2022

LA INFORMACIÓN COMO OBJETIVO DE LOS DELITOS INFORMÁTICOS Y EL TERRORISMO COMPUTACIONAL.

TERRORISMO CIBERNETICO Y DELITOS INFORMATICOS

WILLIAM ALBERTO SALAZAR TREJOS

LA INFORMACIÓN COMO OBJETIVO DE LOS DELITOS INFORMÁTICOS Y EL TERRORISMO COMPUTACIONAL

INTRODUCCIÓN.

Desde que el homo *Homo erectus* aprendió a dominar el fuego, se ha considerado el conocimiento y la forma de difundirlo como el principal activo con el que dispone la especie humana

A lo largo de la historia todas las civilizaciones han buscado la manera de almacenar el conocimiento para poder informarlo a sus generaciones futuras.

Desde las pinturas rupestres de las cuevas de Altamira, en forma de tablillas con escritura cuneiforme como lo hacían los Sumerios, mediante papiros con jeroglíficos empleados por los egipcios, mediante los nudos en sus quipu de los Incas o los códices Aztecas; para mencionar solo unos cuantos ejemplos; La humanidad siempre ha buscado almacenar su conocimiento para generaciones futuras.

El mayor ejemplo de almacenamiento de estos conocimientos del mundo antiguo lo constituyo la gran biblioteca de Alejandría.

Como sucedía en los albores de la sociedad, el conocimiento sigue siendo el bien más preciado… Fausto lo solicito a Mefistófeles; en la maravillosa obra de Goethe: el Fausto; a cambio de su alma.

El conocimiento siempre ha sido reclamado como botín de guerra, por el ganador; como se hizo en la segunda guerra mundial, donde los más grandes científicos alemanes fueron repartidos entre aliados y rusos.

Es importante reconocer que por falta de información (Y la manipulación malintencionada de la misma) se puede decir que se origino la segunda guerra mundial.

En la actualidad gran parte del conocimiento de la especie humana se encuentra almacenada en el ciberespacio, “la Nube”

Debido a que este está a disposición del que sepa acceder a él, actualmente, la información (conocimiento) es víctima de ataques por parte de gente inescrupulosa que desea obtener todo tipo de ventajas con su manipulación.

¿Por qué es importante tener conocimiento sobre este nuevo tipo de actividad delictiva: ciberterrorismo y delitos cibernéticos?

Desde el inicio de la civilización humana, cuando los primeros hombres descubrieron la necesidad de agruparse para lograr mayor seguridad y mejorar sus condiciones de vida; se dieron cuenta que el conocimiento era una de sus herramientas más valiosas para lograr estos objetivos.

Con la adquisición y acumulación del conocimiento, se percataron de su valor y vieron la necesidad de poder protegerlo y compartirlo solo con su comunidad; lo que aseguraría su permanencia y supervivencia a lo largo del tiempo.

Desde que la comunidad primitiva de recolectores empezó a tener excedentes y a competir con otros grupos por territorio, alimento y conocimiento; unos individuos entendieron que una forma de lograr su supremacía sobre otros, era infundiendo terror mediante actos violentos para apoderarse de ellos.

Esto no ha cambiado a lo largo de la historia. En el desarrollo de las diferentes sociedades (en Europa, América, Oriente, etc.) siempre se ha empleado el terror como medio de control geopolítico, eso incluye el uso de las religiones para generar ese terror.

Lo que no cambio, ni cambiara en la "evolución" de la humanidad, es que siempre lo que más han atesorado las diferentes civilizaciones, ha sido y será: el conocimiento, su almacenamiento y difusión del mismo.

A mediados del siglo XX, durante la llamada **Guerra Fría**; entre los Estados Unidos de América (EUA) y sus aliados, en contra de la Unión de Repúblicas Socialistas Soviéticas (URSS o CCCP) y sus aliados. Ambos entendieron que impidiendo la distribución del conocimiento del otro y apropiándose de él, les otorgaría una ventaja extra en una confrontación directa.

Esto se evidencio con el ataque de sabotaje perpetrado contra las antenas de transmisión de Utah, que eran utilizado por las fuerzas militares de los EUA[1], donde quedo evidenciado la debilidad de los sistemas de comunicación de esta nación.

Con el lanzamiento del primer satélite artificial; el SPUTNIK, el 4 de febrero de 1957, la URSS, había tomado la ventaja en cuanto a desarrollo en la transmisión y adquisición de conocimiento

1. El terrorismo cibernético como acto que criminaliza la libertad de expresión: una mirada desde la geo informática página 10

tanto propio como de su antagonista; EUA y sus aliados.

En respuesta al lanzamiento de dicho satélite artificial, los EUA, inicia su carrera espacial creando las agencias NASA y ARPA.

Como resultado de los esfuerzos de estas dos agencias, se puso en funcionamiento un sistema de comunicación descentralizado de uso militar. ARPANET; que posteriormente origino lo que actualmente conocemos como ***la Internet***.

En la actualidad; después de la caída de la URSS y con el fin de la **Guerra Fría**; esta herramienta de comunicación, que inicialmente era de uso exclusivo de la fuerza militares de los EUA, fue liberado al uso de la sociedad civil de todo el mundo.

Con la entrada en funcionamiento de ***la Internet****,* las fronteras físicas (Geopolíticas), ya no fueron un impedimento en la consecución, almacenamiento y la difusión del conocimiento.

Lo que anteriormente llevaba días, ahora está al alcance de un clic.

Con la entrada en funcionamiento de esta herramienta, que bien utilizada, puede mejorar las condiciones de vida de todas las sociedades del globo; como se evidencio en el desarrollo a una velocidad antes impensable, de la vacuna contra el SARS – CoV - 2 (COVID - 19), también ha ocasionado la aparición de una nueva forma de infundir terror en las personas y de cometer delitos en contra de ellas.

La finalidad de esta nueva manera de ocasionar terror y de delinquir, siguen siendo los mismos: Control y ventaja geopolítica y/o una compensación económica no merecida.

La ventaja que ofrece esta herramienta, sobre la forma en que se cometían este tipo de actos antes de su aparición son:

- No exige una presencia física para cometerlo.
- Es posible hacerlos de forma anónima gracias a la diversidad de software que lo permiten.

El perfil de las personas, que realizan este tipo de actos contra la sociedad, ha cambiado, son denominados: Delincuentes de cuello blanco.

Estos delincuentes tienen un conocimiento muy grande de los medios actuales de comunicación, además tiene acceso a software y hardware que les permite realizarlo (Y que cada vez son más fáciles y económicos para adquirir).

Muchos de estos delincuentes son patrocinados por los gobiernos antagónicos de cada país, con el objetivo de recaudar información sobre su antagonista, que le permita generar caos y obtener beneficios estratégicos y financieros.

La gran barrera que enfrentan las autoridades a escala mundial, para hacerle frente a este nuevo acto delictivo, radica en el derecho inalienable que todos los seres humanos promulgan: “La libertad de expresión.” Y por transitividad: el derecho de comunicar y de ser informados.

Esto, alimentado por la necesidad de la mayoría de los seres humanos de validación de sus pares, y el comportamiento de manada que las redes sociales han creado en los seres humanos.

Lo descrito anteriormente, facilita la actividad de estos delincuentes, pues, por la necesidad de ser aprobados, creen a raja tabla todo lo que les llega por estos medios. No dudan en compartir información personal y de interés único, solo porque creen que la mayoría siempre tiene la razón, han dejado de cuestionarse si lo que les llega por estos medios es real.

Lo anteriormente mencionado junto con otro tipo de herramientas (software) creadas por estos delincuentes, permiten que ellos tengan acceso a la información que les permite realizar sus actos delictivos.

Actualmente, a nivel mundial, para combatir este tipo de crímenes cibernéticos, “se ha adoptado una legislación que facilite la prevención de estas conductas delictivas y contribuya con herramientas eficientes en materia penal para detectar, investigar y sancionar conductas antijuridicas cometidos a través de internet[2];” conocido como convenio sobre cibercriminalidad de Budapest; el cual fue firmado el 23 de noviembre de 2001 y entro en vigor el 1 de julio de 2004.

En Colombia, se crearon unos nuevos delitos que se encuentran en la ley 1273 de 1999, el titulo 7 B “de la protección de la información y de los datos los datos”[3]

La forma en que son cometidos estos actos ilícitos, varía según los objetivos que se buscan.

A continuación, se mencionan algunos de los delitos cibernéticos más comunes, que actualmente se sabe son cometidos en Colombia.

---

2. El terrorismo cibernético como acto que criminaliza la libertad de expresión: una mirada desde la geo informática página 8

3 LEY 1273 DE 2009

Cuando se trata de delitos Informáticos:

- Estafa: su ascenso en la actualidad se debe a que pocas veces es denunciada. Las modalidades más empleadas son:
  - El Skimming: clonación bandas magnéticas de tarjetas de crédito y débito.
  - Carta Nigeriana: modalidad a través de correos electrónicos, son algo así como Spam.
  - Smisching: usado principalmente mediante redes sociales que mediante mensajes de texto tratan que la víctima ingrese a paginas ficticias donde se apoderan de información personal.
- Acoso a menores de edad: emplean plataformas como WhatsApp, Skype y software de almacenamiento en la nube.
- Falsificación de documentos: Laborales, personales, legales, imágenes y correos electrónicos.
- Falsificación de ID: esta va acompañada de estafas sus canales preferidos para hacerlo son las redes sociales.

Cuando se trata de terrorismo Cibernéticos:

Generalmente se realiza mediante hackeo de cuentas o empleando software desarrollados para tal fin.

A continuación, se listan algunos de los más empleados:

- Spyware: que se instala en el computador y monitorea todas las acciones que se realicen en él
- Hoaxes o falsos virus, que pretenden saturar la red para obtener listas de correos, recurren a la buena voluntad de los usuarios y en ocasiones con información falsa que pretende atemorizar con la perdida de algún servicio
- Spam: es un malware que generalmente contiene información publicitaria

Toda empresa o usuario de ***la Internet,*** debe considerarse como objetivo de estos ciber delincuentes.

Se recomienda que todas las empresas y usuarios debe tener un control que permita minimizar la posibilidad de ser victimas de este tipo de delitos.

Estas políticas de control deben estar desarrolladas basados en lo que se debe proteger y deben tener una relación costo beneficio que más favorezca a las empresas y a los usuarios.

La premisa de esta políticas debe ser: “**lo que no esta permitido, debe estar Prohibido**”

En la creación de estos controles Se debe tener en cuenta:

- En su gran mayoría los atacantes (ciber delincuentes) suelen ser personas cercanas, ya sea de la empresa o del entorno social de usuario.
- Todo sistema es importante y un posible blanco para estos delincuentes.
- Tener antivirus no asegura estar protegido, estos son creados en respuesta a los virus.
- El no abrir archivos no asegura que no se pueda ser víctima de este tipo de delitos y ataques, los computadores ejecutan acciones automáticas.
- Estar demasiado confiados en nuestro sistema de protección nos hace vulnerables.

El sistema de protección debe ser *hibrido* en lo posible, es decir emplear:

- Controles físicos: llaves de seguridad, teclados controlados por sistemas, números de identificación único de terminales, lectores, configuradores de rutas, entre otros
- Controles de acceso lógico: candados de control de tiempo, verificación de identificación y autenticación, procedimientos de revocación automáticos, pruebas de actividades autorizadas, bitácoras de seguridad, algoritmos de encriptación, salidas automáticas del sistema por tiempo.

Conclusiones:

- Todo usuario (empresa o persona), son blanco y objetivo de los ciber delincuentes

- Toda información, es un activo valioso y debe ser protegido de posibles ataques de estos delincuentes

- El deseo de aceptación de los seres humanos, facilita en gran medida el trabajo de estos delincuentes.

- El uso de forma racional y de forma responsable de ***la Internet,*** es una buena manera de proteger nuestra información.

- Nunca se esta totalmente protegido de los ataques de los ciberdelincuentes.

- Así como la información y el conocimiento son el botín, que persiguen estos delincuentes, también se debe convertir en nuestra principal herramienta para defendernos de ellos.

- Se debe denunciar todo tipo de ataque del que se sea objeto por insignificante que este parezca, eso facilita combatirlos.

- Es importante tanto en el ambiente laboral como personal crear protocolos que dificulten el accionar de estos delincuentes.

- Antes de realizar cualquier acción solicitada por medios electrónicos es recomendable validar la veracidad de la información suministrada y la autenticidad del solicitante.

Referencias Bibliográficas.

R Echeverria Gómez 2017.*El terrorismo cibernético como acto que criminaliza la libertad.*

Normatividad sobre delitos informáticos. Recuperado el 15 de agosto de 2022*. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos*

Argénida García Keyttel. *Guion – El Ensayo*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

Sandra María Ospina Sierra. *Informe Ejecutivo*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

Iván Manjarrés Bolaño. Farid Jiménez Tarriba. *Caracterización de los delitos informáticos en Colombia*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

María Imelda Valdés Salazar. *Seguridad Informática*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

Diario Oficial. *Ley 1273 de 2009*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

Yeffrin Garavito.Los tipos de delitos Informáticos más comunes. Recuperado el 15 de agosto de 2022*. https://uid.org.co/los-tipos-de-delitos-informaticos-mas-comunes-en-colombia/*

María Imelda Valdés Salazar, Elsa Cristina Arenas Martínez. *Controles de aplicación*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.

Edmundo Treviño Gelover. *COBIT y los controles de aplicación*. Formación en ambientes virtuales de aprendizaje Servicio Nacional de aprendizaje.