MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Dirección General de la Policía y de la Guardia Civil
- **GUARDIA CIVIL** –
Dirección Adjunta Operativa
Jefatura de Información

El Uso de Internet por Organizaciones Terroristas

CIBERTERRORISMO

8º Período Ordinario de Sesiones del CICTE

Washington, D.C - 5 a 7 de marzo del 2008

Sumario:

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil
5. Conclusiones

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil
5. Conclusiones

Se debe entender como ***ciberterrorismo*** el empleo generalizado de las tecnologías de la información (TI), por parte de grupos terroristas ó afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como ***instrumento de comisión del delito*** ó como ***acción del delito***.

Se debe desmitificar pero no subestimar la ***amenaza emergente*** que supone Internet.

Modalidades del CIBERTERRORISMO

– Internet como **objeto de ataque** ó acción del delito, (ciberterrorismo estricto)
  - Infraestructuras Críticas.
  - Objetivos Estratégicos.

– **Uso de Internet** para la realización de actividades terroristas (ciberterrorismo amplio)
  - Instrumento.
  - Medio.

Internet como INSTRUMENTO (1)

- Comunicaciones vía e-mail.
  - Correo Anónimo
  - Buzón compartido
- Canales de Chat.
  - Servidores IRC
  - Protocolo cifrado.
- Encriptación.
  - PGP
- Servidores WEB.
  - SSL
  - Autenticación
- Enmascaramiento y Ocultación .
  - Steganografía
  - Alternate Data Stream

Internet como INSTRUMENTO (2)

- Voz sobre IP.
- Dispositivos sin conexión.
  - PDA
  - Movil
- Servicios en PC
- Dominios “seguros”
- Transferencia enmascarada.

Internet como INSTRUMENTO (Experiencia GC)

- Comunicaciones vía e-mail. ▸ **Correo Anónimo**
  - ▸ **Buzón compartido**
- Canales de Chat. ▸ **Servidores IRC**
  - ▸ **Protocolo cifrado**.
- Encriptación. ▸ **PGP**
- Servidores WEB. ▸ **SSL**
  - ▸ **Autenticación**
- Enmascaramiento y Ocultación . ▸ **Steganografía**
  - ▸ Alternate Data Stream
- **Voz sobre IP**.
- Dispositivos sin conexión. ▸ PDA
  - ▸ **Movil**
- **Servicios en PC**
- **Dominios “seguros”**
- **Transferencia enmascarada.**

Internet como MEDIO

- Relaciones y colaboraciones entre organizaciones.
- Guerra psicológica
  - Desinformación
  - Amenazas
- Financiación
- Recluta
- Propaganda
  - Comunicados “oficiales”
  - Mensajes
- Fuente de Información

Internet como MEDIO (Experiencia GC)

- **Relaciones y colaboraciones entre organizaciones.**
- Guerra psicológica
  - **Desinformación**
  - **Amenazas**
- **Financiación**
- **Recluta**
- Propaganda
  - **Comunicados "oficiales"**
  - **Mensajes**
- **Fuente de Información**

Internet como OBJETIVO (1)

Infraestructuras Críticas

Concepto: *«instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos»*
COM (2004) 702 final, 20 octubre

- Economía y Empresa
- Telecomunicaciones
- Servicios Públicos
- Infraestructuras
- Estado y Administración

Internet como OBJETIVO (2)

Peligros que presentan las Infraestructuras Críticas

- *Amplia interconexión entre ellas.*
- *Dependencia tecnológica.*
- *Ataque directo.*
- *Ataque concertado con un atentado convencional.*
- *Posibilidad de efectos en cascada.*
- *Efectos psicológicos amplificadores.*

Internet como OBJETIVO (3)

Medidas de protección

- *Catálogo de Infraestructuras Críticas (CIC)*
- *Red de emergencias (CERT,s y CSIRT,s)*
- *Instituciones de vigilancia:*
  - *Agencia Europea de Seguridad de las Redes y de la Información (ENISA)*
  - *Centro de Ciberdefensa de la OTAN*
  - *Centro Nacional de Protección de Infraestructuras Críticas (PNPIC) –*

CCN-CERT

enisa European Network and Information Security Agency

MINISTERIO DEL INTERIOR
SECRETARIA DE ESTADO DE SEGURIDAD
[CNPIC]

Caso ESTONIA

Primer ciberataque a gran escala contra las infraestructuras TIC de un país, vía Internet.

Caso ESTONIA

Introducción:

- País pionero en Administración Electrónica:
  - ✓Voto en elecciones a través de Internet.
  - ✓80 % declaraciones de la renta y pago de impuestos
  - ✓65 % población usa internet regularmente.
  - ✓Gobierno solo usa documentos electrónicos, no papel.
  - ✓70 % población posee Tarjeta de Identidad Electrónica
- También conocida por e-Stonia.
- Población de 1’35 millones de habitantes.
- Independizada de la URSS en 1991.
- Su economía es de las más pobres de Europa.

Caso ESTONIA

Síntesis:

Desencadenante:

- ✓Traslado estatua homenaje a soldados rusos caídos en IIGM !

Duración:

- ✓¡Dos semanas!,
- ✓del 27/04/07 al 11/05/07

Mayor intensidad:

- ✓9 de Mayo.
- ✓Web del gobierno pasa de recibir 1.500 visitas ***al día*** a 1.000-1.500 ***por segundo***.

Consecuencias:

- ✓El **país tuvo que "desconectarse" de Internet** quedando AISLADO del resto del Mundo.

Caso ESTONIA

Desarrollo:

Objetivos atacados:

- ✓Organismos públicos (gobierno, parlamento, etc.)
- ✓Entidades financieras (banca electrónica)
- ✓Medios de comunicación (ediciones digitales)
- ✓Empresas de Telecomunicaciones (isp, servidores correo)

Primera fase:

- ✓En foros rusos aparecen llamamientos patrióticos con explicaciones para realizar ataques sencillos.

Segunda fase:

- ✓**Oleada de 128 ataques DDoS** desde numerosas botnets.
- ✓Llegan a congregar cerca de **1 MILLÓN** de zombies atacando.

Caso ESTONIA

Desarrollo:

Tercera fase:

Defacements (cambios de apariencia) con propaganda rusa en sitios atacados.

Caso ESTONIA

Desenlace:

Petición de ayuda a Organizaciones y CERTs:

- ✓OTAN (invocan art. 5 del Tratado)
- ✓CERTs europeos
- ✓US-CERT

Soluciones fallidas:

- ✓Desactivar botnets origen ataque. Bullet-proof hosting
- ✓Solicitud a ISP's internacionales filtrado ataques en origen
- ✓Filtrado IP atacantes en nodos enlace entrada al país

Solución definitiva:

- ✓**Desconexión del país del resto del mundo**, ya que 99% tráfico procedía del exterior.

Caso ESTONIA

Enseñanzas:

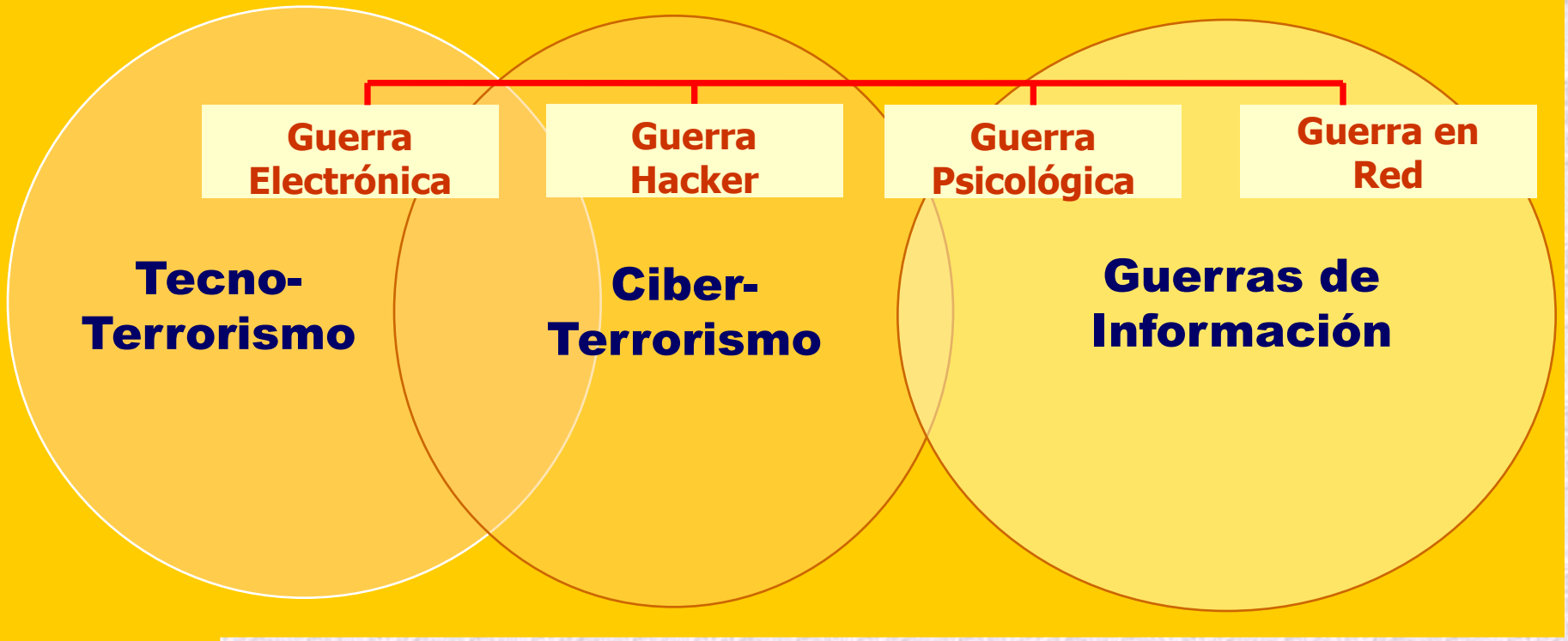
Peligrosidad creciente de las Botnets:

- ✓Cada vez existen más
- ✓ Controlan más PC's
- ✓Acumulan mas ancho de banda
- ✓Dificultad para combatirlas (entorno distribuido)
- ✓Muy peligrosas caso ataque a infraestructuras críticas
- ✓Susceptibles uso terrorista:

Cuando confluyan quienes tienen los conocimientos y los medios con quienes tienen las motivaciones ideológicas.

Ciberterrorismo

Un ataque, o amenaza de ataque, sobre dispositivos electrónicos, de comunicaciones o computadoras para desestabilizar infraestructuras civiles en soporte de propósitos políticos



Yael Shahar
Institute for Counter-Terrorism

Ciberterrorismo frente a Terrorismo tradicional

- **VENTAJAS:**
  - Seguridad: - No riesgo personal
    - Anonimato
  - Ámbito geográfico ilimitado
  - Gran repercusión mediática (Propaganda)
  - Relación coste-beneficio: **OPTIMA**
- **INCONVENIENTES:**
  - Amplios conocimientos técnicos.
  - Falta de dramatismo.
  - Falta de control de los resultados alcanzados.

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil
5. Conclusiones

Creciente inquietud en el AMBITO INTERNACIONAL (1)

- ***PEPIC**: Plan Europeo de Protección de infraestructuras Críticas*
- ***CCC:** Conferencia Internacional de Delitos Informáticos y Ciberterrorismo (Departamento de Defensa de los EEUU)*
- ***EWPTIC:** Grupo Europeo de Delitos relacionados con las Tecnologías de la Información (INTERPOL)*
- ***ASEM:** Grupo de relaciones Económicas Asia-Pacífico (Corea)*
- ***HTCEM:** Reunión de Expertos en Delincuencia de Alta Tecnología (EUROPOL)*

Creciente inquietud en el AMBITO INTERNACIONAL (2)

- ***Curso:*** *Ciberterrorismo (OTAN)*
- ***Seminario:*** *Uso de Internet por Grupos terroristas (EUROPOL)*
- ***G-8:*** *Reunión sobre Ciberdelincuencia y Ciberterrorismo (Moscú).*
- ***BOTNET****-Grupo de Trabajo: INTERPOL-Microsoft*
- ***CICTE.*** *Conferencias sobre Ciberseguridad y Ciberdelincuencia.*
- ***OSCE.*** *Seminarios sobre el uso de Internet por organizaciones terroristas.*
- ***COMISION EUROPE.*** *Seminarios sobre Análisis de ataques a gran escala a través de Internet .*

❷ Visión Internacional

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil
5. Conclusiones

La organización terrorista ETA, tradicionalmente ha tenido entre sus objetivos repetidores de radio y televisión, subestaciones eléctricas, infraestructura ferroviaria y aeroportuarias, entidades financieras, fabriles y de comercio e instalaciones de los operadores de telefonía; ¿por qué no trasladar estos objetivos al entorno ciberterrorista?, nodos de telecomunicaciones y servidores raíz, infraestructura telemática de medios de difusión, empresas e instituciones, etc...

Se constata una presencia creciente de elementos integrantes de la Izquierda Abertzale en Internet y su presencia ya no es tanto cuantitativa como cualitativa; la proliferación de páginas afines al MNLV es evidente.

Pudiendo incrementar la lista con otros objetivos tradicionales de GRAPO (Edificios Oficiales, ETT,s, Sedes del Ministerio de Hacienda e INEM, etc...)

Algunos grupos de ideología radical se están enmascarando y están utilizando a algunos colectivos encuadrados en los denominados grupos antiglobalización; con lo que se está generalizando su presencia y actividad en Internet , utilizando como laboratorio diversas actividades de resistencia o desobediencia de estos últimos, como por ejemplo las denominadas "sentadas virtuales".

Desde sus orígenes, algunos grupos de defensa de los animales vienen utilizando Internet como plataforma de difusión de su filosofía, fomentar acciones de sabotaje y reivindicación de las mismas, todo ello bajo la franquicia del Frente de Liberación Animal (FLA). Estas acciones se encuadran bajo el concepto de ECOTERRORISMO.

Los grupos islamistas radicales utilizan con gran profusión y múltiples fines Internet, destacando sobremanera la actividad alrededor de la denominada YIHAD INFORMATIVA y el apoyo a la financiación y el reclutamiento.

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil
5. Conclusiones

GRUPO DE CIBERTERRORISMO

- Dependiente de la Jefatura del Servicio de Información
- Encuadrado en la Unidad Central Especial nº3
- Forma parte del Grupo Técnico Informático
- Atiende al Area de Responsabilidad Informativa de: Tecnologías de la Información y las Comunicaciones.
- Concepción Teórica: Plan Especial 2000
- Primeros recurso humanos y materiales: año 2002
- Inicio de Operatividad: año 2003

1. Concepto de Ciberterrorismo
2. Visión Internacional
3. Visión Nacional
4. Respuesta de la Guardia Civil

5 Conclusiones

- Internet es VULNERABLE
- Internet como INSTRUMENTO terrorista: realidad
- Internet como MEDIO terrorista: realidad
- Internet como OBJETIVO terrorista: posibilidad
- Ciberterrorismo: **AMENAZA EMERGENTE**

En el momento que crucen sus caminos los entornos hacker y los grupos terroristas dejaremos de hablar de amenazas para hablar de realidades.

MUCHAS GRACIAS

Unidad Central Especial - 3
Grupo Técnico Informático
CIBERTERRORISMO
ciberterrorismo-go@guardiacivil.es