DELITOS INFORMATICOS

CIBERTERRORISMO

LUCIANO SALELLAS
SR HADDEN SECURITY CONSULTING

El presente estudio ha sido fruto de mucho tiempo de análisis y recolección de informes de seguridad de diversas agencias de inteligencia e investigación que se encuentran en la actualidad inmersas en no sólo el análisis para la prevención sino también en la lucha contra el crimen electrónico.

Los nuevos delitos tecnológicos avanzan día a día y con ellos, quienes estudiamos el nuevo mundo que internet ha gestado, preocupados por el avance de los nuevos riesgos que ponen en vilo a las infraestructuras gubernamentales buscamos las colaboración mutua de los gobiernos para la lucha y prevención del crimen tecnológico.

LUCIANO SALELLAS
SR HADDEN SECURITY CONSULTING

A mis padres, que me guiaron por el camino correcto.

A la eterna memoria del Dr. Carl Sagan, quien nos dio luz en un mundo de oscuridad.

A Lucía, que el mundo que te heredemos sea mejor que el mundo que nos legaron.

DELITOS INFORMATICOS

CIBERTERRORISMO

LUCIANO SALELLAS
SR HADDEN SECURITY CONSULTING

QUE ES EL DELITO INFORMATICO?

“Delitos informáticos" son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático

El *Delito Informático* implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Un incidente representa un reto para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia, y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad y conceptos sobre los hechos del incidente.

SEGURIDAD INFORMATICA

Es un compromiso de las instancias técnicas por estar preparadas para actuar y regular el efecto que dicho incidente puede ocasionar a la empresa u organismo gubernamental.

Administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo habilidad y pericia para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema.

Administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo habilidad y pericia para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema.

ANTECEDENTES

CASO X-TEAM

Todo comenzó el 25 de enero de 1998, cuando se cumplía un nuevo aniversario del trágico y lamentable crimen del reportero gráfico José Luis Cabezas. Ese mismo día, el site de la Corte Suprema de Justicia se veía la clásica (aunque también lamentablemente olvidada) foto de "No se olviden de Cabezas".

Junto al emblema, se pedía el esclarecimiento del caso, firmado por un grupo de hackers autodenominado X-Team. Junto al emblema, se pedía el esclarecimiento del caso, firmado por un grupo de hackers autodenominado X-Team.

La reacción de la Corte no se hizo esperar, y al día siguiente presentó una denuncia contra los NN que fue a parar al juzgado de Gustavo Literas, luego la causa la tomó Claudio Bonadio, y finalmente llegó a las manos de Sergio Torres. Así y todo, el X-Team no se detuvo, y el 25 de marzo de 1999 atacaron el site oficial de las Fuerza Aérea Argentina (hoy ya inexistente), denunciando el golpe de Estado de 1976.

Tras un largo recorrido por distintos juzgados, el juez Torres finalmente determinó que en la Argentina no es delito sabotear (hackear) una página Web, basándose en que solamente "las personas, los animales, y las cosas están protegidos por el código penal".

ANTECEDENTES INTERNACIONALES

125 Ciber criminales arrestados en Estados Unidos

Timothy Muris, director de la Comisión Federal de Comercio, se muestra orgulloso ante el éxito de la Operación llamada Ciber-sweep (ciber-barrida). “El ciberespacio no es lo mismo que el espacio exterior, y podemos seguir la pista y detener a cualquiera”.

Desde que comenzara la operación el pasado uno de octubre, se ha descubierto que entre todas las estafas cometidas por estas personas, los ciber criminales se han embolsado más de 100 millones de dólares pertenecientes a unas 125.000 víctimas en los últimos meses, por lo que no es de extrañar que, además de la Comisión de Comercio, el FBI, el Servicio Secreto y hasta 34 abogados dirigidos por el Departamento de Justicia de Estados Unidos, fueran tras su pista.

Entre los casos abarcados, se encuentra el del diseñador **John William Racine II**, culpable de redireccionar el tráfico de la web de Al-Jazeera ala suya propia, donde se podía ver una bandera estadounidense. El fiscal ha pedido tres años de libertas vigilada y mil horas de servicio a la comunidad.

Helen Carr ha sido declarada también culpable por simular correos de America On Line y enviarlos a sus clientes, pidiéndoles la actualización de sus datos de tarjeta de crédito (esto es conocido como "phishing").

Edward Fedora quiso vender una Medalla de Honor del Congreso a través de una subasta on line, a un precio inicial de 30.000 dólares.

En los primeros nueve meses de 2003, el Centro de Quejas de Fraude de Internet, un proyecto común del **FBI** y **National White Collar Crime Center**, registró 58392 fraudes relacionados con Internet, que contrastan con las 48.000 denuncias registradas durante todo 2002.

Dos adolescentes del poblado de Cloverdale, San Francisco (US) fueron acusados de un sabotaje informático.

Mediante una red de internet local (Netdex Internet Services), burlaron claves de seguridad e ingresaron a bancos de información esencial de varias agencias gubernamentales entre otras, una central de proceso de datos de la **NASA** donde habrían estado en contacto con el listado de guardias de seguridad, horarios de sus patrullas y varios secretos más.

De esto se pueden sacar conclusiones sobre qué ocurriría si un grupo terrorista se apoderara de semejante información.

Vladimir Levin. Fue condenado por haber ingresado a los centros de cómputos de algunos bancos efectuando transferencias de fondos en su beneficio por alrededor de 2.8 millones de dólares, aunque se afirma que un banco afectado manifestó haber perdido 10 millones de dólares.

Alexei Lashmanov, considerado uno de sus ayudantes, fue condenado a cinco años de prisión y a pagar 250.000 dólares de multa por efectuar transferencias similares entre bancos estadounidenses, de Finlandia e Israel.

El medio utilizado por estos últimos hackers para cumplir con su cometido no dista mucho de los ya citados, Levin trabajaba en una terminal informática de la empresa AO Sutnr, en St. Petersburg (Rusia), desde donde ingresó, entre otros, al Citibank Cash Management System.

Una diferencia que la misma comunidad hacker se ocupa de remarcar es la siguiente: un hacker es simplemente alguien capaz de manejar con gran habilidad un aparato, no necesariamente una computadora, con el fin de sacarle más partido o divertirse. Los crackers, en cambio, utilizan mal sus conocimientos, y suelen meterse en problemas por eso.

No hay manera, hasta el momento, de impedir que los hackers o crackers intercepten las conexiones entre las oficinas gubernamentales y los centros privados de investigación.

Las autoridades intentan diferenciar dentro de redes como internet, a servidores con información pública y servidores con información clasificada, estos con severas restricciones de acceso.

Los hackers buscan fama y renombre perforando estas barreras. Cuestionan a la autoridad y demuestran ser poseedores de conocimiento y tecnología, de hecho tienen varias direcciones donde se cruzan mensajes (www.260.com ó www.antionline.com).

INTEROPERABILIDAD

La respuesta en los Estados Unidos ha comenzado, aunque se considera aún insuficiente, agentes del FBI, los departamentos de inteligencia de las Fuerzas Armadas, los servicios secretos y la CIA, unidos en la investigación y en el accionar, intentan encontrar a los mayores responsables de las perforaciones en los bancos de datos.

La preocupación es una sola, la capacidad de enfrentar un atentado donde las claves binarias reemplacen al explosivo plástico, al trotil o a la dinamita y donde el ciberterrorista resulta ser un joven menor a 18 años de jeans, camiseta y ojos enrojecidos (tal la descripción de "**Analicer**", uno de los hackers más temidos).

DELITOS INFORMATICOS

Según el responsable de la Asociación para la Investigación de los Delitos de Alta Tecnología (High Technology Crime Investigative Association – HTCIA) las fuerzas de seguridad oficiales no cuentan con el personal o la tecnología suficiente para atender a las demandas de estos sectores frente a un problema calificado como "menor" frente a los delitos usuales.

La HTCIA fue creada por los propios afectados y constantemente incorpora nuevos miembros.

Los fraudes pueden ser de varios tipos, pero los más comunes consisten en la no entrega del / los objetos o dinero, falta de coincidencia entre el objeto presentado y el real, y el viejo y conocido acuerdo entre socios para inflar el precio de venta de un producto subastado.

De los 20 mil casos recolectados por la división del FBI encargada de fraudes informáticos en seis meses, el 64 por ciento de las denuncias corresponden a subastas on line, otro 22 por ciento a mercadería o dinero no enviado y apenas un 5 por ciento al fraude de tarjetas de crédito.

Claro que, recién cuando el fraude es detectado, comienza la historia; ya que ahí es el momento de entregar las pruebas a las fuerzas oficiales para que juzguen el caso y lo enmarquen dentro de las leyes.

Como muestra de este trabajo de investigación privado y condena pública, y de la dureza que se intenta imponer en este juego, en California (Estados Unidos), en abril de 2004, dos personas fueron encontradas culpables de fraude en transacciones on line por inflar los precios en más de mil subastas que habían colocado en E-Bay entre noviembre de 1998 y junio de 2004. Los detenidos pueden llegar a pasar hasta cinco años en prisión y fueron obligados a reintegrar un porcentaje del dinero obtenido en esas operaciones.

Según el FBI, el delito informático número uno que se lleva a cabo en el comercio electrónico es el del fraude en los sitios de subastas on line.

Sitios como el famoso eBay tienen su propio equipo y personal para intentar detectar y poner en evidencia estas acciones en su sistema.

Hasta ahora el caso más importante de fraude detectado sucedió en abril de 2004, durante una transacción que implicó la venta de monedas de plata y oro por un valor cercano al medio millón de dólares.

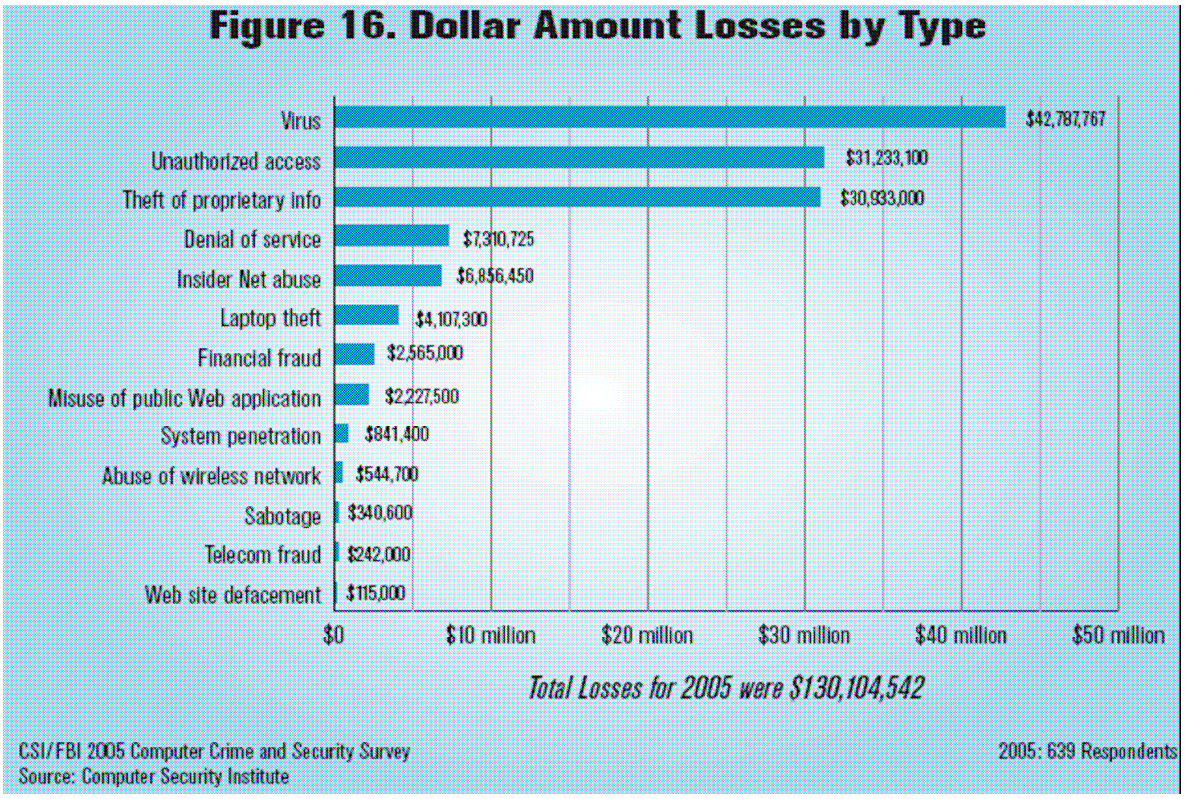
Figure 16. Dollar Amount Losses by Type
Virus
Unauthorized access
Theft of proprietary info
Denial of service
Insider Net abuse
Laptop theft
Financial fraud
Misuse of public Web application
System penetration
Abuse of wireless network
Sabotage
Telecom fraud
Web site defacement
$42,787,767
$31,233,100
$30,933,000
$7,310,725
$6,856,450
$4,107,300
$2,565,000
$2,227,500
$841,400
$544,700
$340,600
$242,000
$115,000
$0
$10 million
$20 million
$30 million
$40 million
$50 million
Total Losses for 2005 were $130,104,542
CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 639 Respondents


Figure 19. Organization Invests the Appropriate Amount on Security Awareness Training
Mean Values Reported on a Seven-Point Scale
High-tech
Federal Government
Other
Transportation
State Government
Telecommunications
Financial
Medical
Retail
Manufacturing
Educational
Local Government
Utility
Legal
1
2
3
4
5
6
7
Strongly Disagree
Strongly Agree
CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 698 Respondents

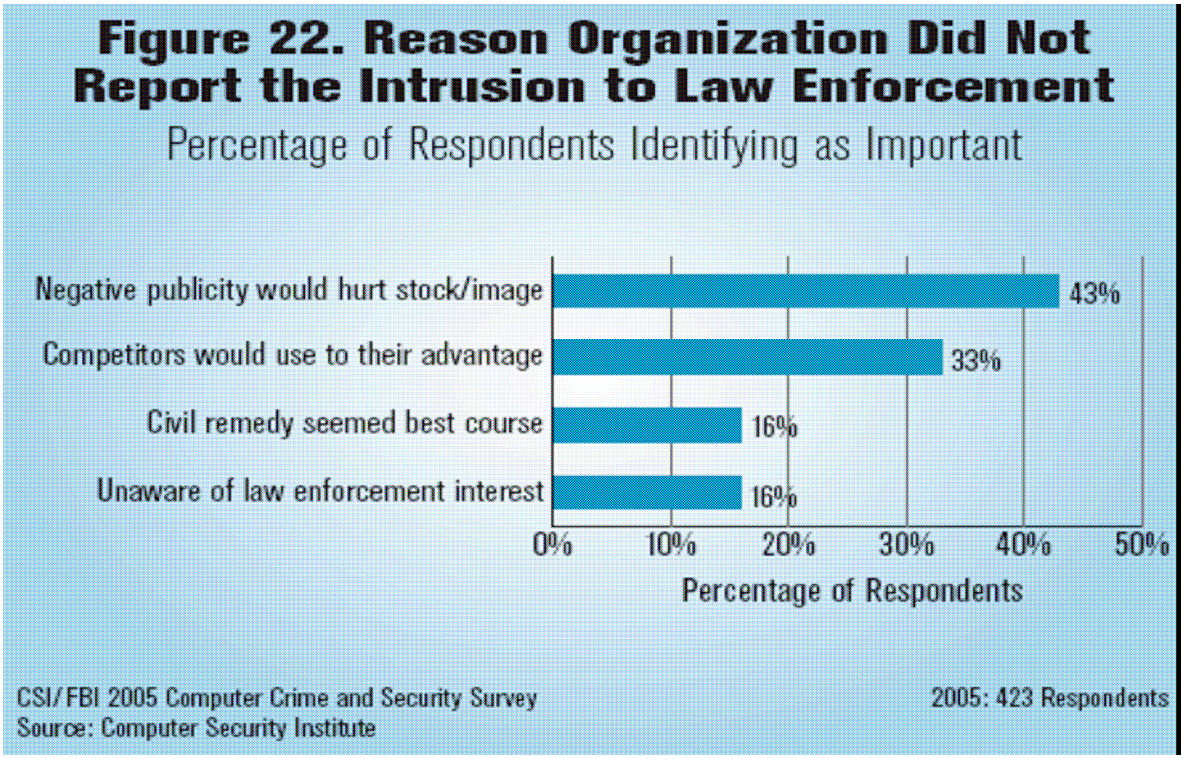
Figure 22. Reason Organization Did Not Report the Intrusion to Law Enforcement
Percentage of Respondents Identifying as Important
Negative publicity would hurt stock/image
43%
Competitors would use to their advantage
33%
Civil remedy seemed best course
16%
Unaware of law enforcement interest
16%
0%
10%
20%
30%
40%
50%
Percentage of Respondents
CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 423 Respondents

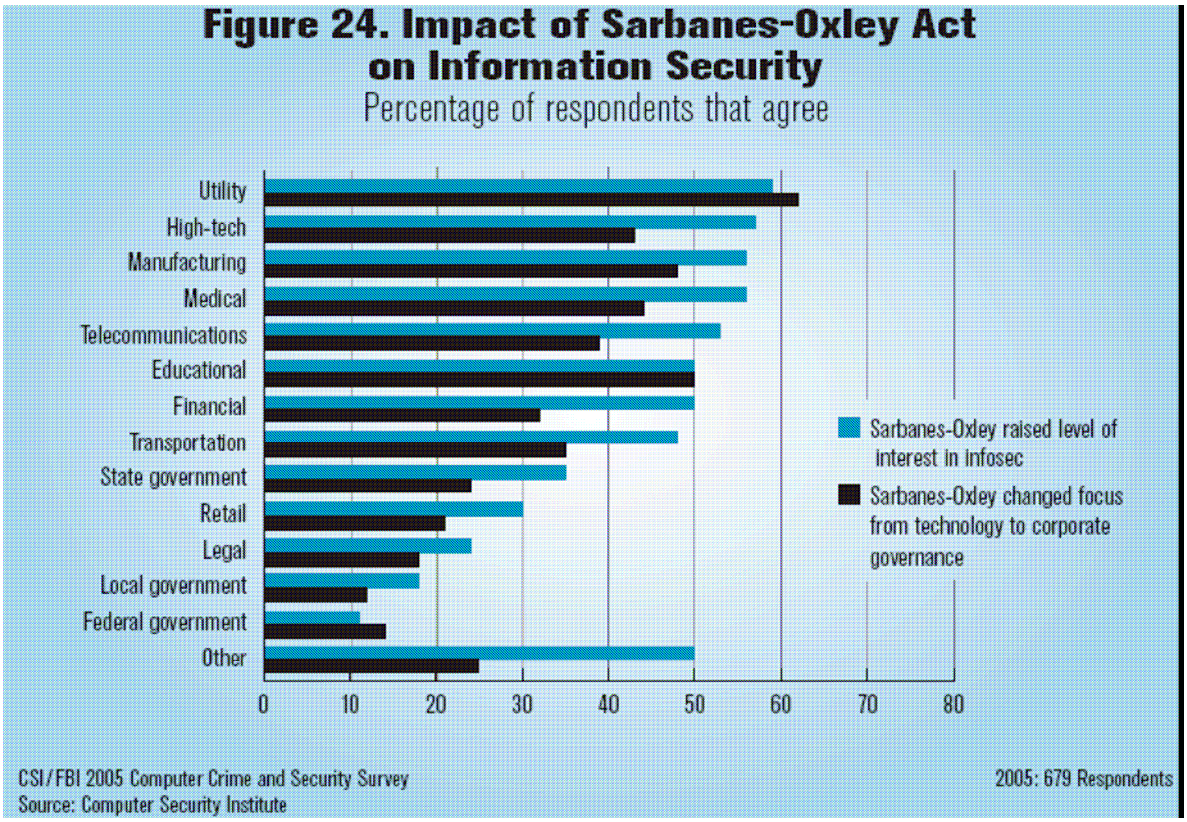
Figure 24. Impact of Sarbanes-Oxley Act on Information Security
Percentage of respondents that agree
Utility
High-tech
Manufacturing
Medical
Telecommunications
Educational
Financial
Transportation
State government
Retail
Legal
Local government
Federal government
Other
0
10
20
30
40
50
60
70
80
Sarbanes-Oxley raised level of interest in infosec
Sarbanes-Oxley changed focus from technology to corporate governance
CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 679 Respondents

Este fenómeno ha provocado preocupación en el mundo y hasta ahora el triunfo es de ellos, ya que llevan la iniciativa, tienen la tecnología y manejan la ciencia. Medidas tales como incrementar la seguridad informática, investigar y mejorar los mecanismos de encriptación standard (paradójicamente tarea desarrollada por hackers retirados y dedicados a una actividad oficial), educar a los usuarios y revisar o formular legislaciones referentes al caso, se tornan insuficientes cuando las redes son sistemáticamente vulneradas.

Los atentados en España nos demostraron que cualquier delito puede cometerse o investigarse con el acopio de medios informáticos.

Las investigaciones por los atentados en Madrid comenzaron como los de otros tantos delitos tecnológicos, intentando ubicar a los vendedores de los tarjetas chip mediante las cuales se cometieron los delitos.

Toda una red de telecomunicaciones, que incluye la transmisión a través de satélites fue utilizada para cometer asesinatos colectivos.

Las instalaciones nucleares y las comunicaciones estratégicas no son accesibles por internet; apenas 1% de los hackers tienen los conocimientos necesarios para generar destrozos a gran escala.

Sería necesario contar con recursos considerables para crear un daño real: 200 millones de dólares y cinco años de preparación de acuerdo a las conclusiones de un experimento llevado a cabo en julio del 2002 por la marina de EEUU.

¿Y qué ocurre en nuestro país?
Hasta ahora, Argentina no ha tenido un desarrollo tan importante de esta tecnología como para temer por el accionar de hackers o crackers a nivel de Seguridad Nacional, si bien ha habido algunos de ellos que en la actualidad trabajan como consultores de seguridad informática o brindando cursos y capacitaciones para profesionales del rubro (Ej. **Julio Ardita** "El gritón" - Cybsec).

En cuanto al Estado, existen tibios esfuerzos para generar políticas de coordinación informática en cuanto al equipamiento y la instalación de redes así como a legislaciones férreas al respecto de este tema.

EN 2005 AUMENTO EL ROBO DE DATOS PERSONALES EN INTERNET

La actividad delictiva a través de Internet tuvo un notable crecimiento en 2005, advirtió el último informe de Symantec sobre amenazas a la seguridad informática, que subrayó que el 80% de las 50 muestras más peligrosas de códigos maliciosos podrían revelar información confidencial. Según el análisis, aunque los ataques anteriores estaban diseñados para destruir la información, actualmente se están diseñando ataques para robar silenciosamente la información por razones económicas sin producir perjuicios notables que pudieran alertar sobre su presencia al usuario.

Las amenazas relacionadas con el delito en el ciberespacio están cobrando impulso a través del uso de herramientas de software para cometer fraudes en línea y robar la información de los consumidores y las empresas.

Los piratas están dejando de lado los grandes ataques de múltiples propósitos a los dispositivos tradicionales de seguridad como los firewalls y routers para centrar sus esfuerzos en objetivos regionales, equipos de escritorio y aplicaciones Web que les permitan robar información personal o corporativa, financiera o confidencial.

La constitución de un sistema centralizado de inteligencia militar, criminal y nacional y otorgar legalmente a la Escuela Nacional de Inteligencia capacidad para coordinar los esfuerzos en la capacitación de personal frente a los desafíos que presenta la era de la información posibilitan un aceleramiento de las respuestas gubernamentales que demanda la actual situación internacional.

CONFERENCIA DE LA OEA SOBRE SEGURIDAD CIBERNÉTICA JULIO DE 2003 – BS. AS.

Entre los puntos más importantes se sugirió que una alerta temprana ayudaría a abordar los ataques cibernéticos permitiendo que los proveedores de servicios de internet eviten que los atacantes usen sus servicios, pero se recalcó que el primer paso en el combate de los delitos cibernéticos sería contar con un software seguro. Existe una epidemia de delitos cibernéticos organizados que no se divulga, y se propuso la creación de iniciativas público-privadas específicas para enfrentar efectivamente esos delitos.

Se afirmó que el objetivo de los enfoques múltiples y las metas comunes de vigilancia y alerta es diagnosticar rápidamente los incidentes cuando ocurren y comunicar a los demás el diagnóstico a efectos de minimizar el impacto y facilitar la recuperación, aspecto clave de la seguridad cibernética en general.

Como punto más importante se concluyó que la OEA sea el líder en este aspecto estableciendo un marco de política de cooperación que en efecto pueda constituir una red de vigilancia y alerta cibernéticas en las Américas.

Acciones coordinadas por organismos nacionales en el campo de la seguridad informática y telecomunicaciones en el marco de la lucha contra el ciberterrorismo

Existe una tarea de cooperación activa de parte del gobierno y el Congreso de Argentina, de los profesionales y de las fuerzas armadas y de seguridad.

El Ing. Castro Lechtaler (miembro de CITEFA, Centro de Investigación Tecnológica de las Fuerzas Armadas) ofreció una serie de becas para que expertos de los Estados miembros de la OEA puedan participar en los cursos de seguridad cibernética dictados por CITEFA.

Gastón Franco (Coordinador Técnico de AR-CERT) explicó los objetivos de AR-CERT, que incluyen la centralización y coordinación de tareas para enfrentar los ataques o intentos de ataques contra redes, y la participación en la infraestructura internacional de respuesta global a incidentes en la seguridad. Afirmó que AR-CERT participa en la protección de recursos de informática, la prevención, detección y gestión de incidentes en la seguridad, y en la capacitación de profesionales.

El Crio. Santillán (Director de la División de Cibercrimen de la Policía Federal) señaló que la gran mayoría de los delitos cibernéticos son desconocidos por el sistema judicial y la policía, lo que significa que no son penados. Observando la gran complejidad y el carácter técnico de estos delitos, así como la dificultad de probar quiénes son los autores, propuso:

La institución de la seguridad informática
La adopción de normas internacionales de la ISO
Que se imponga una actitud institucional de protección de la actividad cibernética
leyes que faciliten la acción policial
Un incremento de la experiencia policial y la participación en cursos y foros internacionales
Una estrategia nacional de garantizar la seguridad de los sistemas estatales críticos, y capacitación permanente.

Steven Monblatt (Secretario Ejecutivo de CICTE) observó que una serie de problemas descritos por los panelistas y que padece Argentina son comunes a otros Estados y convino que pueden ser abordados mediante leyes nuevas o actualizadas, capacitación y suministro de recursos, fomentando a la vez una "cultura de denuncia". Observó que el Gobierno de la Argentina ha tomado medidas para enfrentar estos delitos, inclusive mediante la participación de las comunidades, la asistencia a otras entidades y el intercambio de información sobre delitos cibernéticos.

El señor Monblatt sugirió que la OEA también puede examinar programas encaminados a ayudar a los jueces a comprender los problemas de la seguridad cibernética.

Grupo de Expertos Gubernamentales en materia de Delitos Cibernéticos Reunión de Ministros de Justicia de las Américas (REMJA)

Leonard Bailey, Presidente de este Grupo de Expertos Gubernamentales, presentó las recomendaciones de la Segunda Reunión de Ministros de Justicia y del Grupo de Expertos. Se informó que de acuerdo al análisis de las respuestas de los Estados miembros a los cuestionarios sobre delitos cibernéticos, en general, los agentes del orden habían recibido capacitación y que la legislación aún no ha sido actualizada.

Se describieron las prioridades de este Grupo de Expertos como el establecimiento y fortalecimiento de las dependencias encargadas de la investigación y el procesamiento de los delitos cibernéticos, la capacitación -incluidos los jueces, abogados y fiscales- y el desarrollo jurídico, para permitir la investigación y sanción de estos delitos
Las sesiones de trabajo legislativo regional del Grupo apuntan a asegurar una participación firme de los Estados miembros de la OEA y la actualización de la legislación. La legislación sobre delitos cibernéticos crearía redes seguras y confiables, disuadiría y prevendría los delitos cibernéticos y fomentaría la cooperación internacional.
Se propuso la elaboración de programas para asistir a los Estados miembros en la capacitación, la actualización de la legislación y la concientización del público.

Comisión Interamericana de Telecomunicaciones (CITEL)

El sector de las telecomunicaciones está preocupado por la seguridad cibernética porque Internet ha penetrado en casi todos los niveles de la prestación de servicios sin un análisis previo serio de sus posibles vulnerabilidades.

Se sugirió que son necesarias la prevención y protección, así como una inversión de las Empresas que valga la pena, que la cooperación y colaboración son esenciales, y que deben realizarse también análisis e investigaciones.

Comité Interamericano contra el Terrorismo (CICTE)

El Plan de Trabajo de CICTE incluye programas orientados a la identificación y coordinación de capacitación para los sectores público y privado en los Estados miembros.

CICTE une a los Estados miembros para el intercambio de información e inteligencia con confianza, usando una herramienta de red segura para la comunicación entre los contactos nacionales.

CRITERIO PRINCIPAL DE CICTE

Adopción de una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de Seguridad Cibernética.

Urge a los Estados Miembros a establecer o identificar grupos nacionales "de vigilancia y alerta" también conocidos como "Equipos de Respuesta a Incidentes de Seguridad en Computadoras (ERISC)".

CICTE tiene la misión de asistir a los Estados Miembros en el desarrollo de los ERISC durante los próximos años.

FBI
INTERNET FRAUD COMPILATION CENTER (FBI/NW3C)

El servicio de investigaciones del FBI, ante la creciente demanda de instituciones, empresas y personas afectadas por la acción de delitos informáticos implementa el "National White Collar Crime Center (NW3C), Centro de Delitos de Cuello Blanco" a fin de prevenir y controlar los fraudes y delitos informáticos.

CUERPO NACIONAL DE POLICIA ESPAÑOLA
UNIDAD DE INVESTIGACIÓN DE DELINCUENCIA EN TECNOLOGÍAS DE LA INFORMACIÓN

Esta unidad nace en el año 2000 con el objetivo de impulsar, coordinar y realizar investigaciones relacionadas con los delitos realizados a través del uso indebido de nuevas tecnologías y estrechar relaciones con las nuevas policías de la Comunidad Europea.

POLICIA DE INVESTIGACIONES DE CHILE

Durante el año 2000 se crea la Brigada de Investigación de Delitos Informáticos dedicada exclusivamente al rastreo, prevención y control de los delitos dentro de su frontera, princ`palmente con hechos relacionados con hacking a sitios oficiales del gobierno o defraudaciones a empresas privadas. Se relaciona directamente con el FBI, donde recibe capacitación e intercambio de materias de estudios de los delitos informáticos.

INTERPOL

Interpol Internacional, a través de los últimos años se ha dedicado a la investigación de delitos informáticos a través de lo cual crea una unidad interna conocida como ITC (Information Technology Crime).

AFCEA ARGENTINA

Desde abril de 2000 Argentina es sede para América del Sur de la Asociación Internacional de Comunicaciones Electrónicas de las Fuerzas Armadas (AFCEA Internacional), como organización civil sin fines de lucro, que reúne a especialistas en los problemas del C4ISR (Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento Electrónico) del ámbito Gubernamental, industrial, empresarial, de las Fuerzas Armadas y de seguridad, para fomentar el entendimiento, promover la eficiencia, la cooperación y el desarrollo profesional de sus miembros a fin de lograr una verdadera evolución en el campo de la información.

POLICIA FEDERAL ARGENTINA

El Instituto Universitario de la Policía Federal Argentina además de poseer una carrera de ingeniería en telecomunicaciones se destaca en su Licenciatura en Sistemas de Seguridad en Telecomunicaciones donde se crean capacidades para los estudios de factibilidad, proyección, implementación, mantenimiento y evaluación de sistemas y dispositivos que resguarden la seguridad de la operación y proporcionen confiabilidad a las instalaciones de redes y equipamientos de los sistemas de Telecomunicaciones.

•Se crea la División Seguridad Informática y Cibercrimen.
•Ajustada a las limitaciones presupuestarias del Estado Nacional, adopta políticas de incorporación de tecnologías.

•Implementa incrementalmente un portal de servicios en Internet para satisfacer las necesidades de la ciudadanía.
•En este medio hoy se pueden recibir denuncias y facilitar tramitaciones.
•Se capacita al personal en estas tecnologías, con cursos propios o se les facilita su capacitación en forma privada

POLICIA FEDERAL ARGENTINA
PROPUESTAS

•Se propone por los medios administrativos institucionales la figura legal del "agente encubierto".
•Se propone reglamentar la actividad de los proveedores de Internet (ISP).
•Se propuso ante una iniciativa de la Cámara de Senadores de la Nación, con relación a las figuras del "delito informático", específicamente tratar los delitos contra menores.
•Se impulsa un recurso legal para permitir realizar la intercepción y "escuchas" de correo electrónico y "chat" respectivamente.

•Se formula la implementación de una base de datos nacional para los delitos de "Alta Complejidad".
•En el ámbito del "Convenio Policial Argentino", se propuso la creación de un portal que permita la interacción a esta base de datos; con los medios con que hoy cuenta la Policía Federal.
•Se busca concretar convenios con las fuerzas del orden locales y de otras naciones para aunar esfuerzos, lograr celeridad y ser más efectivos.

GOBIERNO DE LOS ESTADOS UNIDOS DE AMERICA

En julio de 1996 durante la administración Clinton se crea la Comisión Presidencial para la Protección de la Infraestructura Crítica conocida en inglés por la sigla PCCIP (the President´s Commission On Critical Infrastructure Protection).

El fin de este Organismo era estudiar las infraestructuras que constituyen el soporte de vida cotidiana de Estados Unidos, determinar sus vulnerabilidades ante una amplia gama de amenazas, y proponer una estrategia para protegerlas en el futuro.

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURA (NIPC)

El NIPC nació para ser el punto clave de coordinación de las "ciberdefensas" nacionales. Para ello, dicho organismo se encargó de reunir a representantes de agencias gubernamentales, funcionarios de los distintos estados norteamericanos y de los gobiernos municipales, y representantes del sector privado, para "proteger la infraestructura crítica de la nación"

INFORMATION WARFARE

Los desafíos que presenta la era de la información generan una nueva y amplia gama de amenazas. En ese sentido, se enmarca la guerra de la información, Information Warfare (IW) que constituye la primera respuesta en el sentido ofensivo frente al impacto de las Nuevas Tecnologías de la Información (NTI).

La IW actúa en la reconfiguración y preservación de la identidad de los distintos actores frente a este nuevo escenario ya que brinda movilidad e influencia en el campo de la batalla de la información.

ANTITERRORISMO
CONCEPTOS

El Informe del Secretario General de la ONU de julio de 2004, valora el esfuerzo hecho por la ONU, dirigido sobre todo a la prestación de asistencia técnica para ratificar y aplicar los nuevas leyes antiterroristas, la revisión normativa nacional, la formación de funcionarios (más de 500 legisladores y funcionarios policiales de más de 80 países formados en la aplicación y disposiciones de la Resolución 1373), la elaboración de planes de acción nacionales con los gobiernos, se han recaudado más de 3.200.000 $-USA, para el Fondo ONU para la prevención del delito y la justicia penal en relación con proyectos de asistencia técnica de prevención de terrorismo, con aportaciones significativas de Austria, Reino Unido e Italia. Además, el Informe reclama aportaciones económicas adicionales, progresos en la preparación de un proyecto de convención general sobre terrorismo internacional y mejora de la capacidad nacional ante las políticas antiterroristas.

La Unión Europea, fruto de los cambios posteriores a la Guerra Fría, se vio forzada a elaborar, por primera vez en su historia institucional y política, una estrategia para abordar su papel y su responsabilidad en el mundo actual. Esto condujo al documento base "Una Europa segura en un mundo mejor", la Estrategia Europea de Seguridad, de 12 de diciembre de 2003. Con ella, la Unión se dota de una estrategia de carácter político para aumentar su compromiso y responsabilidad en un marco globalizado y de multilateralismo eficaz. Pretende responder a los retos de la seguridad interior y exterior posterior a la Guerra Fría y a la mundialización creciente, considerando cinco amenazas principales, entre las que destaca el terrorismo internacional. Define unos objetivos estratégicos, sus implicaciones, los instrumentos combinados para hacer frente a las amenazas y desafíos, destacando la capacidad de gestión de crisis y prevención de conflictos, en un contexto de mayor refuerzo y cooperación con Naciones Unidas.

Se han sucedido dinámicas multilaterales y unilaterales y se han establecido diferentes estrategias para responder a los ataques terroristas.

En ese punto nos encontramos entre la necesidad de responder coyunturalmente a los ataques producidos y la de estructurar una nueva arquitectura internacional contra el terrorismo. Naciones Unidas se ha puesto a la vanguardia en este último caso. Estados Unidos en el primero, pero como reacción a los ataques contra sus intereses.

CIBERTERRORISMO
CONCEPTOS

El ciberterrorismo es la acción violenta que infunde terror realizada por una o más personas en Internet o a través del uso indebido de tecnologías de comunicaciones.

Estos grupos preparan sus acciones por medio de mensajes encriptados a través del correo electrónico, impidiendo la penetración de los organismos de seguridad de los Estados.

A esto hay que sumar los sitios web donde estos grupos terroristas dan a conocer su historia, postulados, objetivos.

Algunos de estos grupos son: KKK en Estados Unidos, ETA en España, grupos neonazis de Bélgica y Holanda y Verdad Suprema en Japón.

ANÁLISIS DE RIESGO

Un ciberterrorista podría cambiar remotamente la presión de los gasoductos causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios. “De la misma manera, la red eléctrica se vuelve cada día más vulnerable”.

Un ciberterrorista podría atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos grandes aeronaves civiles choquen entre sí. “Este es un escenario realista, desde el momento en que el ciberterrorista también podría interferir los sensores del interior de la cabina”, maniobras similares pueden ser realizadas con las líneas de ferrocarriles.

Un ciberterrorista podría interferir a los bancos, las transacciones financieras de dinero y los centros bursátiles. De esta manera, los habitantes del país perderían su confianza en el sistema económico.

Un ciberterrorista podría alterar las fórmulas de remedios o productos farmacéuticos, causando una gran cantidad de pérdidas humanas.

Las personas encargadas de velar por la seguridad de la Nación no estarán advertidas ni podrán anular al ciberterrorista, que probablemente se encontrará en el otro lado del mundo. Lamentablemente estos ejemplos no son de ciencia ficción. Todos estos escenarios pueden tener lugar hoy. Como muchos sabes, algunos de esos incidentes ya han ocurrido en varias naciones.

Muchos de estos actos ocurrirán en un futuro próximo.

SITIOS DE PROPAGANDA

- www.hizbollah.org - sitio islámico del Hezbollah
- http://osis.ucsd.edu/~ehj/html/eta.html - ETA
- http://burn.ucsd.edu/~farc-ep/ - FARC
- www.csrp.org/ - Sendero Luminoso
- www.hamas.org - Hamas
- www.k-k-k.com - KKK

A nivel mundial los países están preocupados por el ciberterrorismo y por esto mismo existen dos tendencias: los que apoyan la conformación de una "ciberpolicía" que trascienda las fronteras y los que se inclinan a favor de mejorar la cooperación internacional.

Las sedes de Al Qaeda en Afganistan cuentan con equipos de comunicaciones los cuales a través de Internet sirven como medio de apoyo logístico en la diversificación de la circulación y protección de las finanzas de Al Qaeda.

Los últimos ciber ataques a los Estados Unidos han tenido como objetivo atacar la propia infraestructura de Internet a través de ataques DoS (Denegación de Servicio) a los servidores de la Red.

El más sofisticado de estos ataques se produjo en octubre de 2001 y afectó a 9 de los 13 grandes servidores raíz de la red.

El FBI NIPC (National Infraestructure Protection Center) informó que encontró evidencia de que un grupo terrorista estaba preparando un ciber ataque al sistema de aprovisionamiento de agua en USA. (AP. 31/01/02)

Internet ha gestado 3 formas de ciberterrorismo:

¨Escenario abierto a millones de potenciales adherentes, desde el cual se practica la propaganda política.
¨Ejercicio de la violencia, donde la información se convierte en objetivo deseado y, en apariencia, en extremo vulnerables para los atentados.
¨Coordinación de la operación y logística de ataques terroristas

OBJETIVOS COMUNES DE CIBER ATAQUES

¨Redes de Gobierno y FFAA
¨Servidores de nodos de comunicación
¨Servidores DNS locales
¨Centrales telefónicas digitales
¨Estaciones de radio y televisión
¨Centros satelitales
¨Represas, centrales eléctricas, centrales nucleares.

TIPOS DE ATAQUES

¨Siembra de virus y gusanos
¨DNS (Cambio en las direcciones de dominio)
¨Intrusiones no autorizadas.
¨DDoS (Distributed Denial of Service)
¨Saturación de correos
¨Bloquear servicios públicos
¨Blind radars (bloquear tráfico aéreo)
¨Interferencia electrónica de comunicaciones

CIBERTERRORISMO

REFLEXIONES FINALES

Dos conceptos básicos, el Terrorismo e Internet se combinan para crear una nueva arma llamada Ciberterrorismo (INFOGUERRA-CIBERGUERRA) son personas que desean un cambio radical, total y brusco a nuestra forma de gobierno democrático y sistema social establecido.

El ciberterrorista es un arma de bajo costo ya que requiere de un alto entrenamiento, dedicación, pero al mismo tiempo es difícil de rastrear y el daño al "enemigo" puede ser desde considerable hasta muy grave.Desde el punto de vista de la guerra y de la doctrina táctico-militar, la ciberguerra y el ciberterrorismo incorporan a los tradicionales campos de batalla (tierra, aire y mar) dos nuevos campos los cuales son el ciberespacio y la información.

El ciberterrorismo es un método de alto riesgo y bajo costo, al alcance de las naciones pobres, que pueden causar enormes daños al país atacado. Dos países pueden tener relaciones diplomáticas y comerciales normales, estar en estado de paz, pero, al mismo tiempo, en estado de ciberguerra. (Ej. China – USA)

Uno puede atacar las redes del otro desde su territorio o desde otras plataformas cibernéticas, de otros países o continentes. No es una guerra en *close-contact* y los combatientes no se conocen y posiblemente, nunca se van a conocer.

La ciberguerra y el ciberterrorismo son una parte del lado oscuro de la globalización.

La cibernética e Internet son un campo muy fácil de abordar para los dos bandos. Debemos estar muy alertas a este nuevo tipo de guerra y terrorismo, debido que la civilización de tipo occidental se apoya en un grado mucho más alto en la tecnología basada en computación y redes.

Las asimetrías políticas, económicas, militares, tácticas, estratégicas, sociales y culturales se acentuaran más, al paso del tiempo y con la acentuación aumenta la dependencia de medios electrónicos.

Los sabotajes, el ciberterrorismo, las municiones de precisión y los misiles armados con todo tipo explosivos, de agentes químicos, atómicos y radiológicos serán las armas de los nuevos arsenales del futuro. La unión de medios tradicionales: *balas, explosivos, cohetes y misiles* con medios no convencionales: *químicos, atómicos, bacteriológicos*, combinados en el fondo de Internet, como plataforma de búsqueda, compra, logística y comunicación, es el ámbito de esta guerra generalizada y mortífera, en que el mundo esta hoy envuelto.

En referencia a posibles grupos o células terroristas se cruzan de múltiples maneras con la economía y la sociedad legítimas. Para hacer frente a este desafío es fundamental que la comunidad internacional asigne recursos y mantenga una firme voluntad política colectiva, sino las consecuencias a largo plazo para el ejercicio democrático del poder y el imperio de la ley serán desfavorables.

Hoy Internet es un trampolín y base para que los terroristas pueden concebir, planear, tener logística y ejecutar futuros ataques por esto mismo debemos establecer una continua cooperación en materia de seguridad, manejo de crisis y tecnología avanzada en la lucha contra el terrorismo.

"De todos depende el éxito en la lucha contra el ciberterrorismo y el fundamentalismo que lo sustenta", del gobierno, las Industrias, empresas, fuerzas armadas y de seguridad, de la cultura de no violencia y tolerancia.

AGRADECIMIENTOS

A mi socio, Fabio Zamero, por la paciencia y sus invalorables consejos que muchas veces han dado luz. A Marcelo Morello, por sus aportes y conocimientos. Al Grupo Educativo Forum por su abierta disposición a colaborar para la difusión en la ciudad de Paraná. Al Prof. Edgardo Frigo, del Foro Latinoamericano de Profesionales en Seguridad. A nuestros partners, Alejandro Barbero y Marcelo Lescano. Y a todo el grupo de colaboradores de SR HADDEN SECURITY CONSULTING, Dr. Pablo Zapata Libert, Comisario Principal Lic. Héctor Olivera, Laureano Isaac, Albertina Schvartz, Héctor Rodriguez y Marcelo Echeverría. A todos, gracias.

FUENTES CONSULTADAS

AFCEA (CAPITULO ARGENTINA)
ASSOCIATED PRESS
BARRY COLLIN
ESTUDIO JURIDICO CHIARAVALLOTTI & ASOCIADOS
CSI - FBI SURVEY
http://www.delitosinformaticos.com
ING. HEDI ENGHELBERG
ING. SEBASTIAN MASANA
INTERPOL
POLICIA FEDERAL ARGENTINA
REVISTA NOTICIAS
TECNIPOL

LUCIANO SALELLAS
AUDITOR EN SEGURIDAD INFORMATICA
SR HADDEN SECURITY CONSULTING
Tel: (0054-0343) 155-121-554
E mail: sr_hadden@hotmail.com
http://www.sr-hadden.com.ar