Guerra de la información y tanatología digital

Fredys A. Simanca H.[1], Fabián Blanco Garrido[2], Pedro Forero Saboya[3]

Recibido: 22/01/2018 Evaluado: 25/01/2018 Aceptado: 26/01/2018

Resumen

Si en el lejano ayer el hundimiento del régimen zarista, la devastación de Hiroshima y Nagasaki y los bombardeos de Dresde y Hamburgo, estremecieron e impactaron el contexto social, hoy cuando en el verdadero siglo de las luces, la economía de la información, categoriza al ciberespacio como el escenario sobre el cual se construye el desarrollo, los continuos ataques sobre las arquitecturas teleinformáticas, preocupan al capital cerebral de la organización inteligente y de las esferas administrativas del estado, pues la confiabilidad, consistencia, sustentabilidad y seguridad, se revisten de un alto índice de riesgo, que afecta tanto la cadena de valor asociada con el intercambio transaccional como la función de utilidad, empoderamiento y posicionamiento organizacional. La guerra de la información, exige que la ingeniería de sistemas, diseñe y construya herramientas de filtrado, detección y recuperación de información, aquí es donde la tanatología digital, como máxima expresión de la informática forense, se presenta como entidad e instrumento para la recuperación y reestructuración de los valores informáticos que fueron declarados como objetivo de destrucción en un vector de ataque.

Palabras Claves: Ataque, Confiabilidad, Consistencia. Seguridad, Tanatología

1. Introducción

La atención que se dispensa en el ciberespacio, para contrarrestar las amenazas de la seguridad: Intercepción, Interrupción, Modificación y Fabricación, se materializa en la existencia de políticas y mecanismos de seguridad, establecidos por la agencias reguladoras del proceso de intercambio transaccional: IAB, IETF y la IESG, pero a pesar de su existencia, el software dañino y otras estrategias y procesos de la guerra de la información, estropean muchas plataformas computacionales, de igual manera, la aparición de agentes lógicos en la red, contribuyen a la congelación de los sistemas de cómputo distribuido, por el registro de falla de omisión, de tiempo o de respuesta. La guerra de la información, manifiesta en la guerra de comando de control, la guerra electrónica, la guerra basada en la inteligencia, la guerra psicológica, la guerra cibernética y la guerra de la información económica, inquieta a las agencias de seguridad, pues la vulnerabilidad evidenciada por determinadas configuraciones, obliga al empleo como base defensiva de los efectos generados por el chipping, las armas electromagnéticas, las nano maquinas, la radiación Van Eck y los microbios destructivos, la tanatología, se presenta entonces como la disciplina orientada a la interpretación fenomenológica de los ataques informáticos, al reconocimiento estructural del andamiaje de ataque y a la reestructuración del escenario declarado como objetivo de destrucción, para valorar y formalizar la tipología del delito y proceder a parametrizar y definir los niveles de inmunidad frente a nuevos intentos de ataque.

2. Tanatología Digital: Interpretación Sistémica Funcional

En la mitología, Thanatos es la diosa de la muerte, sobrina de Erebo y nieta del Caos, etimológicamente Thanatos, significa muerte y Logos es discurso[1], pero formalmente, se entiende como la rama de la medicina legal que se encarga del estudio del cadáver, empleando para ello la Tanatosemiologia, el Cronotanodiagnostico y la necropsia, dentro del marco de la tanatolegislacion, independientemente de la tipología de muerte: Somática o celular; con la Tanatología forense, se determinan las causas, mecanismos y tiempo recorrido desde la aparición del cadáver.

Al interior del programa de Ingeniería de Sistemas de la Universidad Libre, en el área de formación electiva de seguridad digital, se consideró adaptar dicha significancia al entorno operacional de la seguridad digital, para considerar prospectivamente las implicaciones y problemas de la guerra de la información.

La guerra de la información, es definida por el ejército de los Estados Unidos, como el conjunto de acciones llevadas a cabo para el logro de la superioridad de la información, afectando los procesos, sistemas y los valores informáticos [2], su abstracción involucra el uso de equipos de cómputo y de dispositivos de alta tecnología y por ende para la formulación de estrategias de defensa, es preciso saltar de los instrumentos convencionales al empleo de unidades logísticas con alta confiabilidad e integridad, aquí reside el interés del grupo de ingenieros adscritos al programa en la Universidad Libre, para catalogar y dimensionar los alcances y la teleología operacional y funcional de la tanatología digital, como unidad sistémica que garantiza el RESTITIUM AD INTEGRUM –Restituir a la Integridad-.

Al interpretar normativamente, la tanatología digital, se pueden identificar los principios sistémicos que relacionan el isomorfismo, el homomorfismo y el isofuncionalismo, pues el análisis del objetivo atacado implica el traslado de la información a un esquema prototipificado, para evaluar las variables y el esquema de daños producido, para establecer tanto el marco de acción jurídico requerido para tipificar el delito como la tecnología electrónica , telemática e informática que permita elaborar el constructo de recuperación y restitución de la plataforma afectada por los intrusos, al considerar las medidas para la detección, bien sea por atención a la falacia de base o por efectos de detección distribuida [3].

Con el empleo de la tanatología digital, se podrá por ejemplo de manera sencilla y fácil, evaluar las fallas generadas por congelación, omisión de recepción o de envió y no sincronización de reloj [4], pero también se podrá recuperar un disco afectado, eliminar el bloqueo de puerto y unidades y restablecer la conectividad integral de los dispositivos afectados por el chipping, los microbios electrónicos o las nano maquinas.

3. Tanatología y Seguridad de la Información

El manejo y seguridad de la información, implica por necesidad, el estar familiarizado con los servicios de autentificación, control de acceso, confidencialidad, integridad y no repudio y con los mecanismos de cifrado, firma digital, relleno y control de tráfico, y las actividades de notarizacion acorde con los referentes señalados por X.800 y X.509 [3], por consiguiente entonces, debe manejarse con objetividad las aplicaciones de autentificación, la seguridad en la WEB, la seguridad IP y la seguridad en el correo electrónico, por ejemplo para el experto en seguridad de la información, es primordial el estar familiarizado con el proceso de clases de certificados de clave pública VeriSign y con el proceso de certificados S/MIME.

El tanatologo digital, debe entonces trabajar el entorno y esquema formal de la seguridad de la información, centrando su actividad en los procesos de detección de intrusos, en las técnicas de intrusión, en la funcionalidad del software dañino, en los sistemas de inmunidad digital y en los sistemas de confianza, pues solo así, podrá trabajar plenamente con los ejes de acción focal de la guerra de la información, sin olvidar obviamente lo descrito por el RFC3237.

El Tanatologo digital, con su experiencia, puede enfrentar la problemática base generada por ataques triviales, pero puede dilucidar los problemas asociados con las fallas de temporización, respuesta, transición de estado o bizantinas, como consecuencia de la realización de un ataque de guerra electrónica o de la acción semántica RPC [5].

4. Tanatología y Guerra de la Información

Contrarrestar los protocolos generados por ataques fundamentados en el chipping, las puertas traseras, las armas electromagnéticas con los cañones HERF (High Energy Radio Frecuency) y las bombas EMP (Electromagnetic Pulse), las Nano Maquinas, la Radiación Van Eck o los microbios destructivos, demanda poseer el conocimiento integral de las arquitecturas computacionales, los sistemas operativos, los protocolos de seguridad, el Middleware y las herramientas hardware y software para

análisis forense. El tanatologo digital, no es ajeno a los mecanismos de protección en redes SDH, ni a la estructura de las redes de acceso [6], debiendo por obligación identificar la funcionalidad Rambus y DDR, a comprender el nivel de operación Ultra3SCSI, a interactuar con el proceso de comprensión y extracción de audio, lo mismo que el operar con los recursos y efectos de las tarjetas 3D o con los monitores OLED [7].

El tanatólogo digital, en la guerra de la información - luego de registrarse un ataque -, procederá a evaluar el escenario de muerte digital, procediendo de manera similar a un experto en informática forense, es decir, deberá dar comienzo y contenidos de la cache, a evaluar los estados de conexión de red con las tablas de rutas, estados de proceso en ejecución, estado actual de las unidades de almacenamiento y registro de conectividad, evaluando los índices de acción y configurando el esquema de prueba jurídica y de recuperación del objetivo afectado; el tanatólogo podrá entonces verificar el problema causado por la activación de la señal de Chipping, diagnosticar la saturación de un circuito emisor por un emisor de alta potencia o por radiación Tempest y de la misma manera cuantificar los daños producidos por la operación de puertas trasera en la arquitectura.

5. Conclusiones

La guerra de la información, reclama la formación de un capital cerebral cuya solvencia y dominio temático de la tanatología digital, garantice el sortear los problemas generados por un ataque calificado, el conocimiento funcional de las variantes de ataque, que esgrime la guerra de comando de control, la guerra basada en inteligencia y la guerra electrónica, precisa la identificación plena de la arquitectura lógica computacional y teleinformática por parte del tanatólogo, pues sin esta fundamentación le será imposible verificar con su actuar el RESTITIUM AD INTEGRUM, los esquemas de Ciberdefensa y Ciberseguridad que se establecen en todos los países del orbe, señalan con urgencia la presencia de expertos en la eliminación y filtrado de ataques, cuyo nivel de integración, se encuentra definido en los esquemas diversos que manifiesta la guerra de la información, como nuevo emblema de conflicto en el ciberespacio.

Referencias

[1] Brino Mariño Margarita. Que es la tanatología. Revista Digital Universitaria UNAM, Vol. 7 No 8, 2006.

[2] Gavidia Arriscue José. La guerra de la información. Revista Escuela Superior de Guerra. No 187 Julio 2008.

[3] Stallings William. Fundamentos de seguridad en redes. Editorial Pearson 2010.

[4] Tanebaum Andrew y Van Steen Maarteu. Sistemas Distribuidos principios y paradigmas. Editorial Pearson 2008.

[5] Nelson A. Remote Procedure Call. Tesis doctoral. Carnegie Mellón University. 1999.

[6] Capmany José y Ortega Beatriz. Redes ópticas. Editorial Limusa 2008.

[7] Duran Luis. El gran libro del PC interno. Editorial Alfa Omega 2008.