENSA

El tema a desarrollar es eminentemente técnico y tiene conceptos que son poco conocidos en profundidad, razón por la cual es necesario establecer definiciones para una mejor comprensión acerca de lo investigado.

Redes

Como se planteó en párrafos anteriores, un sistema de defensa se vincula con sus sensores y sistemas de armas a través de redes, por lo tanto, es necesario definir que es una red; según Andrew S. Tanenbaum es:

> *…un conjunto de equipos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios*[11]*…*

[11] Tanenbaum, Andrew S.; *Redes de computadoras*; traducción Guillermo Trujano Mendoza; editorial Pearson Educación; México; 2003; p.3

Esta vinculación entre equipos permite intercambiar información rápidamente y a grandes distancias, o bien asegurar que la misma sea accesible cuando se la requiera. Existen diversos tipos de redes, las cuales pueden ser de comunicaciones, informática o bien las conocidas redes sociales entre otras; las usadas por los sistemas de defensa son redes de comunicaciones con integración de voz datos e imágenes.

La cantidad de integrantes y la jerarquía de estos dentro de la organización determinará el tipo de red que deberá implementarse, la cual puede ser de diversos tipos, como se ejemplifica en el ANEXO 1.

Arquitectura y diseño de redes

Cuando los usuarios o *terminales* de una red son muchos, es necesario realizar una "*tarea de arquitectura y diseño"* en la red de modo que la misma sea más eficiente, en la cual se hará la especificación de sus componentes físicos, organización funcional, procedimientos y formatos de datos que se usarán.

La arquitectura de la misma determinará donde deben ubicarse los principales componentes o nodos de la red y como estarán distribuidas las líneas de comunicaciones, como se especificó en el ANEXO 1; el diseño de la red especificará los detalles de cada parte de los nodos, determinando el tipo de protocolo de comunicación, el software a utilizar y el tipo de seguridad necesaria. Asimismo, para comprobar que esa arquitectura es correcta, debe cumplir con cuatro características básicas[12]:

- Tolerancia a fallos
- Escalabilidad
- Calidad de servicio
- Seguridad

[12] Álvarez, Sara; "*Arquitectura de red";* desarrollo web; recuperado de : http://www.desarrolloweb.com/articulos/arquitectura-red.html

Protocolos de comunicación

La interconexión de los equipos debe tener un código o lenguaje común para poder compartir y descifrar la información que se envía, es decir un protocolo de comunicación. Esto es definido por Licesio J. Rodriguez-Aragón como: *…conjunto concreto de normas y reglas de transmisión que permiten ponerse de acuerdo a los equipos de comunicación en cómo debe realizarse la comunicación a través de un canal determinado*[13].

Este lenguaje permite abrir las comunicaciones dentro del sistema e intercambiar los datos entre los usuarios de la red. Constituye la primera medida de seguridad ya que si alguien intenta vincularse a la red sin el mismo protocolo, no podrá acceder a la misma. De esta forma comienza a restringirse la accesibilidad a la red para aquellos usuarios ajenos a la misma.

Sistema integrado de defensa

Un sistema integrado de defensa es un sistema compuesto por sensores activos y pasivos que permiten mantener la vigilancia y control de una determinada área y que ante la detección de una intrusión u amenaza permite la respuesta de uno o más sistemas de armas, en forma coordinada, para repeler la penetración del sector defendido.

Este sistema está compuesto por sensores de superficie (terrestres y marítimos) y aéreos, al igual que los sistemas de armas, para dar una respuesta activa. Están vinculados a través de redes de comunicaciones cuyo tamaño será directamente proporcional al área de responsabilidad. La información obtenida es procesada y presentada en centros de comando y control, donde se deciden las acciones a seguir y qué sistema de armas la ejecutará.

En resumen, se puede definir a un sistema integrado de defensa como la conjugación de sensores y sistemas de armas vinculados, a través de redes de

---

[13] Rodríguez-Aragón, Licesio J.; "*internet y teleinformática"*; clase de informática básica, Departamento de informática, estadística y telemática, Universidad Rey Juan Carlos; recuperado de: http://www.uclm.es/profesorado/licesio/Docencia/IB/IBTema4.pdf; diapositiva 3

comunicaciones, a un centro de comando y control único, con el fin de coordinar la respuesta más eficiente ante un estímulo externo.

Como se dijo al principio, es necesaria la disposición de varios sensores que cubran diferentes sectores del área de responsabilidad para lograr la vigilancia y control de una determinada área.

A su vez es necesaria la interoperabilidad de los sensores de las fuerzas armadas para que estos puedan enviar los datos colectados en tiempo real al centro de información y control (que todos utilicen el mismo protocolo de envío de datos), permitiendo construir una imagen más detallada de la situación en el aérea de responsabilidad; por ejemplo: los buques y los aviones de exploración de la Armada pueden enviar por enlace de datos (datalink) y a través de un satélite la información obtenida por sus sensores a un centro de información y control (C.I.C.) general donde se integren a los datos enviados por los sensores de la Fuerza Aérea y del Ejercito, estos serán procesados y presentados en la pantalla de información del teatro de Operaciones (TO) para ser visualizados por el comandante del TO.

Con esta información, el comandante podrá tener una visión general y en tiempo real de lo que está sucediendo en su área de responsabilidad.

Integración de datos de los sensores

El sistema, cuando esté en servicio operativo, recibirá información de varios sensores y de distinto tipo (radar, imágenes, firmas electromagnéticas, etc.) para lo cual deberá contarse con un sistema que fusione o integre todos estos datos para ser presentados en la pantalla de información, para lo cual deberá resolver cuál es la representación más conveniente para los datos de cada tipo de sensor o bien si son datos de un mismo tipo de sensor comparar los datos obtenidos y presentarlos filtrando aquellos contactos que son obtenidos por dos o más sensores al mismo tiempo.

Para lograr este resultado se deben aplicar varios niveles de fusión de datos[14], donde se aplican complejos algoritmos matemáticos para obtener un dato a representar en la pantalla; estos procesos son detallados en el ANEXO 2.

Ciberguerra

Este es un concepto que en la actualidad se ha hecho conocido pero poco entendido a la vez; mucho se habla de ciberguerra debido a las noticias en los medios de comunicación pero comúnmente no se sabe de qué se trata en realidad.

Las acciones de la ciberguerra pueden influir drásticamente en las actividades que se realizan diariamente y su peligrosidad es directamente proporcional a la dependencia que se tiene de la tecnología, ya que hoy día la mayoría de los servicios básicos (servicio de agua, gas natural, electricidad, medios de información, etc.) de una ciudad están controlados por computadoras y se manejan a través de una red de comunicaciones.

En el caso de un país poco desarrollado que no tenga su estructura básica tecnificada, no podrá ser afectado por las acciones de la ciberguerra. Con otras palabras: todo sistema que sea controlado a través de un software es vulnerable a las acciones de la ciberguerra[15].

El gobierno de los EE.UU. en su documento *The National Strategy to Secure Cyberspace*, deja claramente establecido que:

> *…existe un espectro de actores maliciosos que pueden y llevan a cabo ataques contra nuestras infraestructuras de información críticas. Una de las principales preocupaciones es la amenaza de ataques cibernéticos organizados capaces de ocasionar una interrupción debilitante a la infraestructura crítica, a la economía o a la seguridad nacional de nuestro país*[16].

En este documento se refleja claramente la significancia de la ciberguerra como amenaza hoy día para un país altamente desarrollado.

---

[14] Hall, David L. y LLinas, James; "Handbook of multisensor data fusion"; CRC Press; 2001; Pág 18

[15] Alford, Lionel D.; *Cyber Warfare: A New Doctrine and Taxonomy*; CROSSTALK The Journal of Defense Software Engineering, recuperado de: http://www.crosstalkonline.org/storage/issue-archives/2001/200104/200104-Alford.pdf

[16] White house; *The National Strategy to Secure Cyberspace*; traducción del autor; Washington; Febrero 2003; Pág. VIII

Al igual que los servicios básicos, los sistemas de defensa están conectados en redes para permitir el intercambio de información y poder minimizar tiempos de toma de decisión y respuesta ante una amenaza.

Estás redes, si bien cuentan con seguridad para evitar ser afectadas por terceros de forma accidental o intencionalmente, no siempre es suficiente. A través de las redes se maneja desde información almacenada en bases de datos hasta impartimiento de órdenes de acción para los sistemas de armas del país; estas no son cerradas o aisladas y están controladas por programas o software diseñados para tal fín, por lo tanto son vulnerables a la acción de la ciberguerra.

En definitiva, ¿qué es la ciberguerra? Para responder a este interrogante se hace referencia a una definición dada por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), principal centro docente militar conjunto de las Fuerzas Armadas Españolas, el cual define a la Ciberguerra como: *…el uso de las capacidades basadas en la red de un estado para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores o los propios ordenadores y redes de otro estado*[17].

Antecedentes de la Ciberguerra

La ciberguerra no es algo nuevo, pero ha tomado gran relevancia en estos tiempos debido a que su accionar se ha intensificado. Prueba de ello es la importancia que le confieren los estados en la instalación y desarrollo de organismos de *ciberdefensa,* con el fin de protegerse de los efectos que ocasiona este nuevo uso de la tecnología.

El desarrollo tecnológico sumado al amplio uso de las computadoras en todos los ámbitos de la estructura estatal y organismos privados (fuerzas armadas, servicios públicos, ministerios, etc.) han propiciado la propagación de estas acciones que persiguen variado fines, desde el simple desafío de penetrar una red hasta el espionaje y/o sabotaje.

---

[17] Prieto Osés, Ramón, Hernández Mosquera, Alejandro y otros; *Guerra Cibernética: Aspectos Organizativos*; XXXIII CURSO DE DEFENSA NACIONAL – CESEDEN; 2013; Pág. 4, recuperado de:http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Hoy día la dependencia de internet es elevada y está demostrado en la cantidad de actividades que se realizan en el ciberespacio tales como enviar un simple mensaje, pagar impuestos o comprar y vender productos.

El inicio de la ciberguerra está dado por el desarrollo de internet, cuyo origen es una intranet de ordenadores desarrollada en el año 1969[18] por DARPA (Defense Advance Research Project Agency) comercializada en el año 1982, cuando Vinton Cerf, creador del protocolo TCP/IP, dejó esa Agencia y comenzó a trabajar en una empresa de comunicaciones implementando lo que luego fue internet[19].

Esta red fue creciendo rápidamente hasta alcanzar una conexión de tipo global, donde algunos países comenzaron a visualizar las ventajas de su uso.

En este contexto se produjo lo que puede considerarse el primer ciberataque que tuvo lugar en Junio de 1982 cuando la C.I.A. detectó un intento de la Unión Soviética (U.R.S.S.) de robar un software para controlar su oleoducto transiberiano, el cual era un complejo sistema de bombas, válvulas y sistemas de control.

Por su parte, la C.I.A. alteró el software y permitió que la URSS lo robara y lo instalara en sus controladores, provocando una gran explosión del oleoducto reduciéndolo a cenizas[20]. Desde esa fecha en adelante comenzaron a ocurrir diferentes hechos, algunos públicos (y otros no), demostrando que la ciberguerra se consolidaba como una amenaza real, llegando inclusive a afectar a países completos, como el caso de Estonia en 2007.

---

[18] Rowen, Beth; Cyberwar Timeline-The roots of this increasingly menacing challenge facing nations and businesses; recuperado de: http://www.infoplease.com/world/events/cyberwar-timeline.html

[19] Clayton, Mark; Cyberwar timeline-Tracing the history of cyberespionage and cyberwarfare from the invention of the Internet up to the targeted attacks on US banks by an Islamic hacktivist group; 2011; recuperado de: http://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline

[20] Stephens, Bret; Los limites de Stuxnet; 2011; recuperado de: http://soysionista.blogspot.com.ar/2011/01/los-limites-de-stuxnet.html

"...debemos conseguir: básicamente un fuerza conjunta, conectada en red y geográficamente distribuida, capaz de obtener la superioridad a través de una decisión rápida y la concentración de efectos a través del campo de batalla. Desarrollar esta capacidad requerirá la transformación de nuestro personal, de nuestros procedimientos y unidades militares..."

Donald Rumsfeld, Secretario de Defensa EUA
("Transformation Planning Guidance", Abril 2003)

CAPÍTULO II - FORTALEZAS Y DEBILIDADES DE UN SISTEMA INTEGRADO DE DEFENSA BASADO EN REDES

FORTALEZAS DEL SISTEMA DE DEFENSA INTEGRADO EN REDES

Un sistema de defensa es la conjugación de sensores y sistemas de armas que funcionan vinculados a través de redes de comunicaciones ; estas redes pueden ser físicas o inalámbricas según a la distancia a la que se encuentren cada una de sus partes constitutivas.

El hecho de que el sistema pueda hacer funcionar de forma coordinada a los sensores que detectan a la amenaza y a su vez enviar órdenes por las mismas redes a los sistemas de armas para que repelan esa acción, constituye una fortaleza de estos sistemas ya que permite que un solo comandante concentre toda la información en su puesto de comando y desde allí pueda tomar la decisión y dar la orden que considere necesaria.

Un sistema de defensa integrado a través de redes otorga una ventaja ya que permite lograr una mayor dispersión de las fuerzas militares pero sin que esto comprometa el flujo de información que reciben como el que pueden enviar a los centros de comando. A su vez, esta conexión posibilita coordinar el accionar de todas estas fuerzas[21] para obtener una sinergia y así actuar en tiempo real y a su vez economizar medios.

La implementación de este tipo de sistemas de defensa produce una mayor velocidad de Comando, mejor ritmo de operación, mayor letalidad, aumento de capacidad de supervivencia y auto-sincronización[22].

---

[21] Reigert, Claudio; *defensa basada en redes y su aplicación en el teatro de operaciones*; Trabajo Final Integrador de la Especialización en Estrategia Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta; 2011; Pág. 6.
[22] Ibíd.

A través de los sistemas de este tipo lo que se consigue es concentrar los efectos a través de la coordinación, velocidad y precisión[23] produciendo un mejor aprovechamiento de los medios. La velocidad de transmisión de información permite al comandante retener la iniciativa en las acciones de combate manteniendo un ciclo OODA[24] elevado con respecto al adversario.

La implementación de estos sistemas ha llevado el conflicto a un nuevo plano, el de la información, ya que el manejo de esta permite tener ventaja sobre el adversario sobre todo si se puede manipular la información que este recibe.

Esto ha sido bien comprendido por otros países y han obrado en consecuencia creando organismos que aseguren las redes de los sistemas de defensa nacionales. Como ejemplo, la Fuerza Aérea de los EE.UU. modificó su misión, actualizándola según sus necesidades operacionales:

…*La misión de la Fuerza Aérea de Estados Unidos es proporcionar opciones soberanas para la defensa de Estados Unidos de América y sus intereses globales—para volar y combatir en el aire, en el espacio y en el ciberespacio*[25].

Por lo tanto, se puede decir que si bien el integrar los sistemas de defensa en una gran red y transformarlo en uno solo ofrece múltiples ventajas operativas, la mayor de todas es que esto es un multiplicador de fuerzas, debido a la sinergia que se logra al conseguir que todos actúen de forma coordinada y maximizando las capacidades de todos los componentes (sensores y sistemas de armas).

DEBILIDADES DE UN SISTEMA INTEGRADO EN REDES

Debido a que este tipo de sistemas es la integración de otros sistemas es necesario que estos se comuniquen entre sí para poder intercambiar información. Generalmente, cuando los equipos son de la misma fuerza armada no hay

---

[23] Ibíd; Pág. 7.
[24] Ciclo OODA: ciclo desarrollado por el Coronel John Boyd para la toma de decisiones que consiste en la Observación, Orientación de la acción, Decisión y Acción para luego comenzar otra vez (O.O.D.A. Loop). Mientras se realice el ciclo más rápido que el adversario, siempre se mantendrá la iniciativa.
[25] Umphress, David; *el ciberespacio: ¿un aire y un espacio nuevo?*; *Air & Space Power Journal* - Español Tercer Trimestre 2007; recuperado de: http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2007/3tri07/umphress.html

inconveniente. El problema radica cuando deben integrarse sensores y sistemas de armas de otras fuerzas armadas e inclusive, de otros países.

De aquí que un sistema de defensa integrado en redes es altamente dependiente de la interoperabilidad de sus componentes (sensores, sistemas de armas, comunicaciones, software, etc.)[26] ya que la conectividad entre estos es donde radica la fuerza en los sistemas en red, además es lo que le permite realizar un mejor gerenciamiento de la información.

Como el cúmulo de información a enviar es elevado, los canales de comunicación deberán contar con anchos de banda adecuados que le permitan realizar tráficos de mucha información a alta velocidad. Esto constituye una debilidad en tanto si se restringe de alguna forma el ancho de banda, se está limitando indirectamente la cantidad de información y la capacidad de respuesta de todo el sistema. Ello implica que las redes deben diseñarse en forma redundante y con la duplicidad necesaria para asegurar su confiabilidad.

Para materializar esta red de defensa es necesario también un lenguaje común entre todos los sistemas, el cual está dado por el software que utilizan para vincularse entre sí. Generalmente, estos programas no son desarrollos propios sino que son hechos por empresas especializadas lo que obliga a los usuarios a comprometerse en todas las etapas de este desarrollo para evitar que se les introduzca una subrutina que genere un efecto adverso, o bien retransmita copia de la información recibida a otra terminal, vulnerando la seguridad de todo el sistema[27].

En la descripción de las fortalezas del sistema se aclaró que los canales pueden ser físicos e inalámbricos; estos canales pueden ser vulnerados y su debilidad radica en el tipo de enlace.

Un enlace físico es más difícil de vulnerar ya que para penetrar un canal hay que hacerlo a través de un nodo donde confluyan las demás líneas y conectar la línea allí, o bien se debe "pinchar" la línea para introducir o extraer datos. Esto obligará a

[26] Reigert, C; Óp. Cit. 21; Pág. 14
[27] Ibíd.; Pág. 16

quien diseña las líneas a protegerlas e inclusive esconderlas para dificultar su hallazgo.

Existen cableados de alto nivel de seguridad que se utilizan para configurar redes de instalaciones militares, están diseñadas para impedir la infiltración y el monitoreo de la red; consiste en un sistema de tubos herméticamente sellados, en el interior de estos circula aire a presión y el cable. A lo largo de toda la tubería hay sensores que disparan una alarma ante cualquier presión en la tubería[28].

Estas líneas son muy costosas y muchas veces no pueden utilizarse para toda la red debido a la distancia a la que se encuentran emplazados los sensores y los centros de comando.

Si el sistema se configura con líneas físicas, generalmente se utilizan las líneas de los sistemas de comunicación territorial, compuestos por los tendidos de líneas telefónicas; estas generalmente pertenecen a empresas privadas por lo tanto deben acordarse canales privados y con un ancho de banda específico y encriptado para la seguridad de la información.

En cuanto las líneas inalámbricas, no necesitan un canal físico, la información es transmitida al aire para ser captada por las antenas de recepción los componentes que integran el sistema. Este tipo de enlace es más fácil de vulnerar si se dispone de la tecnología para interferirlos.

Para evitar su vulneración, las frecuencias que llevan la señal con la información poseen protecciones del tipo de salto aleatorio de frecuencias e información codificada, de forma tal que sea muy difícil sintonizar la frecuencia y en caso de poder hacerlo la información captada estará codificada.

La información que recibe el comandante proviene de varios sensores y debe ser decodificada y procesada antes de ser presentada. Esta información proviene de distinto tipo de sensores tales como radares fijos, satélites de imágenes, vehículos no

[28] Borghello, Cristian Fabián; *Seguridad informática sus implicancias y su implementación*; Tesis de licenciatura en sistemas – Universidad tecnológica Nacional; 2001; Pág. 21

tripulados (UAV) y medios de combate en operaciones (aviones, buques, helicópteros, etc.).

Debido a que los sensores no envían el mismo tipo de información (imágenes, video, datos radar, datos meteorológicos, etc.) se le debe dar un formato para ser presentada de forma tal que permita obtener una idea general del teatro de operaciones.

Esto es realizado por los integradores de señal que reciben los datos que además corroboran que no se repitan y los presentan en el formato que solicite el operador, al momento de mostrarlos en un panel de situación general.

Este proceso se logra a través de distintos pasos y algoritmos de procesamiento (mencionados en el Capítulo I - integración de datos de los sensores) los cuales se realizan con software y computadoras con una elevada velocidad de procesamiento de datos. En el caso de que pueda manipularse la información en esta etapa, todo dato que se le presente a un comandante estará comprometido.

Un punto a tener en cuenta aquí es que un comandante en operaciones siempre necesita información precisa y en tiempo real, pero el hecho de contar con demasiados datos al mismo tiempo puede producir un efecto contrario y dejar al comandante paralizado y sin poder tomar una decisión acorde a la situación que está viviendo. Por lo tanto, es importante tener en cuenta qué información se debe presentar y en qué grado debe hacerse[29].

Como corolario, las debilidades de un sistema de defensa integrado en redes está dado por la interoperabilidad de sus componentes, el ancho de banda disponible, el tipo de software que se utiliza para manejar la información, el tipo de enlace usado para transportar la información y por el sistema de integración de datos de los sensores.

[29] Reigert, C; Óp. Cit. 2; Pág. 17

Debilidades explotadas por la ciberguerra

Luego de la descripción de las fortalezas y debilidades de un sistema de defensa integrado en redes, se aprecia que a la luz de la ciberguerra este sistema posee una puerta de entrada en los canales que llevan la información y que a su vez tiene un ámbito donde realizar sus acciones, materializado en el software que controla a los sensores, el tráfico de información o bien la alteración del proceso de integración de la información recibida por los sensores.

La característica de este tipo de ataque es que el mismo es subrepticio, los procesos que realizan los atacantes para robar, modificar o espiar la información son transparentes al sistema y a los operadores. Estos sólo son detectados a través de sistemas de seguridad dedicados al análisis de los usuarios que acceden al sistema.

Este tipo de acciones es llevado adelante por un *intruso* o *atacante*, denominándose así a quien accede o intenta acceder a un sistema sin autorización, de forma intencionada o no. Estos pueden ser clasificados desde el punto de vista de capacidades y conocimientos, ordenados de la siguiente forma[30]:

- Clase A[31]: constituyen el 80% de la población total, son grupos que están experimentando software adquirido o bien desarrollados por ellos. Realizan esta actividad como un desafío.
- Clase B[32]: constituido por el 12%, son más peligrosos debido a que tienen la capacidad de compilar programas, pueden reconocer los sistemas operativos que está usando la víctima y pueden testear sistemáticamente sus vulnerabilidades para acceder al sistema.
- Clase C[33]: constituido por el 5%, compuesto por operadores que saben programar y conocen los sistemas operativos y sus vulnerabilidades, actúan con objetivos específicos y pueden realizar accesos remotos a los sistemas.

[30] Borghello, C.; Óp. Cit. 28; Pág. 11
[31] Ibíd.
[32] Ibíd.; Pág. 12
[33] Ibíd.

- Clase D[34]: constituido por el 3% restante de la población, acceden a sistemas complejos. Mantienen el anonimato para mantener las líneas abiertas, buscan información específica.

Estos ataques se dedican en primera medida a una exploración sistemática de posibles vulnerabilidades en la red para poder acceder al sistema y luego de que consiguen acceder comienzan a explorar todo el sistema con distintos fines, desde la búsqueda de información precisa, instalar programas maliciosos, o bien recorrer el sistema para conocerlo en su totalidad.

El negar el acceso a un sistema integrado de defensa es una prioridad ya que este puede constituirse a su vez en la entrada a sistemas del nivel militar y nacional; tal como fue el caso en 1999 donde el acceso a la red de defensa del portaviones USS NIMITZ permitió acceder a las bases de datos de OTAN, *...el Capitán Dragan Vasiljković, uno de los lugartenientes de Milosevic, al mando de una unidad de guerra digital, hizo colapsar momentáneamente las computadoras de distintas unidades de la OTAN y del portaaviones norteamericano Nimitz*[35].

Por lo tanto, el alcance que tenga un ciberataque estará dado por los niveles a los que esté conectada la red afectada.

Técnicas empleadas por la ciberguerra

Antes de avanzar sobre este tema es necesario hacer una diferenciación importante y que ayudará a comprender mejor los conceptos que se enunciarán a continuación.

En el escenario virtual de batalla que es el ciberespacio se pueden diferenciar ejércitos, armas y tácticas de combate.

Los ejércitos están compuestos por computadoras que integran una red robot o *botnet;* estas redes se forman luego de infectar miles de ordenadores con software malicioso del tipo *troyano* o *malware bot*,(se detalla más adelante) que permite que

[34] Ibíd.
[35] Sifuentes, Marco; *Breve diario de la ciberguerra fría III*; recuperado de: http://larepublica.pe/blogs/pasado/category/ciberguerra/

quien lo ha diseñado tome el control de la computadora en un segundo plano, sin que el dueño pueda percibirlo[36].

Una *botnet* es una red de equipos infectados por códigos maliciosos que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida.

Cuando una computadora ha sido afectada por un malware de este tipo, se dice que ese equipo es un robot o zombi[37].

Las armas utilizadas en estas batallas son las variantes del denominado *software malicioso o malware,* del cual existen diversas variantes pero las más comunes son las que se detallan en el ANEXO 3.

Estas ciberarmas, son empleadas generalmente por unos pocos atacantes y solo en algunas técnicas se utilizan las *botnet* tratando de generar efectos de saturación sobre la víctima. El resto de las técnicas busca otro tipos de efectos que van desde espiar y copiar información hasta dejar inoperativo el sistema.

Las técnicas empleadas en los ciberataques son detalladas en el ANEXO 3.

Efectos de la ciberguerra en un sistema de defensa integrado en redes

Dado el caso de que un atacante penetre en la red de defensa de un sistema integrado, este podría causar efectos en todo el sistema y si no se cuenta con las herramientas apropiadas para su detección, no se podrá saber que se está siendo atacado.

Una de las características de estos ataques es ser subrepticio y a su vez mantener el anonimato de quien lo realiza; de esta forma se puede mantener la influencia dentro del sistema sin que la víctima pueda defenderse.

Entre los efectos que podría generar un ataque de este tipo en un sistema se encuentra la manipulación de las bases de datos. Dicha manipulación podrá generar

---

[36] Martós, José Ángel; *¡Esto es la ciberguerra!*; Muy interesante; 2008; recuperado de: http://www.muyinteresante.es/tecnologia/articulo/iesto-es-la-ciberguerra

[37] Rivero, Marcelo; *¿Qué son los malwares?*; Infospyware; 2013; recuperado de: http://www.infospyware.com/articulos/que-son-los-malwares/

una *fricción virtual* haciéndole creer al comandante o al personal que opere ese sistema, que los datos que están viendo son verdaderos. Por ejemplo: en la base de datos del estado de aeronaves de transporte que están en servicio, el atacante podría manipular la numérica de estos aviones y esto produciría cambios en la planificación e inclusive confusión entre el personal, aumentando en consecuencia la fricción en las operaciones.

Se podría generar engaño a través de la información que obtienen los radares, manipulando la cantidad de ecos presentados, incrementándolos o bien *borrándolos* según le convenga a quien está atacando o bien introducir imágenes falsas de inteligencia en el sistema, entre otras cosas.

Todas estas acciones, si bien son realizables, podrían delatar que el sistema está siendo manipulado. Por lo tanto, es muy probable que quien lo haga solo realice monitoreo y robo de la información para no delatar su presencia pudiendo, en caso de ser descubierto, encriptar toda la información contenida en los servidores. Esto inutilizaría todo el sistema.

FACTORES IMPORTANTES A TENER EN CUENTA PARA LA SEGURIDAD INFORMÁTICA

Luego de describir los efectos de la ciberguerra en un sistema de defensa integrado en redes, se explicitará cuáles son los recaudos que se deben adoptar para minimizar su accionar.

Al diseñar una red generalmente se dedica mucho esfuerzo en su funcionalidad-operatividad pero no se aborda seriamente su seguridad. En una red de este tipo deberá diseñarse primero su seguridad y esta será el basamento de lo demás de forma tal de integrarla desde el desarrollo mismo y que no sea algo que se "*agrega"* después para cumplir regulaciones estipuladas[38].

Esto debe ser así ya que existe una relación indirectamente proporcional entre la seguridad y la operatividad de la red[39]. Para que la red sea segura debe ser cerrada

[38] Borghello, C.; Óp. Cit. 28; Pág. 217
[39] Ibíd.; Pág. 14.

y mientras más cerrada esta sea será más segura, pero su operatividad será nula porque estará aislada de sus componentes externos. Esta es la relación de compromiso que se debe evaluar y sobre la cual se debe establecer la seguridad de sus canales de comunicación.

Además, se debe tener en cuenta que la seguridad informática es como un problema militar operativo (PMO) en el cual se está enfrentando a una oposición inteligente que evoluciona sobre la base de las reacciones planteadas a sus acciones, es decir que esto constituye un problema sin fin, solo tiene soluciones temporales y que ninguna es infalible.

En este sentido, el objetivo de la seguridad informática es: *…mantener la disponibilidad, integridad, privacidad (sus aspectos fundamentales), control y autenticidad de la información manejada por computadoras*[40].

De aquí se deduce que el bien a proteger es la información y para protegerla, la política y procedimientos deben estar en condiciones de analizar las posibles amenazas en tres momentos, antes, durante y después del ataque al sistema. Para esto se deberán adoptar tres mecanismos que garantizarán la seguridad de la red[41]:

- La prevención (antes): compuesta por procedimientos y protocolos que mantienen alto el nivel de seguridad, como puede ser control de accesos, autenticidad o cifrado de datos para su transmisión.

- La detección (durante): vigilancia permanente de la red y del tráfico en la misma para detectar cualquier intento de penetración no autorizado.

- La recuperación (después): tener la capacidad de rechazar el ataque y restaurar el sistema a su funcionamiento normal, en caso de ser necesario cargando los backups del mismo.

Es necesario tener en cuenta de que luego de un ataque se deben replantear las defensas y probarlas exhaustivamente ya que el evento rechazado no soluciona el problema, solo lo retrasa y transforma, ya que la oposición es inteligente y aprende

---

[40] Aldegani, Gustavo Miguel; *Seguridad Informática*; MP ediciones; Argentina; 1997; Pág. 22
[41] Borghello, C.; Óp. Cit. 28; Pág. 9

de sus errores por lo tanto las incógnitas sobre las que debe plantearse la defensa serían[42]:

- ¿Cuánto tardaría la amenaza en superar las propias defensas?
- ¿Cómo se la puede detectar e identificar a tiempo?
- ¿Cómo se hace para neutralizarla?

Otros elementos a considerar en el diseño de la seguridad de la red son generar defensas fuertes para disuadir/minimizar la posible ocurrencia de un ataque; en caso de no poder evitarse, generar control de daños para reducir los perjuicios a la información, diseñar procedimientos de rápida recuperación y duplicación de canales de comunicación, asimismo la corrección de las medidas de seguridad sobre la base de la experiencia recogida[43].

Unidades de seguridad informática – equipo de respuesta ante emergencias informáticas (CERT - Computer Emergency Response Team)

La seguridad de la información que se transmite en las redes es compleja y debe ser llevada a cabo en forma permanente, de aquí que deben organizarse equipos dedicados a esta función y que tengan la capacidad de proteger y rechazar todo intento de ataque a la red, como así también la capacidad de recuperar el sistema si no se pudo detener el ataque; también debe tener la capacidad de aprender de los ataques y evolucionar su defensa para estar preparados ante un nuevo intento.

El Ministerio de Defensa de España, en su guía de seguridad (ccn-stic-810) - Guía de creación de un CERT / CSIRT de septiembre de 2011 dice:

> *...El panorama descrito* [la amenaza de la ciberguerra[44]] *obliga a las organizaciones, bien sean públicas o privadas, a realizar un esfuerzo adicional en preservar la seguridad de sus sistemas y responder a estos nuevos riesgos e incidentes. Una preservación que requiere de una política de seguridad integral y especialmente del desarrollo de unos servicios y capacidades operativas específicas en materia de operación y respuesta ante incidentes de seguridad.*

[42] Ibíd.
[43] Ibíd.; Pág. 10.
[44] La aclaración pertenece al autor.

> *De este modo, en los últimos años, se han venido desarrollando estructuras orientadas a la operación y gestión de incidentes de seguridad, llamados CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incidente Response Team), como solución más adecuada para dar una respuesta eficaz y eficiente a estos nuevos riesgos.*[45]

Debido a la especificidad de las tareas que este equipo debe realizar y los problemas e inconvenientes que debe afrontar y solucionar, el mismo debe ser dirigido por expertos en seguridad informática y resolución de problemas[46].

Asimismo, deben desarrollar procedimientos para el control y la recuperación rápida de incidentes, determinación del sector/sectores donde recaerá la responsabilidad de la seguridad, la identificación de las herramientas y procedimientos adecuados para la seguridad, mantener la investigación y desarrollo para perfeccionar las herramientas de seguridad informática, generar conciencia y capacitación dentro de la organización, investigación de ataques, software y procedimientos utilizados para contrarrestarlos[47].

El hecho de contar con un organismo de este tipo dentro del sistema permite repeler los ingresos no autorizados o en el caso de que tengan éxito en su acometida, minimizar los efectos de sus acciones permitiendo contar con un plan de recuperación rápida para que el sistema siga funcionando.

Trasladando esto a un sistema de defensa integrado en redes deberá existir un centro donde se recibirá toda la información, a su vez se conformarán sub centros que constituirán nodos donde confluirá la información enviada por los sensores más cercanos a cada uno de ellos. El problema se plantea dónde ubicar el CERT para plantear una mejor defensa, o si debe ser uno solo o varios.

Sensores, nodos y centro de información estarán separados por mucha distancia entre sí por lo cual serán altamente dependientes de sus enlaces, lo que los hace vulnerables a un corte/interferencia en los mismos.

---

[45] Ministerio de Defensa del Reino de España, Centro Criptológico Nacional; *Guía de creación de un CERT / CSIRT*; guía de seguridad (ccn-stic-810); 2011; Párr. 2-3, Pág. 6.
[46] Borghello, C.; Óp. Cit. 28; Pág. 285.
[47] Ibíd.; Pág. 209.

Si se diseñara un único CERT para la defensa de las redes del sistema y se ubicara en el centro de información, se reducirían los costos en cuanto a personal y equipos pero indirectamente se incrementaría la probabilidad de que este quede aislado de sus nodos sin poder restablecer los enlaces y recuperar el sistema, dejando indefensos, desde el punto de vista informático, a los sensores que dependen de los nodos de comunicación afectados.

Para evitar el aislamiento intencional del CERT, se deberá incrementar los gastos de diseño e instalación para elevar el nivel en la seguridad de líneas de comunicación, duplicándolas para tener alternativas o bien incrementar su resistencia a las interferencias o interrupciones.

Si se diseñaran varios CERT, de los cuales el principal se ubicaría en el centro de información y los dependientes en los nodos de comunicaciones, los costos se incrementarían debido a la cantidad de personal necesaria y los equipos para que puedan defender las redes aunque se aumentaría la probabilidad de evitar un corte en los enlaces de datos y a la vez actuaría como elemento disuasivo.

De esta forma se podría reducir costos en los enlaces y su seguridad, ya que estos no serían tan extensos y los CERT dependientes tendrían un determinado nivel de iniciativa para actuar en caso ser aislado del CERT principal. Asimismo, cabe aclarar que la oposición es inteligente y evoluciona acorde a nuestras acciones por lo tanto esto no es garantía de que se puedan rechazar todos los ataques.

Si bien a nivel mundial se utilizan estos CERT, debería analizarse qué tipo de organización es la que da solución a nuestro problema, teniendo en cuenta los factores como la extensión territorial, geografía, sistemas de comunicaciones disponibles e instalaciones existentes en nuestro país para la instalación de una organización de este tipo, ya que todos estos factores condicionarían el tipo de enlaces a usar en forma segura y se incrementan los costos de diseño e instalación de los mismos.

Otro factor importante y que condicionará la conformación de este tipo de organización es el tipo de formación que deberá tener el personal que la integrará o bien que perfil se le solicitará a los candidatos a trabajar en este equipo, sobre todo por el tiempo de formación y adiestramiento del mismo.

Formación de un nuevo tipo de soldado

El Teniente General Robert J. Elder Jr., Comandante (desde jun 2006 – hasta jul 2009) de la Octava Fuerza Aérea, Comandante del Componente Conjunto para Ataque e Integración Global - Comando Estratégico de EE.UU. (USSTRATCOM) declaró:

> *...El cambio cultural es que vamos a tratar a Internet como un campo de guerra y vamos a concentrarnos en él y darle prioridad para acciones en el ciberespacio y acompañarla, si es necesario, con acciones en el espacio aéreo y terrestre. Vamos a desarrollar, junto con las universidades, guerreros ciberespaciales que sean capaces de reaccionar ante cualquier amenaza las 24 horas del día durante los siete días de la semana*[48].

Luego de conocer las amenazas que debe enfrentar un CERT y las tareas que deberían realizar, fácilmente se puede inferir que los integrantes del mismo que deban conducir las batallas virtuales, deberán ser personal altamente calificado y sus operadores deberán estar debidamente capacitados para estar a la altura de lo que estas nuevas amenazas y la tecnología le demandan.

El personal que lo integra deberá estar en capacidad de analizar las redes del adversario y sus vulnerabilidades, desarrollar y usar software para la detección de intrusos y defensa de las redes, localización de averías y reparación de las mismas, coordinación y dirección de esfuerzos para rechazar un ataque. Al mismo tiempo deberán mantener las capacidades de ingeniería y desarrollo de software para la creación de nuevas armas y herramientas[49].

No son simples *operadores* lo que se necesita para integrar estos equipos, sino que se debe formar un: *…equipo de profesionales de lucha de ciberguerra, cada uno con sus propias responsabilidades y conjunto de habilidades, para establecer, controlar y proyectar poder de combate en y a través del ciberespacio*[50].

Por el ámbito donde deben actuar y por su competencia, este personal deberá tener una preparación eminentemente universitaria, orientada hacia el área de

---

[48] Mexidor, Francis Deisy; Ciberguerra: mercenarismo en la red; Las razones de Cuba; 2011; recuperado de: http://www.granma.cu/granmad/secciones/razones_de_cuba/artic-06.html

[49] Franz, Timothy; *El profesional de la ciberguerra – principios para desarrollar la próxima generación*; Air&space Power Journal en español; primer trimestre 2012; Pág. 42

[50] Ibíd.

informática, redes y criptología para cubrir todas las áreas de la red que integra al sistema de defensa (computadoras, comunicaciones y seguridad de datos).

Estos nuevos soldados pueden estar agrupados en cuatro grandes grupos: operadores de ciberdefensa, técnicos, analistas de ciberdefensa y desarrolladores de armas[51], los cuales pueden formar unidades de operaciones, tanto para el ciberataque como para la ciberdefensa, en capacidad de dar respuesta a las diversas variantes que se planteen en una misión.

Otro punto importante en la formación de los cibersoldados, es la "*cultura de combate de guerra a desarrollar*"[52], según lo dicho por el Teniente Coronel de la USAF Timothy Franz, en su artículo "El profesional de la ciberguerra – principios para desarrollar la próxima generación" ya que:

> *...la mayoría de los profesionales de la ciberguerra actuales provienen de los campos profesionales de comunicaciones e información,* [ellos[53]] *históricamente se han concentrado en mantener las comunicaciones en funcionamiento, no en comprender las misiones apoyadas por cada enlace o nodo* […] *nuestros ciberdefensores necesitan familiarizarse mejor con la gama completa de amenazas hostiles a nuestros sistemas de información y mas habilidades en combatir ataques de tales amenazas. La cultura de los actuales profesionales de la ciberguerra debe evolucionar de una cultura que provee servicios a una que ofrezca un equilibrio de servicio, seguridad y conocimiento de amenazas, todo en nombre de la seguridad de la misión[54].*

Si bien la formación profesional, en cuanto a conocimientos técnicos se refiere, es importante también que estos nuevos tipos de soldados sean formados también con la cultura y los valores que enarbolan las fuerzas armadas a la que pertenecen, ya que estarán inmersos en una guerra virtual todos los días y de ellos dependerá la seguridad de las redes de información e inclusive el mismo comando y control de las mismas operaciones.

---

[51] Franz, T.; Óp. Cit. 49; Pág. 46
[52] Ibíd.; Pág. 49
[53] Nota agregada por el autor
[54] Franz, T.; Óp. Cit. 49; Pág. 49

CONCLUSIONES

La tecnología brinda herramientas con las cuales se puede apoyar la toma de decisiones de un comandante del teatro de operaciones, con datos extraídos por sensores ubicados a cientos de kilómetros de distancia. Esto es posible gracias a la integración de los sistemas de defensa en una red que permite obtener una visión del área de responsabilidad en tiempo real.

Los sistemas de defensa en red actúan como multiplicador de fuerzas, brindándole al comandante herramientas para llevar su esfuerzo a la victoria, con acciones coordinadas y manteniendo la iniciativa en las acciones.

Este sistema actúa como un organismo vivo, en el cual los sensores constituyen los sentidos y sus enlaces son su *sistema nervioso*, por el cual se envía toda la información recibida y sobre la cual se tomarán las decisiones.

Por otro lado, la ciberguerra es una nueva amenaza que ha surgido también por el desarrollo tecnológico de las comunicaciones y que afecta directamente al *sistema nervioso*, penetrando en la red del sistema de defensa de un país. Esta amenaza tiene la capacidad de monitorear, borrar, modificar o negar la información sobre la cual el comandante tomará sus decisiones.

Luego de ver la importancia y las ventajas de conformar una red de defensa, de conocer la vigencia de la ciberguerra y sus efectos en las redes de todo tipo, es innegable la necesidad de conformar un organismo que sirva como barrera a esta nueva amenaza.

Ello obliga a crear unidades especializadas y formar profesionales para luchar y defender estas redes en un ámbito intangible como es el ciberespacio, en el cual será vital obtener la supremacía en las guerras del futuro.

Los países más desarrollados se han concientizado de esto y generaron sus instituciones constituidas en ejércitos virtuales que actúan desde un único centro de comando y control para vigilar y defender sus redes críticas. Su operación centralizada está basada en el desarrollo tecnológico y de comunicaciones de estos

países, que les permite tener redundancia de medios para mantener sus esfuerzos de defensa en ejecución.

El desarrollo tecnológico en Argentina, su extensión territorial e infraestructura de comunicaciones (pública y privada) no permite obtener una redundancia de enlaces para ejercer una defensa de redes de forma centralizada.

Los enlaces que pudieran establecerse para dar forma a esta red de defensa, tal vez no tendría la seguridad necesaria para evitar que alguno de sus nodos sea aislado y/o atacado, de aquí que es necesario que estos cuenten con sus defensas y cierta autonomía para actuar en caso de quedar *desconectados* de la red.

Teniendo en cuenta la importancia de proteger la información que fluye en la red de defensa y que se debe mantener las defensas en el ciberespacio, se intuye que la forma más conveniente de proteger las redes nacionales sería a través de una ejecución descentralizada, materializada en la constitución de un CERT, con la organización más conveniente en cada nodo que centralice información de los sensores más cercanos.

Los equipos de estas unidades deberían ser móviles y tener capacidad de instalarse en donde se configuren o reubiquen los nodos que se deban defender.

Estos nodos estarían coordinados por un CERT principal, que a su vez le permitiría al comandante conducir la ciberguerra, la cual también será su responsabilidad.

Es muy importante que los enlaces tengan todas las medidas de seguridad necesarias para impedir su vulneración. En caso de ser físicas que cumplan con todos las características, desde el punto de vista de seguridad informática, para un enlace de datos de este tipo al igual que los enlaces inalámbricos, los que además deberán contar con el ancho de banda necesario para permitir configurar una red ágil y rápida.

Por lo visto a lo largo del trabajo, el personal que integre estas unidades deberá ser personal calificado y adiestrado ya que su tarea es muy compleja y se debe asegurar el uso de las redes, ya que el comando y control de las fuerzas del comandante está basada en estas redes.

Tanto la implementación de los CERT como la formación del personal que los integrará llevará un tiempo considerable por lo tanto, la planificación que se realice con estos objetivos debe “seguirse de cerca” en su ejecución y con asesoramiento de profesionales con conocimiento en seguridad informática, redes y comunicaciones ya que la defensa de las redes de los sistemas de defensa integrados dependerá de su correcta implementación.

BIBLIOGRAFÍA

- Aldegani, G. M.; *Seguridad Informática*; MP ediciones; Argentina; 1997

- Bazán, G. M. (2010). *Consideraciones para la integración de sensores, para la elaboración de un sistema de control y vigilancia aeroespacial conjunto.* CABA: Escuela Superior de Guerra Conjunta.

- Bogotá Galvis, F. (2012). *De la ciberguerra y el papel de la fuerza aérea colombiana* . Revista Taktika , 47-51.

- Borghello, C. (2001). *Seguridad informática, sus implicancias e implementación.* UTN. Buenos Aires: Universidad Tecnológica Nacional.

- Cobb, J. (2012). *Ejecución centralizada, caos descentralizado: como la fuerza aerea está al borde de perder una ciberguerra*. Air & space power journal , 89-95.

- Franz, T. (2012). *El profesional de la ciberguerra: principios para desarrollar la próxima generación*. Air & space power journal , 42-55.

- Giuduci, D. -C. (2013). *Lineamientos para la seguridad cibernética en un teatro de operaciones.* CABA: Escuela Superior de Guerra Conjunta.

- Halll, D. L. y Llinas, J.; *Handbook of multisensor data fusion*; CRC Press; 2001

- Llambí, E. -C. (2011). *Nuevas tecnologías de información y comunicación (TIC) y su influencia en los teatros de operaciones (TO) modernos.* CABA: Escuela Superior de Guerra Conjunta.

- Ministerio de Defensa del Reino de España, Centro Criptológico Nacional; *Guía de creación de un CERT / CSIRT*; guía de seguridad (ccn-stic-810); 2011

- Ossa Ceballos, E. (2012). *Guerra ciberespacial*. Revista Taktika , 43-46.

- Petit, B. (2003). *Chechen Use of the Internet in the Russo-Chechen Conflict.* Fort Leavenworth, Kansas: Faculty of the U.S. Army Command and General Staff College.

- Puime Maroto, J. (2009). *El ciberespionaje y la ciberseguridad*. En J. Puime Maroto, La violencia del siglo XXI. Nuevas dimensiones de la guerra (págs. 47-76). Reino de España: Centro Superior de Estudios de la Defensa Nacional.

- Reigert, C. -M. (2011). *Defensa basada en redes y su aplicación en el teatro de operaciones.* CABA: Escuela Superior de Guerra Conjunta.

- Riquelme, E. -M. (2012). *La influencia de la guerra de información en un teatro de operaciones.* CABA: Escuela Superior de Guerra Conjunta.

- Rodriguez Cisneros, E. -M. (2012). *Desafíos operacionales en el ciberespacio como nuevo campo de lucha.* CABA: Escuela Superior de Guerra Conjunta.

- Stel, E. (2005). *Guerra cibernética.* Buenos Aires: Circulo Militar.

- Tanenbaum, A. S. (2003). *redes de computadoras.* México: Pearson Educación.

- White House; *The National Strategy to Secure Cyberspace*; Washington; Febrero 2003

SITIOS DE INTERNET VISITADOS

- Alford, Lionel D.; *Cyber Warfare: A New Doctrine and Taxonomy*; CROSSTALK The Journal of Defense Software Engineering, recuperado de: http://www.crosstalkonline.org/storage/issue-archives/2001/200104/200104-Alford.pdf

- Álvarez, Sara; *Arquitectura de red;* desarrollo web; recuperado de : http://www.desarrolloweb.com/articulos/arquitectura-red.html

- Anón; *EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán*, recuperado de: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html

- Anón.;*Operación Huerta*, recuperado de: http://miblog-shomer.blogspot.com.ar/2006/07/operacin-huerta-destruccin-del-programa.html

- Anón.; *Report: Israel 'blinded' Syrian radar*; ynetnews; recuperado de http://www.ynetnews.com/articles/0,7340,L-3456456,00.html.

- Clayton, Mark; Cyberwar timeline-Tracing the history of cyberespionage and cyberwarfare from the invention of the Internet up to the targeted attacks on US banks by an Islamic hacktivist group; 2011; recuperado de: http://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline

- Díaz, Gilberto; *Redes de Computadoras-Introducción*; Arquitectura de Redes; Universidad de Los Andes-Facultad de Ingeniería-Escuela de Sistemas; Mérida, Venezuela; recuperado de: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/04_conceptosBasicos2.pdf

- Fulghum, David A.; *Why Syria's Air Defenses Failed to Detect Israelis*; Strategy Page; recuperado de: http://www.strategypage.com/militaryforums/512-40367.aspx#startofcomments

- Fulghum, David A.; Dornheim, Michael A. and Scott, William B. ; *Black Surprises*. Aviation Week and Space Technology; recuperado de: http://www.aviationnow.com/avnow/noys_story.jsp?id=news/02145p04.xml

- Huerta, Pablo; c*iberguerras: las batallas del futuro hoy*; Discovery; recuperado de http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/

- Martós, José Ángel; *¡Esto es la ciberguerra!*; Muy interesante; 2008; recuperado de: http://www.muyinteresante.es/tecnologia/articulo/iesto-es-la-ciberguerra

- Mcdowell, Mindi; *Understanding Denial-of-Service Attacks;* US-CERT; 2013; recuperado de: https://www.us-cert.gov/ncas/tips/ST04-015

- Pérez, Jesús; *Cómo Israel destruyó el programa nuclear sirio*. En Guerras Posmodernas. Los conflictos armados en el siglo XXI, recuperado de; http://www.guerrasposmodernas.com/tag/operacion-huerto/

- Prieto Osés, Ramón, Hernández Mosquera, Alejandro y otros; *Guerra Cibernética: Aspectos Organizativos*; XXXIII CURSO DE DEFENSA NACIONAL – CESEDEN; 2013; recuperado de: http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

- Rauscher, Karl; *Ciberguerra: es hora de escribir sus reglas*; prueba&Error; recuperado de: http://www.pruebayerror.net/2013/12/ciberguerra-es-hora-de-escribir-sus-reglas/

- Rivero, Marcelo; *¿Qué son los malwares?*; Infospyware; 2013; recuperado de: http://www.infospyware.com/articulos/que-son-los-malwares/

- Rodriguez Aragón, Licesio J.; "*internet y teleinformática"*; clase de informática básica, Departamento de informática, estadística y telemática, Universidad Rey Juan Carlos; recuperado de: http://www.uclm.es/profesorado/licesio/Docencia/IB/IBTema4.pdf

- Rowen, Beth; *Cyberwar Timeline-The roots of this increasingly menacing challenge facing nations and businesses*; recuperado de: http://www.infoplease.com/world/events/cyberwar-timeline.html

- Stephens, Bret; Los limites de Stuxnet; 2011; recuperado de: http://soysionista.blogspot.com.ar/2011/01/los-limites-de-stuxnet.html

- Sifuentes, Marco; *Breve diario de la ciberguerra fría III*; recuperado de: http://larepublica.pe/blogs/pasado/category/ciberguerra/

- Über, Denken; *Georgia y Rusia en escalada de ciberataques*, recuperado de: http://www.uberbin.net/archivos/internet/georgia-y-rusia-en-escalada-de-ciberataques.php

- Umphress, David; *el ciberespacio: ¿un aire y un espacio nuevo?*; *Air & Space Power Journal* - Español Tercer Trimestre 2007; recuperado de: http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2007/3tri07/umphress.html

ANEXO 1

TIPOS DE REDES

Una red informática puede adoptar diferentes formas, según la organización y la función que deba desempeñar. La forma que esta adopte condicionará también la distribución de la información y a su vez servirá para establecer jerarquías dentro de la organización.

Las redes informáticas pueden configurarse de la siguiente forma:

Bus[55]: se implementa un troncal único y todos los nodos se conectan a este, compartiendo el medio y la información

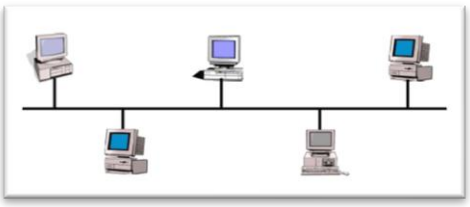

FIGURA 1

Anillo[56]: un nodo se conecta con el más próximo, así sucesivamente hasta que el último se conecta al primero. las terminales no comparten la misma información, se pueden hacer filtros sobre los datos que se dejan pasar al terminal siguiente.

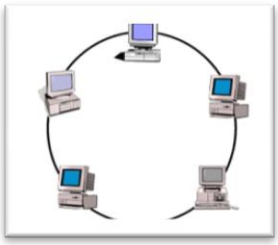

FIGURA 2

Estrella[57]: todos los nodos se conectan a un switch central, que gerencia y administra el orden del tráfico de la información. Todos pueden compartir la información pero al mismo tiempo una de las terminales puede ejercer la administración de la red y acceder a todas las terminales.

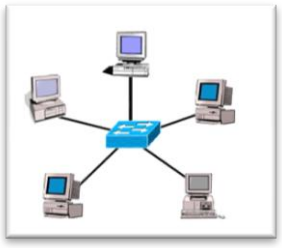

FIGURA 3

---

[55] Díaz, Gilberto; *"Redes de Computadoras-Introducción"*; Arquitectura de Redes; Universidad de Los Andes-Facultad de Ingeniería-Escuela de Sistemas; Mérida, Venezuela; recuperado de: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/04_conceptosBasicos2.pdf ; diapositiva 11.
[56] Ibíd. 12; diapositiva 12
[57] Ibíd. 12, diapositiva 13

Estrella Extendida[58]: conecta todas las estrellas a un solo switch central, administrando la información. Establece una jerarquía ya que el switch central es el que decide el tráfico de información a los nodos centrales de las estrellas que la conforman.

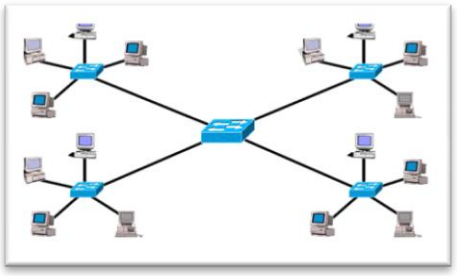

FIGURA 4

Generalmente, las redes militares son organizadas de acuerdo a tres tipos de arquitectura, estas dependen del nivel donde este implementada, el uso que se le dé a la información y la jerarquía del destinatario final de la misma.

Una de estas arquitecturas es del tipo centralizada (FIGURA 5[59]), donde el órgano decisor es alimentado por la información de las demás terminales, pero estas no tienen enlace entre sí, son solo órganos ejecutores. Este tipo de red es usado en organizaciones donde se deben tomar decisiones de forma rápida.

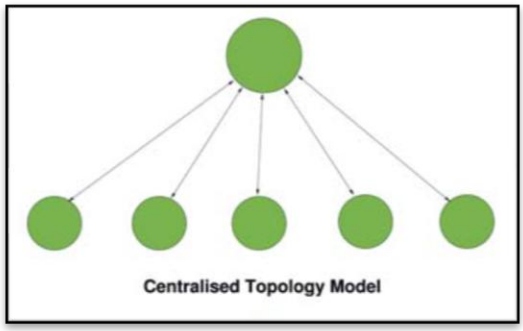

FIGURA 5

Otro tipo de arquitectura que se implementa es la de jerarquizar posiciones intermedias (FIGURA 6[60]) que pueden actuar como filtros de la información, donde la misma puede ser procesada y luego transmitida al centro decisor para que la misma pueda ser mejor comprendida.

---

[58] Ibíd. 12: diapositiva 14
[59] Kopp, Carlo; *NWC 101 Networked Operation*; Defense Today Magazine; 2005; Parte II; Pág 36
[60] Ibíd.

Estas posiciones intermedias se constituyen en nodos de comunicaciones y centralizan un grupo de terminales, generalmente las más cercanas a su posición, administrando su flujo de información.

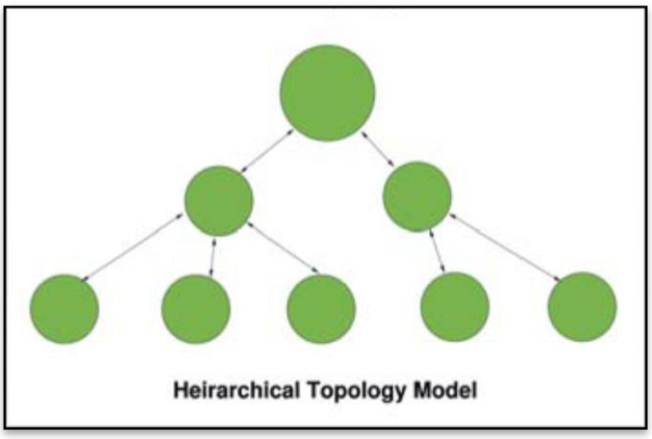

FIGURA 6

Por último, los elementos tácticos necesitan compartir información de forma rápida, razón por la cual conforman las denominadas redes AD HOC (FIGURA 7[61]), en donde todos están enlazados entre sí y no hay una jerarquía o administrador de la red.

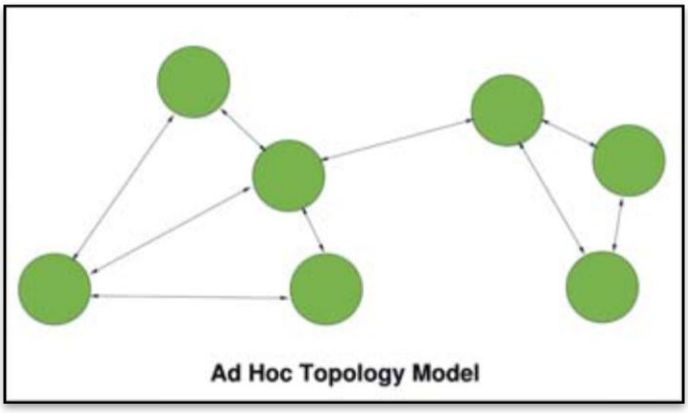

FIGURA 7

[61] Ibíd.

FIGURAS DE EJEMPLOS REDES AD-HOC[62]:

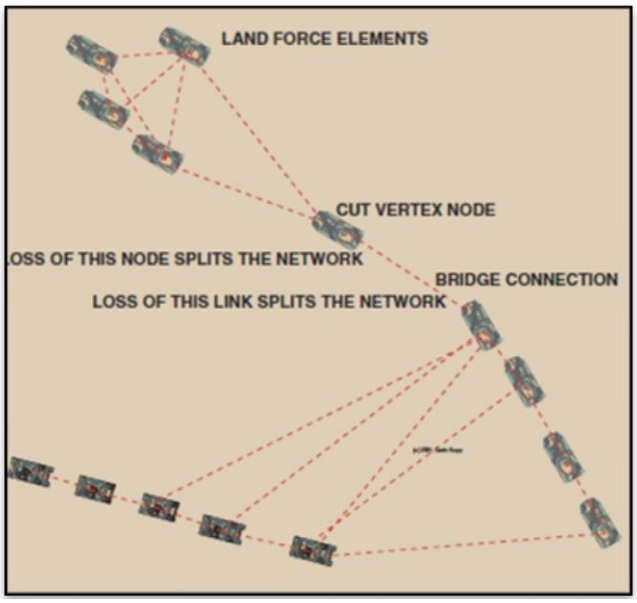

FIGURA 8 – Fuerzas terrestres comparten información y comunicaciones para generar una conciencia situacional del sector

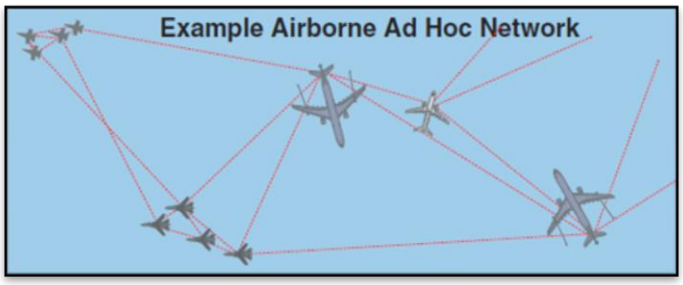

FIGURA 9 – Medios aéreos comparten información obtenida por sus sensores y datos para generar una conciencia situacional del aérea de responsabilidad donde están operando

[62] Ibíd.; Parte IV; Pág. 62

NIVELES DE PROCESOS REALIZADOS PARA LA INTEGRACIÓN DE INFORMACIÓN

La recepción de información de los sensores de un sistema de defensa es reunida y presentada en centros de información y control, como el de la FIGURA 9[63]

FIGURA 9: Ilustracion de un centro de información y control, donde se recibe y procesa la información de todos sensores desplegados.

En estos centros se cuenta con sistemas que procesan e integran la información recibida, contando para ello con software diseñado a tal efecto.

Estos integradores de información deben realizar complicados procesos y cálculos antes de entregar datos, los cuales se detallan a continuación:

Nivel 1[64]: evaluación del objeto (alineación de datos – correlación de dato/ objeto – estimación de posición, cinemática y otros atributos del objeto – estimación de la identidad del objeto).

[63] Kopp, C.; Óp. Cit. 59

Nivel 2[65]: evaluación de la situación (agregación de objetos – interpretación contextual – evaluación multiperspectiva).

Nivel 3[66]: evaluación del futuro (estimación/agregación de capacidad de fuerza – estimación de implicaciones - evaluación multiperspectiva).

Nivel 4[67]: proceso de refinamiento (gestión de la misión – predicción de entidad – requerimientos de las fuentes – modelización del rendimiento del sistema – control del sistema)

Nivel 5[68]: refinamiento cognitivo (gestión de la base de datos – interacción persona/ordenador).

En todos los niveles mencionados, se aplican algoritmos que son resueltos por software para acelerar el proceso y así obtener el producto en "*tiempo real*".

Los sensores de los que comúnmente se recibe información, son radares, sensores de imágenes o radiofrecuencias, como los que se ilustran en la FIGURA 10[69]

FIGURA 10

---

[64] Bazán, Guillermo; C*onsideraciones para la integración se sensores, para la elaboración de un sistema de control y vigilancia aeroespacial conjunta;* Trabajo de Investigación Profesional; Escuela Superior de Guerra Conjunta, Buenos Aires, 2010, Pág 13.
[65] Ibíd.; Pág. 14
[66] Ibíd.; Pág. 20
[67] Ibíd.; Pág. 15
[68] Ibíd.: Pág. 22
[69] Kopp, C.; Óp. Cit. 59

Estos sistemas permiten procesar toda esta información recibida y que la misma sea presentada sobre un mapa o carta, para que el comandante pueda tomar la mejor decisión posible sobre la situación del momento.

Debido a que deben recibir información del exterior y que el resultado de su proceso se presentará a quien debe tomar las decisiones, la integración de información se convierte en una parte vital a proteger de los ciberataques.

EJEMPLO DE UN SISTEMA DE DEFENSA INTEGRADO EN REDES

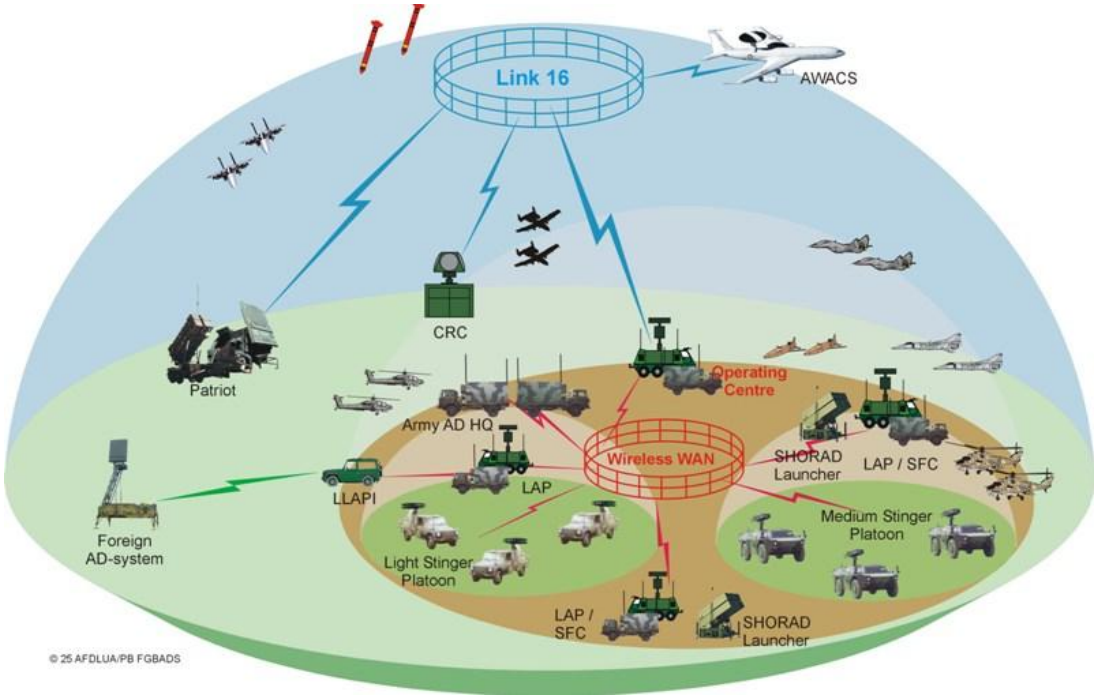

FIGURA 11 – Ejemplo de la conexión entre los distintos sensores y sistemas de armas a través de sus redes, para ejemplificar la cantidad de información que se debe integrar y procesar[70]

[70] Anón; *Neues Nahbereichsradar;* recuperado de: http://home.hccnet.nl/e.boukes/images/systemhistory/FGBADS%20version%205.5.jpg

TIPOS DE VIRUS INFORMÁTICOS MÁS COMUNES

- Virus informático[71]: son programas maliciosos que "infectan" a otros archivos del sistema buscando modificarlo o dañarlo. Instalan un código malicioso en el del archivo "víctima", normalmente un archivo de ejecución de forma que al iniciarse infecta los archivos que están en el sistema.

- Adware[72]: software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario. Registran actividad del usuario.

- Backdoors[73]: diseñados para abrir una "puerta trasera" en el sistema de modo tal de permitir al programador el acceso al sistema y hacer lo que desee con él. El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes.

- Bomba Lógica[74]: programa ilegítimo contenido dentro de un sistema que ante un evento o una fecha provoca un efecto en el sistema en el que está instalado. No se reproduce a sí mismo como un gusano y generalmente está programado para causar daño.

- Malware bot: está diseñado para armar *botnets*, de forma tal que el programador toma el control de varias computadores a la vez. Constituyen una de las principales amenazas en la actualidad. Este tipo apareció de forma masiva a partir del año 2004, aumentando año a año sus tasas de aparición.

---

[71] Rivero, Marcelo; *¿Qué son los malwares?*; Infospyware; 2013; recuperado de: http://www.infospyware.com/articulos/que-son-los-malwares/
[72] Ibid.
[73] Ibid
[74] Borghello, C.; Óp. Cit. 28; Pág. 284.

- Gusanos[75]: sub-conjunto de malware. No necesitan de un archivo anfitrión para mantenerse operativo dentro del sistema. Los gusanos pueden autocopiarse y propagarse utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P y dispositivos USBs. Se reproducen a sí mismos infinitas veces hasta agotar los recursos y hacer colapsar el sistema.

- Hijackers[76]: secuestran las funciones del navegador web modificando la página de inicio y búsqueda por alguna predeterminada, a su vez impide que sea restaurada por el usuario.

- Keyloggers[77]: almacenan en un archivo todo lo que el usuario ingrese por el teclado. Son programas ingresados mediante troyanos para robar contraseñas e información de los equipos en los que están instalados.

- Pup[78]: (potentially Unwanted Programs - Programa potencialmente no deseado) software que se instala sin el consentimiento del usuario y realiza acciones o tiene características que pueden menoscabar el control del usuario sobre su privacidad, confidencialidad, uso de recursos del ordenador.

- Riskware[79]: Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar ingresos no autorizados en el sistema.

- Rootkit[80]: son los programas más sofisticados de malware, funcionando de una manera no muy diferente a las unidades de elite de las fuerzas especiales: colarse, establecer comunicaciones con la sede, las defensas de reconocimiento, y el ataque de fuerza. Si se detectan y se hacen intentos por eliminarlas, se puede llegar a inutilizar todo el sistema. Eso es porque este programa se entierra profundamente en el sistema operativo y sustituye archivos críticos necesarios para el

[75] Rivero, M.; Óp. Cit. 68
[76] Ibíd.
[77] Ibíd.
[78] Ibíd.
[79] Ibíd.
[80] Ibíd.

funcionamiento del sistema. Cuando los archivos del rootkit se retiran, el sistema operativo puede ser inutilizado.

- Troyano[81]: En la teoría no es malware, ya que no cumple con todas las características de los mismos pero funciona como un transporte para estos ya que pueden propagarse de igual manera. Generalmente, es un pequeño programa generalmente alojado dentro de otro archivo normal. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo "huésped". Luego de instalarse, pueden realizar las más diversas tareas, ocultas al usuario. Se los utiliza para la instalación de otros malware como *backdoors*.

- Spyware[82]: es una aplicación que recopila información el usuario sin su conocimiento ni consentimiento. Normalmente, este software envía información a sus servidores detallando los hábitos de navegación del usuario.

- Ransomware[83]: programa que encripta la información del ordenador e ingresa en él una serie de instrucciones para que el usuario no pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero.

TECNICAS USADAS EN LA CIBERGUERRA

Las técnicas empleadas suelen ser:

- DoS[84]: (denial of service) consiste básicamente en la saturación de un servidor a través del envió de un flujo continuo y masivo de solicitudes de modo tal de dejarlo fuera de servicio volviendo inestable al sistema

- DDoS[85]: (distribuited denial of service) es un ataque DoS pero su variante consiste en que se realiza desde varios puntos de conexión, aumentando la

---

[81] Ibíd.
[82] Ibíd.
[83] Ibíd.
[84] Giudici, Eduardo Daniel; *lineamientos para la seguridad cibernética en un teatro de operaciones*; Trabajo Final Integrador de la Especialización en Estrategia Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta; 2013; Pág. 17.
[85] Mcdowell, Mindi; *Understanding Denial-of-Service Attacks;* US-CERT; 2013; recuperado de: https://www.us-cert.gov/ncas/tips/ST04-015

cantidad de solicitudes para *noquear* al servidor rápidamente. Las *botnets* pueden actuar simultáneamente o en forma alternada, según las coordine quien las controla.

- Pishing[86]: consiste en el robo de información personal y/o financiera del usuario a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

- Spam[87]: envío sistemático y masivo de correo electrónico no deseado que contiene archivos ejecutables para ingresar de forma no autorizada al sistema.

[86] Guidici, E.; Óp. Cit. 69
[87] Rivero, M.; Óp. Cit. 68