Título Ciberguerra y Ciberseguridad, las nuevas amenazas del Siglo XXI

Tipo de Producto Material Didáctico

Autores Rubbi, Lautaro

Código del Proyecto y Título del Proyecto

A17S28 - Ciberseguridad, Ciberguerra y Deep Web, las nuevas amenazas del Siglo XXI. Aproximación al caso chino 2010 - 2016

Responsable del Proyecto

Rubbi, Lautaro

Línea

Agenda Internacional

Área Temática

Ciencias Políticias y RRII

Fecha

Junio 2017

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

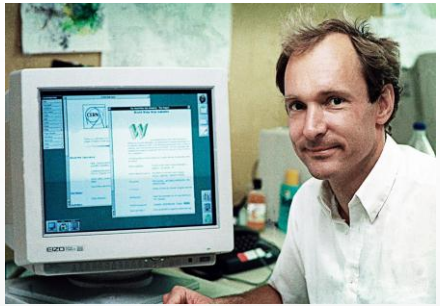
UADE Fundación UADE

Ciberguerra y Ciberseguridad, las nuevas amenazas del Siglo XXI

Gobierno y Relaciones Internacionales

Introducción

1844 → Primer telégrafo -- 1858 → Primer cable oceánico



23 de Agosto de 1991 → Se “crea” la World Wide Web

Jun, 2016 → 3,611 millions → 49.2 % de la población mundial

Más de 1100 millones de páginas web

Internet of Things (IoT)

Nuevo campo militar. El quinto dominio

Escaso conocimiento y repercusión académica

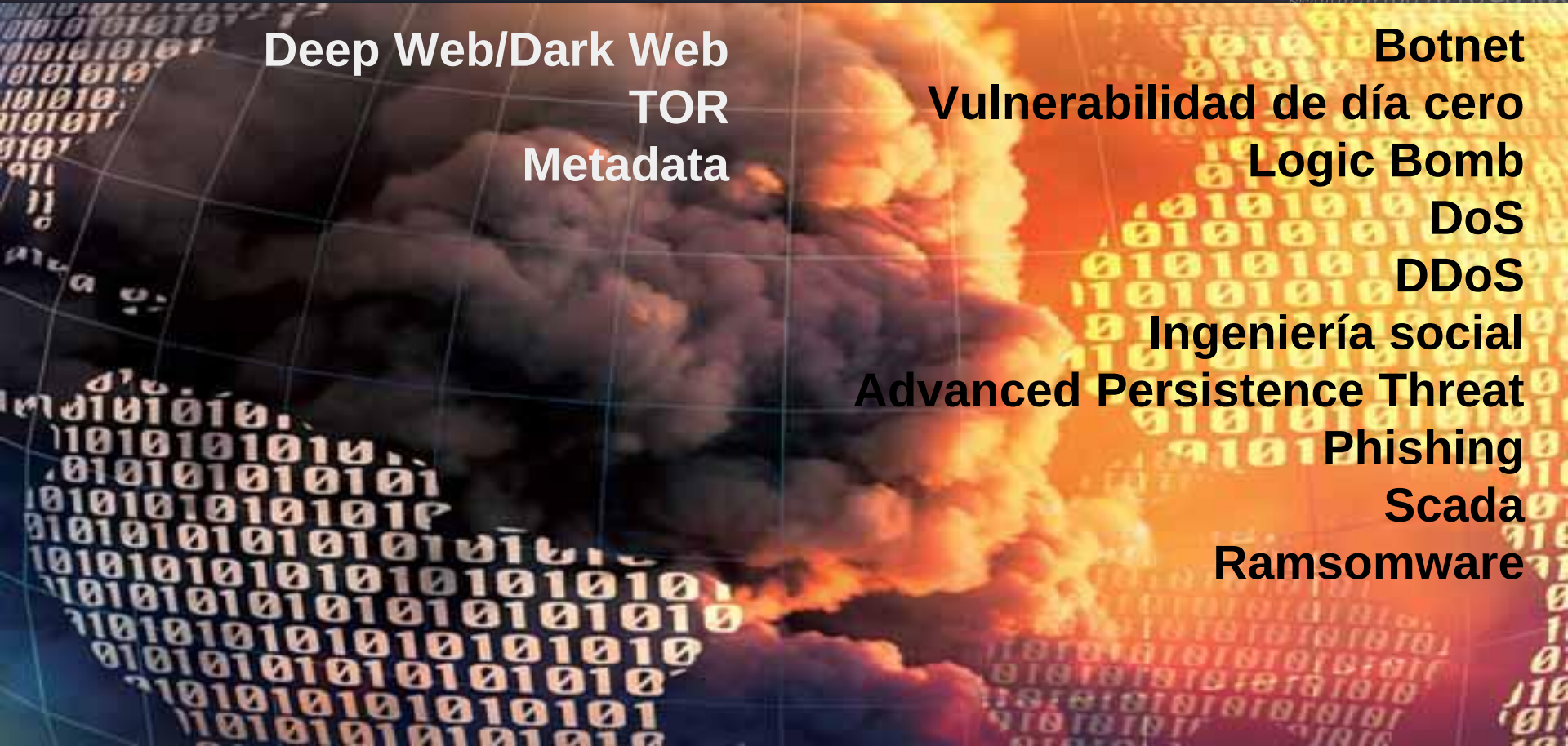
Difusión de poder

Nuevas amenazas y actores
Capacidades diferenciadas

- Ciberguerra
- Multi-Domain Operations
- Ciberespionaje
- Hacktivismo
- Ciberterrorismo
- Cibercriminalidad

Arma de disrupción masiva

Términos clave



Deep Web/Dark Web
TOR
Metadata

Botnet
Vulnerabilidad de día cero
Logic Bomb
DoS
DDoS
Ingeniería social
Advanced Persistence Threat
Phishing
Scada
Ramsomware

Algunos de los principales debates

¿Quién maneja internet?
¿Libertad o control?
¿Libertad o seguridad?
Soberanía
Atribución - Sponsoreo
Disuasión
¿Cyberwar o Competencia “legítima”?
¿Cyberwar o Cibercrimen?
¿Un ciberataque es un ataque?
“How do we know we are at war?”
¿Enfoque defensivo u ofensivo?

Principales actores

Estados Unidos: Apoyo militar
China: Espionaje
Rusia: Disrupción
Irán
Israel
Unión Europea
Corea del N y del S

Aspectos Legales

- Ciberespacio
  - Regulación
    - Autorregulación
      - ventajas
      - desventajas
    - Heterorregulación
      - ventajas
      - desventajas
  - Vacío Legal

Principal Normativa Vigente

Naciones Unidas:

- **Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001)**. Se **invita** a los Estados Miembros a que tomen en cuenta las medidas propuestas, al elaborar leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos
- **Resolución de la Asamblea General 57/239 (2002)** para la creación de una cultura global de ciberseguridad
- **Resolución de la Asamblea General 58/199 (2004)** para la protección de las infraestructuras de información. Se persigue **estimular** el desarrollo de normas de conducta en el ciberespacio que sirvan para la promoción del desarrollo socioeconómico y el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información.

Principal Normativa Vigente

- ★ **OTAN:** Conferencia de Praga (2002). Cumbre de Lisboa (2010) > Nueva política de ciberdefensa.

- ★ **Consejo de Europa:** Convenio del Consejo de Europa sobre Ciberdelincuencia/ Convenio de Budapest (2004) > primer tratado sobre delitos informáticos mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre Estados.

- ★ **Unión Europea:** Una agenda digital para Europa (2010) en el marco de los objetivos para Europa 2020.

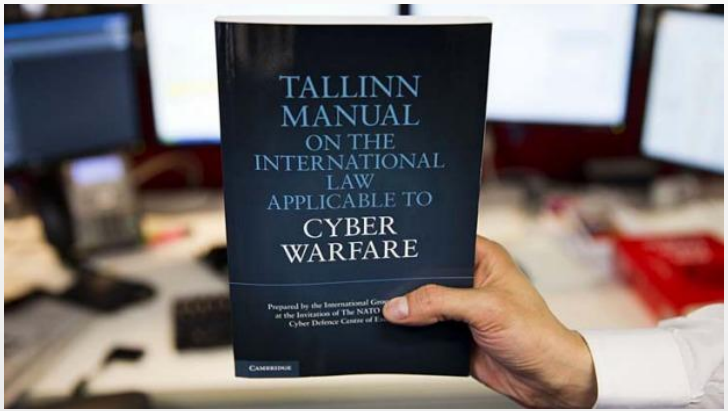
- ★ **EEUU- CHINA:** Negociaciones y posterior acuerdo para buscar combatir delitos cibernéticos (2015)

Ciberguerra y Derecho Internacional Humanitario

★ **<u>Manual de Tallin</u>** como herramienta para los juristas para la regulación del ciberespacio.

Aspectos claves:

a) Ciberataque y conflictos del DIH
b) Soberanía y responsabilidad
c) Uso de la fuerza
d) Ataque armado
e) Legítima defensa. Inminencia e inmediatez
f) Principio de necesidad y proporcionalidad
g) Participación directa en las hostilidades



Ciberguerra y Derecho Internacional Humanitario

Jus ad bellum y ciberguerra:

- ★ Severidad
- ★ Inmediatez
- ★ Directo-Indirecto
- ★ Invasividad
- ★ Mensurabilidad
- ★ Legitimidad
- ★ Responsabilidad
- ★ Combatiente- No combatiente
- ★ Necesidad militar
- ★ Proporcionalidad
- ★ Armas indiscriminadas
- ★ Daños
- ★ Traición
- ★ Neutralidad

Principales Casos

Estonia 2007

- **Fecha**: Abril 2007
- **Atacado**: República de Estonia
- **Sospechoso de haber realizado el ataque**: Federación de Rusia
- **Blanco**: Páginas oficiales del gobierno, canales de noticias y bancos.
- **Motivo**: Político.

Georgia 2008

- **Fecha**: Agosto 2008
- **Atacado**: Georgia
- **Sospechoso de haber realizado el ataque**: Federación de Rusia
- **Blanco**: Páginas oficiales del gobierno, canales de noticias y bancos.
- **Motivo**: Político.

Corea del Norte - Sony

- **Fecha**: Noviembre 2014.
- **Atacado**: Sony Pictures.
- **Sospechoso de haber realizado el ataque**: Corea del Norte.
- **Blanco**: Documentos sensibles: películas sin estrenar, mails personales, etc.
- **Motivo**: Político. Estreno pelicula “The Interview.

Snowden

- **Fecha**: 2013 - 2015.
- Divulgación de documentos del proyecto de vigilancia PRISM.
- Héroe o traidor.
- Doble moral de Estados Unidos.

Stuxnet

“Realmente nunca hemos visto algo así antes y el hecho de que pueda controlar el funcionamiento de una maquinaria física es inquietante”

- **Fecha**: Junio 2010 (descubierto).
- **Atacado**: Irán.
- **Sospechoso de haber realizado el ataque**: Estados Unidos e Israel.
- **Blanco**: Infraestructura física sensible. Base nuclear Natanz.
- **Motivo**: Político.

Conclusiones y escenarios futuros

Otros casos: Ghostnet - Operación Aurora - Nanhaishu - Flame - Gasolineria en Siberia - China y los F-35 - Minado de Bitcoins - Código de barras en el ejército

Ámbito que requiere de forma urgente de cooperación internacional

¿Ataque? ¿Disuasión? ¿Respuesta? La decisión final es arbitraria

Dificultad por las distintas visiones sobre el ciberespacio de los actores

¿Seguridad o privacidad? Un eterno debate

Importancia de la Ciberseguridad


Mapa de ciberataques en tiempo real