Cyber&Law

Juan Pablo Salazar H

juan.salazar@cyberlaw.digital

ESTADO DE LA CIBERSEGURIDAD Y CIBERGUERA

Contexto Latinoamérica

Juan Pablo Salazar H
CyberLaw
www.CyberLaw.digital
juan.salazar@cyberlaw.digital
juansala@ucm.es

Cyber&Law

LA IMPORTANCIA DEL ESPACIO DIGITAL

“Estamos en la mitad de una importante revolución, y estamos solo iniciando a entender sus implicaciones”.
Daniel J. Solove. – The Digital Person

La espacialidad digital

ESPACIO DIGITAL
"Red de nodos interconectados"
(Castell)

ESPACIO DIGITAL
VS
ESPACIO FÍSICO

- Es una **reducción del lenguaje artificial computacional,** que genera que todo lo que percibimos en el mundo digital sea representado por números, lo cual genera como consecuencia una antítesis del lenguaje natural.
- El uso de robots será generalizado y conllevará aún más a un natural remplazo de las labores humanas por labores robóticas, harán que la base de la pirámide cambie y los robots tengan un masivo lugar en ésta. [Visión 2080 Friedmann]
- Es esa **imbricación entre lo natural y lo artificial** en la que se hace necesario profundizar. [Milton Santos]

Cyber&Law

La configuración de un nuevo espacio de poder

- Reevaluación de fronteras
- Interdependencia de las economías nacionales globalizadas
- Expansión de los medios de comunicación y de transporte
- Se ha generado transformaciones del mercado y sus relaciones de producción.
- El espacio digital, cuenta con sus propias reglas, protocolos y grupos de interés ajenos a las realidades del mundo regido por los Estados.

Cyber&Law

¿CÓMO SE MIDE EL PODER DE UN PAÍS?

“LA CIENCIA Y LA TECNOLOGÍA HAN AGREGADO UNA DRAMATICA NUEVA DIMENSIÓN DEL PODER DE LOS RECURSOS”

Clarke, Richard (2012)

Cyber&Law

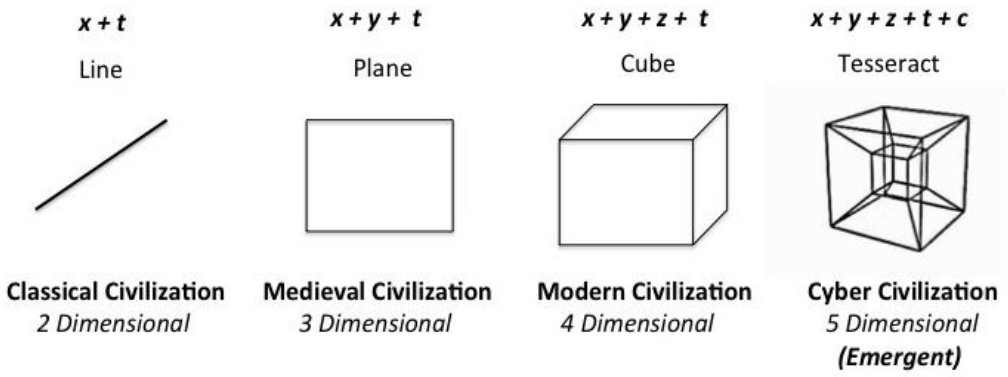
LA GUERRA MULTIDIMENSIONAL

The Economist

“Cyberspace has become the fifth domain of warfare, after land, sea, air and space”

(2010)

Cyber&Law



- **DIMENSIÓN PLANA:** Suelo y mar
- **DIMENSIÓN TRIDIMENSIONAL:** + Uso del aire y el espacio ultraterrestre (incluido cuerpos celestes)
- **DIMENSIÓN GEOMÉTRICA:** + el espacio digital donde no ha restricciones espacio-temporal, dado que es un espacio artificial.

Robert J. Bunker, 'Fifth Dimensional Battlespace: Terrorism and Counter-Terrorism Implications | TRENDS' <http://trendsinstitution.org/?p=1004> [accessed 14 October 2015].

¿QUÉ ES Y QUÉ NO ES CIBERGUERRA O CIBERSEGURIDAD?

¿Qué es un ciberincidente, qué es una ciberoperación?

Clarke, Richard (2012)

Cyber&Law

¿Qué es ciberguerra?

Ciber Guerra
(Ronfedt y Arquilla, 20 años)

Acciones efectuadas por una Organización-Nación-Estado con el propósito de penetrar los sistemas informáticos y redes de computadores de otra Nación-Estado, con el propósito de causar daños o interrupción de los mismos. (Clarke, 2004)

Intrusión en sistemas privados estratégicos, debido que pueden poner en riesgo el funcionamiento económico o social.

Manifestaciones

- Espionaje
- DoS – Denial of service atack [reprogramación tráfico]
- Sabotaje
- Hurto electrónico de material estratégico o de interés nacional [patentes]
- Toma de control instalaciones esenciales [Energía, Finanzas…]

Ciberoperación desarrollada principalmente por organizaciones cuyo blanco son la infraestructuras redes de información, y sistemas de información.

Richard A. Clarke and Robert K. Knake, *Cyberwar* (New York: HapperCollins, 2010).

Cyber&Law

¿Qué es ciberseguridad?

"Herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno"

Cyber&Law

Unión Internacional de Telecomunicaciones UIT, 'Recomendación UIT-T X.1205: Seguridad En El Ciberespacio – Ciberseguridad' (Geneva: Unión Internacional de Telecomunicaciones, 2008)

¿Qué es ciberseguridad?

Eventos que afectan la confidencialidad, integridad y disponibilidad de los datos de los individuos o empresas

Finalidad: Mitigación de riesgos y la disminución de delitos a partir del uso de sistemas IT o TIC

- Protección de los usuarios
- Protección infraestructuras críticas
- Preparación del Estado
- Datos transfroterizos

TARGET:

Sistemas de control que activan o monitorean aspectos industriales o de control
Energía, Telco, Agua, Finanzas, Transporte.

Cyber&Law

Algunos datos - cíbercrímenes

- Costos ascienden a una cifra entre **US$ 375 y US$ 575 millones** de dólares (Estudios CSIS – McAfee citados por BM)
- En 2021 se estima el costo en 1 trillón de dólares
- Costo de solo un incidente de ciberseguridad puede ascender en promedio en US $861.000 (grandes empresas) y US $86.500 (Pymes) – Kaspersky (2016).
- 44% de las pymes tienden a pagar rescate
- 27% de las grandes empresas tienden a pagar rescate
- Los ciberincidentes se trasladan de los PC y Servidores a las cosas (automóviles, cajeros, cámaras conectadas a internet, monitores de bebé, equipos médicos, máquinas venta alimentos)
- Uber(2016) pagó $100.000 x ranson (54 millones cuentas y 100 mil conductores US)
- Ataque a Equifax (2017) generó reducción en su valor en 34%:
  500.00 clientes afectados

Cyber&Law


LA HISTORIA DE LAS CIBEROPERACIONES
ATTACK ORIGINS
COUNTRY
Saudi Arabia
China
United States
Australia
Netherlands
South Korea
Russia
Taiwan
Germany
Venezuela
ATTACK TYPES
PORT SERVICE TYPE
46 137 unknown
23 25 smtp
22 50864 unknown
14 50856 unknown
11 5900 vnc
9 445 microsoft-ds
8 1500 vlsi-lm
7 138 unknown
7 515 printer
6 3306 mysql
ATTACK TARGETS
COUNTRY
104 United States
61 Saudi Arabia
25 France
16 United Arab Emir...
3 Russia
3 Spain
1 Mil/Gov
1 Cyprus
1 Bulgaria
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
19:55:43.209 National Computer Systems Co. 46.151.210.66 Riyadh, SA Riyadh, SA unknown 137
19:55:43.220 National Computer Systems Co. 46.151.210.138 Riyadh, SA Riyadh, SA unknown 137
19:55:43.508 National Computer Systems Co. 46.151.215.82 Riyadh, SA Riyadh, SA unknown 137
19:55:43.832 Riskiq 64.125.239.236 San Francisco... De Kalb Juncti... http-alt 8000
19:55:44.190 Telecom Italia S.P.A. 82.57.200.102 Milan, IT Aix-En-Proven... smtp 25
19:55:44.502 Joint Stock Company Teo Lt Ab 82.135.246.8 Vilnius, LT Lynnwood, US microsoft-ds 445
19:55:44.869 Plusserver Ag 85.25.43.94 Cologne, DE Lynnwood, US unknown 20547
19:55:45.199 Chinanet Guangdong Province Network 183.54.200.203 Guangzhou, CN Lynnwood, US unknown 50864
19:55:45.542 Chinanet Jiangsu Province Network 222.186.34.160 Nanjing, CN Moscow, RU unknown 9200
19:55:45.851 National Computer Systems Co. 46.151.208.26 Riyadh, SA Riyadh, SA vlsi-lm 1500

La historia de las ciberoperaciones

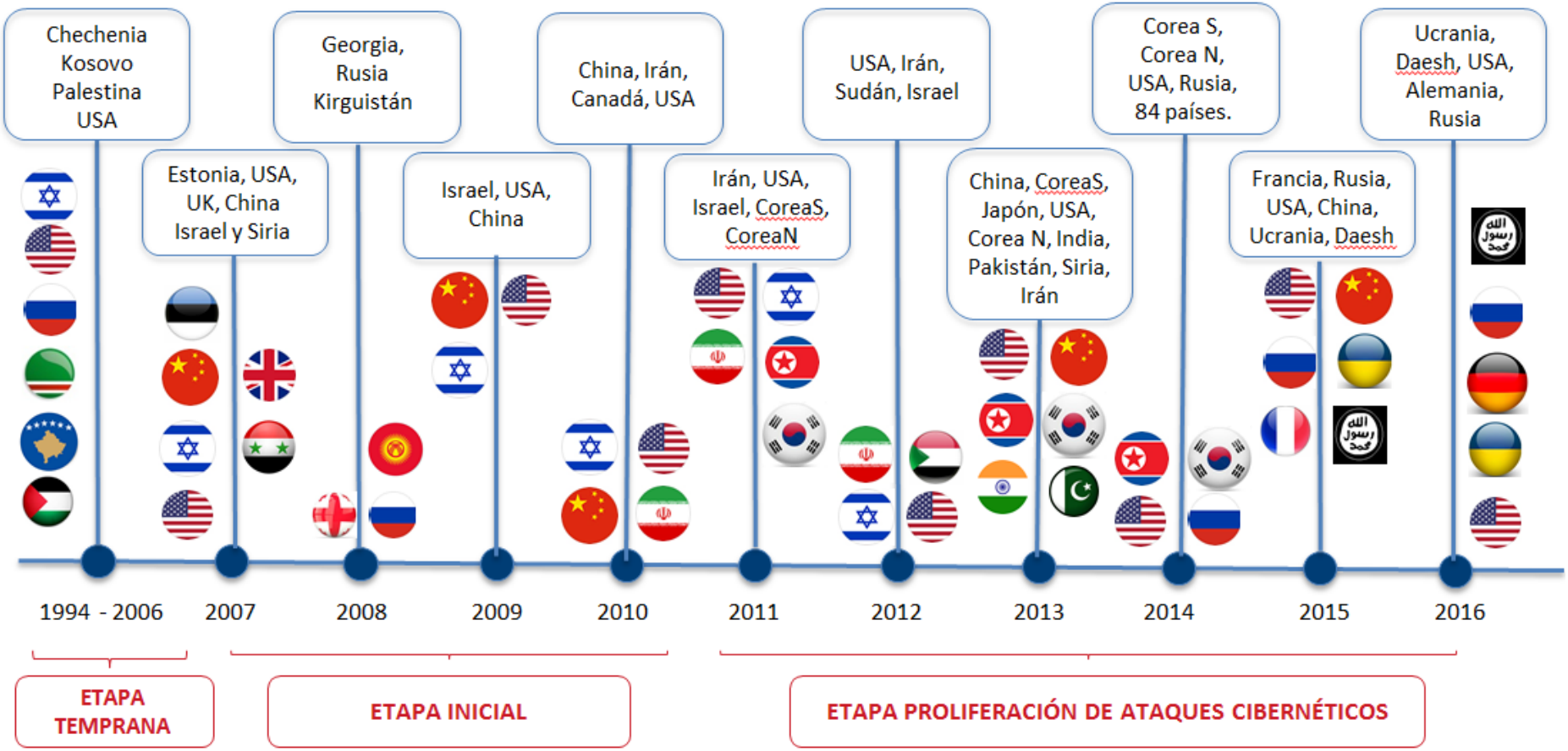
ETAPAS

TEMPRANA	INICIAL	PROLIFERACIÓN	INFLEXIÓN
1994-2006	2007-2009	2010-2016	Desde 2017

Cyber&Law

Fuente: Gartner, 2015

Timeline de la guerra digital



Cyber&Law

Ataques a Estonia

JUN OSAWA, 'Is Cyber War Around the Corner? Collective Cyber Defense in the Near Future', *Brookings Research*,
BBC News, 'Tallinn Tense after Deadly Riots',
Michael Schmitt, *The Law of Cyber Targeting*
TOMAS MADAR, 'Limiting Cyber Arms: Testing the Provisions of the Chemical Weapons Convention for the Cyber Domain'
Financial Times, 'Timeline: Cyberwarfare and Cybercrime',
OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Reccommendation and Companion Document.*

Cyber&Law

Ataques a Estonia

Principales manifestaciones:

Denegación Servicios

Se estimó que cerca de un millón de computadores sirvieron de atacantes y ubicados en 178 países, se generó incluso que “los servicios bancarios online pertenecientes a los dos grandes bancos de Estonia estuvieren paralizados”.

Flooding

Como resultado, Estonia “perdió 3 millones de euros, alrededor de 4 millones de dólares”, perdiendo el “1.85% de su PBI de 2007”

Fuentes:
OSAWA.
TIKK, KASKA and VIHUL (2010). Op. cit.
CAREY CASIMIR C., ‘The International Community Must Hold Russia Accountable for Its Cyber Militias

Fuente: Varias

Cyber&Law

Irán: Ejército Ciber y Olimpic Games

BEN ROONEY, 'A History of the World in 15 Viruses.', *Wall Street Journal*. OECD. Digital Security Risk Management for Economic and Social Prosperity (2015). BARBARA; SLAVIN AND JASON HEALEY, *Iran: How a Third Tier Cyber Power Can Still Threaten the United States.* OTÁN.

Cyber&Law

Ucrania

- **País más afectado en los últimos 2 años**

- En 2015 un virus llamado “Serpiente (en español)” **atacó objetivos diplomáticos** para hurto de información estratégica.

- En 2015 su **sistema electoral fué bombardeado** con ataques distribuídos de denegación de Servicio, tratando de paralizar el Sistema en pleno período de eleccciones

- A finales del 2015, **apagón eléctrico en la región de Ivano-Frakivsk** que ocasionó que 80 mil hogares se quedaran sin energía

- A comienzos del 2016 **los sistemas de control aéreo del Aeropuerto de Kiev**, fueron atacados

- En julio del 2017, **sufren ataques Petya**

Cyber&Law

Otras ciberoperaciones

20 ATAQUES HASTA 2016
+20 ATAQUES DESDE 2017

Principales manifestaciones:

- Denegación Servicios
- Redes sociales
- Hurto Información confidencial
- Ataques Infraestructura
- Hurto Patentes
- Apagón Eléctrico
- Malware
- Hurto Información Comercial Estratégica
- Ataque Planta Nuclear

Cyber&Law

Latinoamérica

TOP 5 PAÍSES MÁS ATACADOS

- Brasil 25.13%
- México 15.53%
- Venezuela 11.91%
- Argentina 9,63%
- Colombia 8.05%

Otros datos:

- BRAZIL: Al año 30 millones brasileros afectados
- COLOMBIA: 198 millones de ataques al año. 542.465 ataques diarios (financiero, telecomunicaciones, gobierno, energético, industria y retail)

Cyber&Law

México 2018

Ataque sistema financiero:

- 300 millones pesos mexicanos en riesgo (US $15 millones)
- 3 Bancos impactados: Banorte, Citibanamex, Banco Bajío
- 191 quejas de usuarios
- No se comprometió a SPEI

Cyber&Law

Incidentes famosos

Check in/out bloqueado

RANSONWARE

- 1500 euros extorsión
- Bloqueo sistema de reservas del hotel

Cyber&Law

A través de la pecera

DATA BREACH

- Encontraron vulnerabilidad a través de los termostatos de las peceras
- Hurtaron bases de datos sensibles, incluyendo clientes VIP

Cyber&Law

Carros hackeados

DATA BREACH

- Tomaron el sistema de entretenimiento y detuvieron el vehículo [prueba]
- Tesla otro vehículo hackeado bajo test

[https://youtu.be/c1XyhReNcHY]

Cyber&Law

Aspiradora peligrosa

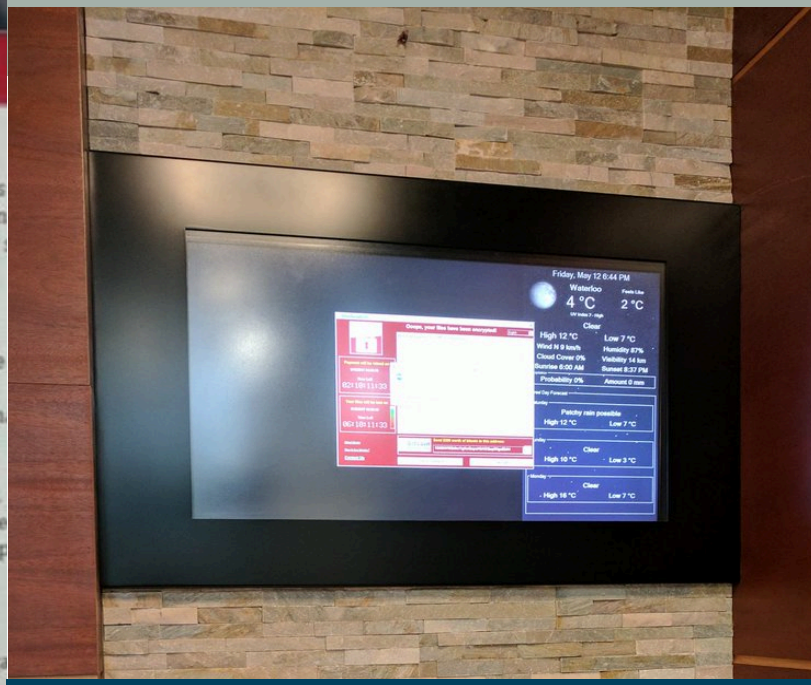
ESPIONAJE DE ALTO NIVEL

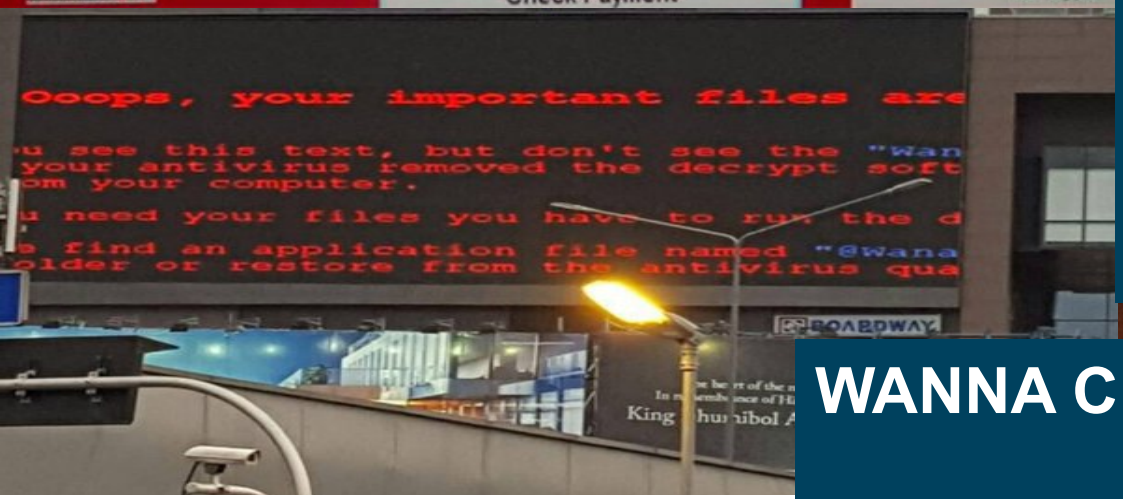
- Construye plano de casa/oficina

PHISHING

- Phishing a través de cupones falsos

Cyber&Law





RESUMEN

- 300.000 computadores
- + 250.000 víctimas
- 85 víctimas en Colombia
- Atacados: + 150 países
- Atacante: Corea del Norte

WANNA CRY

RESUMEN

- 100.000 máquinas encriptadas
- Atacados: Ucrania, USA (principalmente)
- Impactos en Ucrania
  - Cajeros fuera de servicio
  - Pantallas computador
  - Oficinas postales, gobiernos y bancos
  - Tarjetas del Metro de Kiev
  - Chernobyl sensores radiación afectados
- Impactos USA:
  - DLA Piper, firma abogados
  - Merck, gigante de medicamentos

¿DAY ZERO?

Eighth Army G2X
COUNTERINTELLIGENCE ADVISORY
as of 21 September 2017

False NEO Evacuation Alerts

On Thursday, 21 September 2017, multiple reports indicated a fake NEO alert had been issued to multiple service members and spouses in the Republic of Korea.

USFK DID NOT ISSUE a "Real World Noncombatant Evacuation Operation Order". This false message has been delivered via Facebook and SMS messages.

What should you do?

Always confirm NEO-related information with your NEO Warden.

Do not accept information from unconfirmed sources and verify official announcements with your appropriate chain of command.

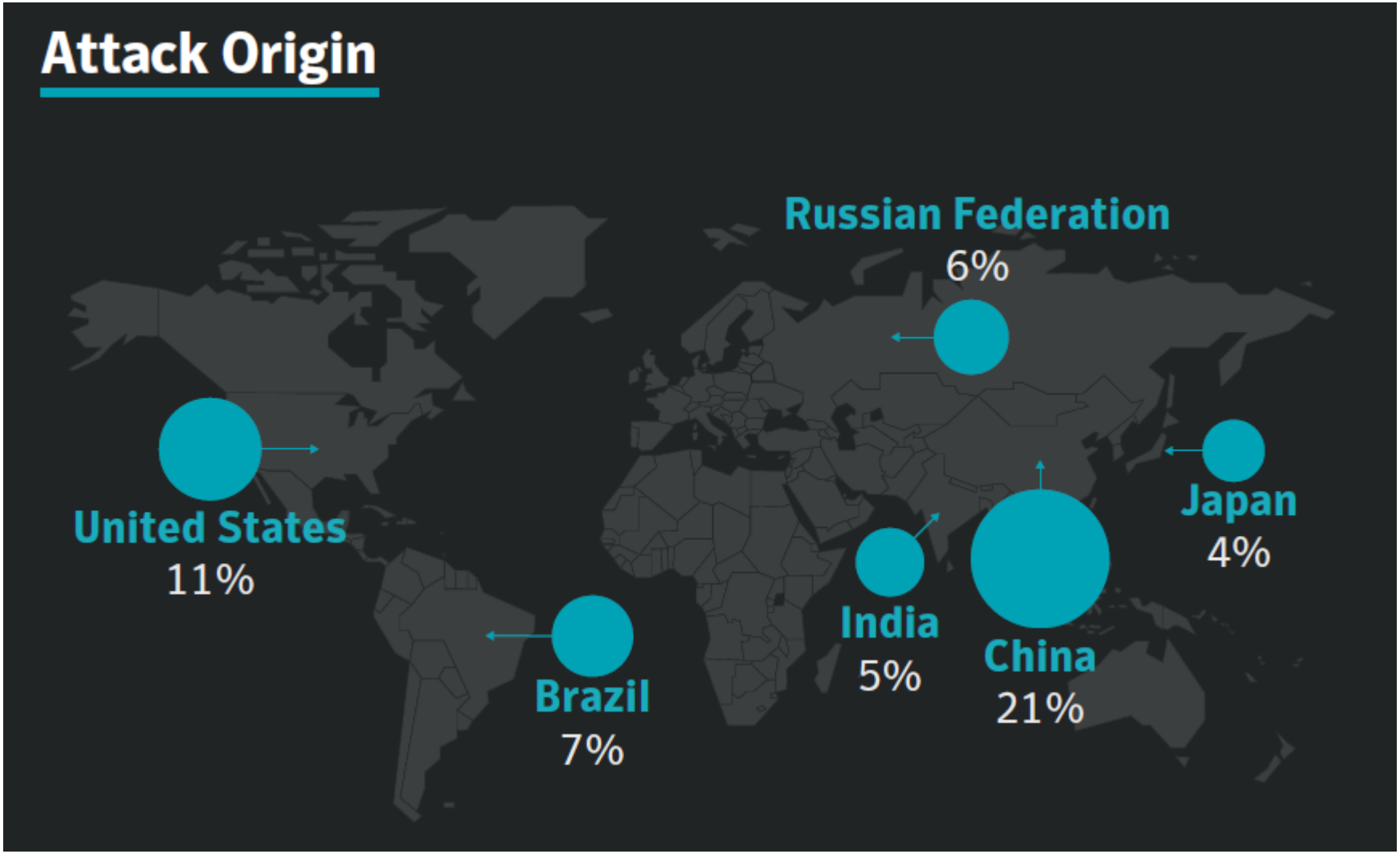
Do not click any links or open any attachments included in unexpected correspondence. Verify the legitimacy of the sender.

If you received the alert depicted in this advisory or anything similar, please contact US Army Counterintelligence via the reporting hotlines listed to the right.

See something, say something!

Reporting Hotlines:
0503-323-3299
010-3100-0171

Origen de los ataques 2017



Estado actual

ESTRATEGIA CYBER:
solo la tienen 6 países

INFRAESTRUCTURA CRÍTICA: 18 países no la identifican

COORDINACIÓN
24 países no cuentan con mecanismos

CONTROL DE MANDO
Solo en 7 países

CERT
Todos los países

Cyber&Law

MAPA CYBERSEGURIDAD 2017

	Argentina	Brasil	Bolivia	Chile	Colombia	Costa Rica	Panamá	Perú
Estrategia	✗	☑ 2010	✗	✗	☑ 2011	☑ 2012	☑ 2013	✗
Leyes penales	☑ TODOS LOS PAÍSES CUENTAN CON NORMATIVA PENAL SOBRE DELITOS INFORMÁTICOS							
CERT	☑ 1994	☑ 2004	☑ 2015	☑ 2004	☑ 2011	☑ 2012	☑ 2011	☑ 2009
Conv. de Budapest	Invitación	✗	✗	Invitación	Invitación	☑ 2018	☑ 2014	Invitación
Agencia responsable	Jefe Oficina Gabinete Presidencial	Departamento Seguridad de la Información y las Comunicaciones	ADSIB Agencia para el Desarrollo de la Sociedad de la Información	Ministerio del Interior y Seguridad Pública SUBTEL	MinTIC MinDefensa	Ministerio Ciencia Tecnología y Telecomunicaciones	Autoridad Nacional de Innovación Gubernamenta006C	ONGEI Oficina Nacional Gobierno Electrónico e Informática

Cyber&Law

“QUE LOS PROGRESOS DE LA CIVILIZACIÓN DEBEN TENER POR EFECTO ATENUAR EN CUANTO SEA POSIBLE LAS CALAMIDADES DE LA GUERRA”

Declaración de San Petersburgo de 1968 con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra.

RETOS PARA LAS EMPRESAS Y LOS GOBIERNOS

Cyber&Law

¿En dónde estamos?
ETAPAS DE LA CIBERSEGURIDAD

ETAPA 1 CERT	ETAPA 2 PENAL	ETAPA 3 ESTRATEGIA	ETAPA 4 REGULACIÓN**
Desde 1988	Desde 2000/2001	Desde 2007	Desde 2016
Gusano Morris Hasta años recientes	Era Bush (Condoleezza Rice) /Obama Internet Freedom Convenio de Budapest	Hechos de Taillin Incidencia de la OTÁN	Incremento de la Regulación (Wanna Cry/ Petya)

Cyber&Law

21 Países quieren incrementar regulación

- Se expide Directiva UE 2016/1148 para garantizar nivel común de seguridad de las redes y sistemas de información

- Inicia NIS – Network and Information Security. Mayo 2018: Requerimientos de Seguridad para operadores y DSP (Digital Services Providers). Reportes de incidentes por operadores y DSP

- Se espera la creación de la Agencia Europea de Cyberseguridad, y la creación de estándares comunes obligatorios para las empresas

- Singapur. Se espera Ley de Ciberseguridad en 2018

- Primeras sanciones a iraníes que hackearon Wall Street. (Lista OFAC / Clinton)
- Presiones Cámara de Representantes: H.R.3878 - Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act

Fuente: Varias

Cyber&Law

INCREMENTO REGULACIÓN 2017-2018

- Ley para elecciones 2018 sobre redes sociales

- Autoriza el apagón digital con notificación gubernamental en asuntos de Emergencias Públicas o Seguridad Pública.

- Bill 2018 Security of Critical Infraestructure

OTROS:

- Canadá: Bill C-59 Act Respecting National Security Matters
- INDIA: Estraategia de Internet Shutdowns
- Commonwealth Cyber Declaration
- GDPR: Reporte en 72 horas $20 millones euros sancić facturación mjundial

Fuente: Varias

Cyber&Law

“QUE LOS PROGRESOS DE LA CIVILIZACIÓN DEBEN TENER POR EFECTO ATENUAR EN CUANTO SEA POSIBLE LAS CALAMIDADES DE LA GUERRA”

Declaración de San Petersburgo de 1968 con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra.

Cyber&Law

Prepararse

CERT DE INDUSTRIA Y SOC – SECURITY OPERATIONS CENTER EMPRESARIALES

- **Responsabilidad como personas jurídicas**
  Artículo 12 Convención de Budapest. Responsabilidad por comisión de delitos a título individual o como miembro de los órganos de dirección

- **Autorregulación**
  - Tratamiento Descubrir Riegos
  - Tratar vulnerabilidades
  - Detectar comportamientos comunes
  - Detención / Respuesta a incidentes: “Caza” de la amenaza
  - Compartición de información
  - Comunicación de incidentes al Estado y al Usuario

- **Continuidad del negocio**

Cyber&Law

¿Qué normas aplicar?

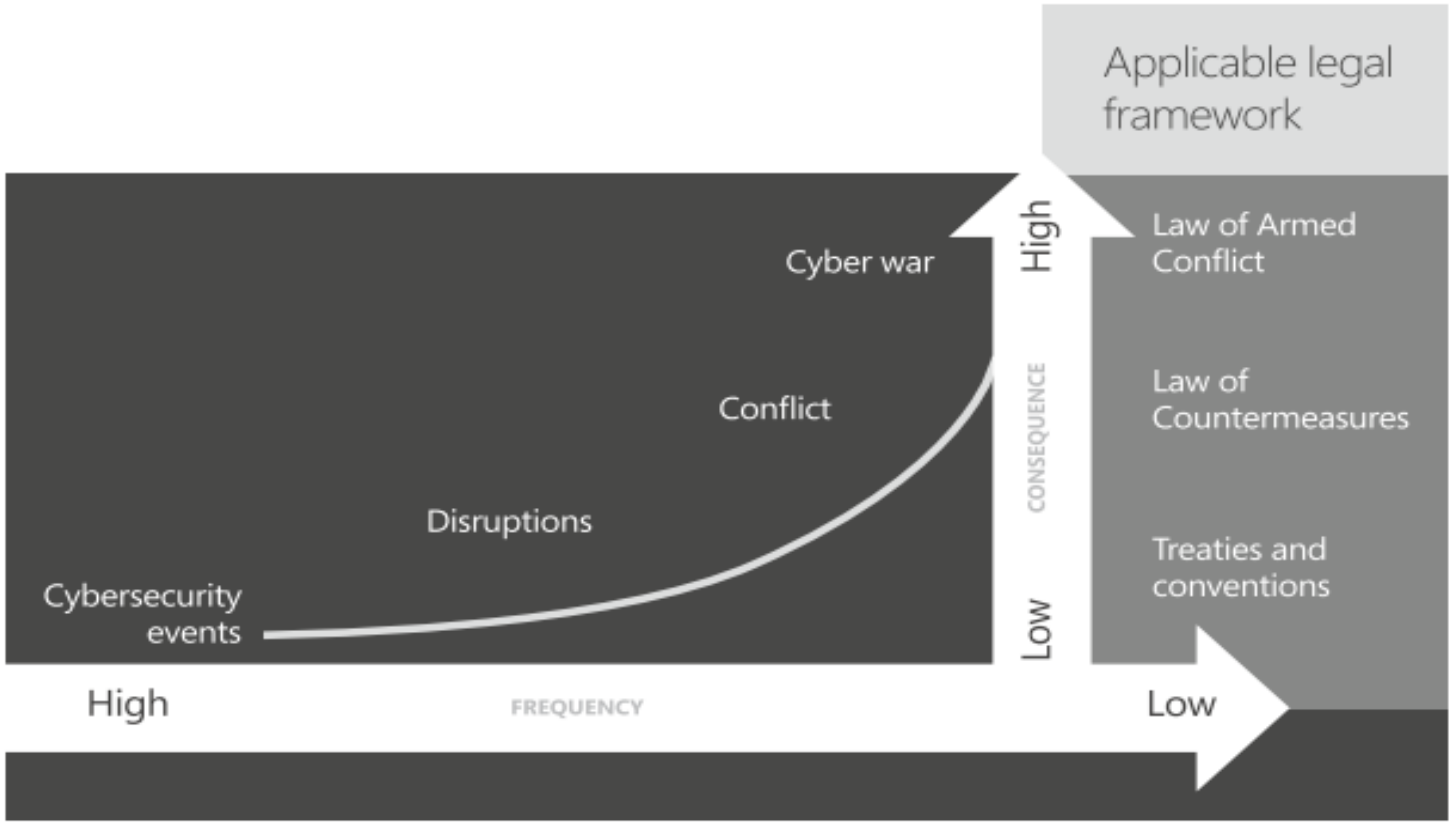


Figure 1. Escalation of cyber events and applicable legal frameworks.

Fuente: Cybersecurity Norms by Microsoft©

Cyber&Law

Importante tener en cuenta:

- Convenio de Budapest (confidencialidad, integridad y disponibilidad de datos, acceso ilícito, interceptación, interferencia, fraude etc.)

- Jurisdicción cibernética: acciones incluso cuándo los delitos se cometan por fuera de las fronteras del propio Estado víctima.

- Los Estados tienen prerrogativas
  - Obtener o grabar mediante la aplicación de medios técnicos existentes.
  - Obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: i) a obtener o grabar mediante la aplicación de medios técnicos existentes; ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
  - c) Registrar y confiscar datos informáticos almacenados
  - d) Posibilita la interceptación de datos sobre el contenido en la red.

- Los Estados están fortaleciendo sus programas de ciberseguridad CERT.

Cyber&Law

¿Qué normas aplicar?

NORMATIVA INTERNACIONAL CIVIL

- **Reglamento Unión Internacional de Telecomunicaciones.**
  Artículo 7 SUSPENSIÓN DEL SERVICIÓ: se pueden suspender las telecomunicaciones notificando aviso inmediato al secretario de la UIT, quien transmitirá a todos los miembros.

- **Convención del derecho del mar**
  Artículo 79: los Estados pueden establecer condiciones para la entrada de cable o tuberías en su territorio o en su mar territorial. ¿Telescopes?
  Artículo 112: Todos los Estados tienen derecho a tender cables y tuberías submarinas en el lecho de alta mar más allá de sus plataforma continental.
  Artículo 113 y 114. Establecen reglas para casos de ruptura o deterioro cables.

- **Convención de aviación civil internacional – Chicago**
  En caso de guerra, las disposiciones del presente Convenio no afectarán la libertad de acción de los Estados contratantes afectados, ya sean beligerantes o neutrales. El mismo principio se aplicará cuando un Estado contratante declare estado de emer nacional y lo comunique al Consejo.

Cyber&Law

GRACIAS

juan.salazar@cyberlaw.digital