I+D en Seguridad de TIC

Experiencias y observaciones

Iván Arce – Programa de Seguridad en TIC Fundación Dr. Manuel Sadosky

Charla invitada en LACSEC – LACNIC25 - 7 de Mayo de 2016, La Habana, Cuba

Ministerio de Ciencia, Tecnología e Innovación Productiva
Presidencia de la Nación

fundación SADOSKY
Investigación y Desarrollo en TIC

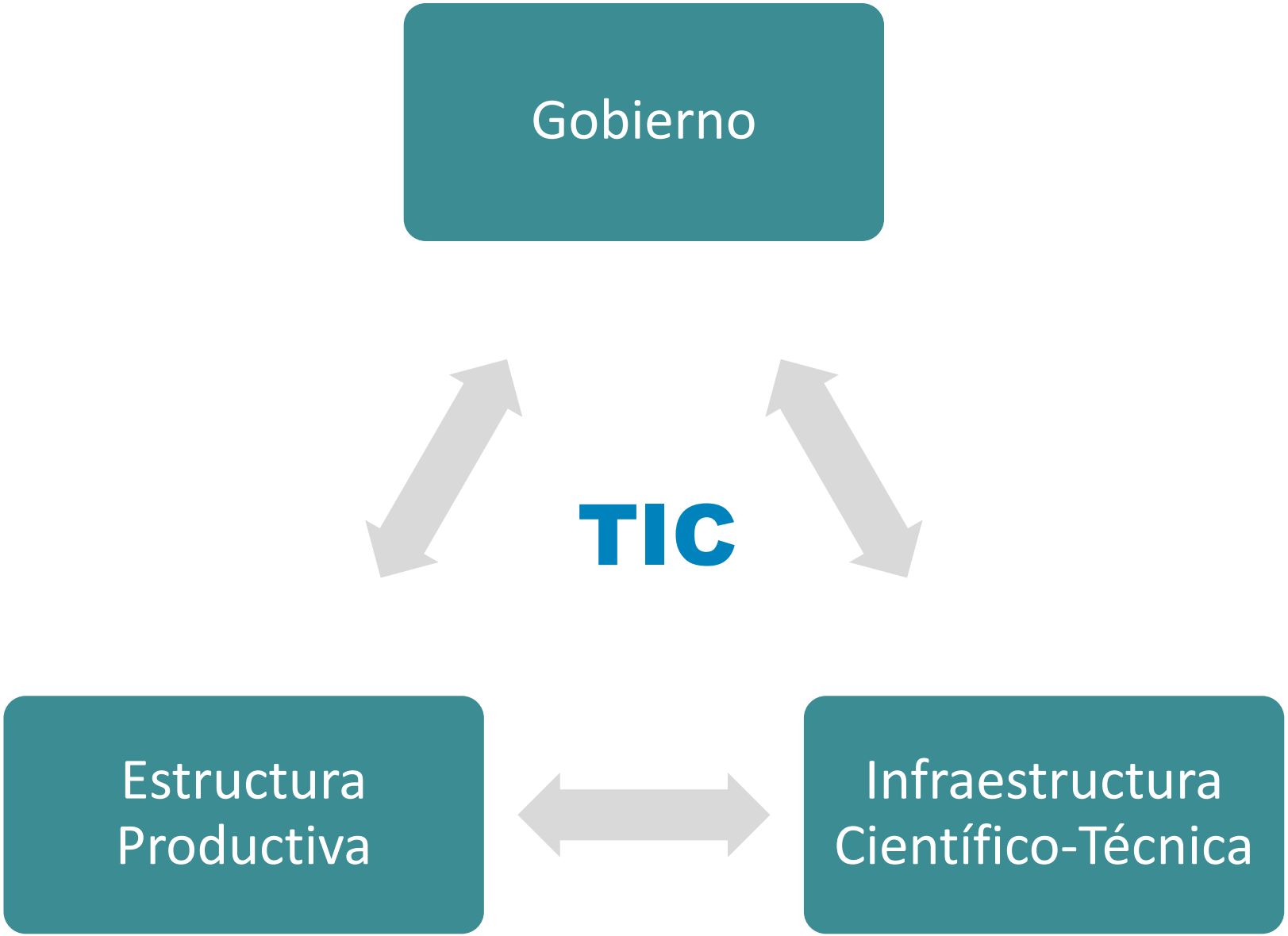
cessi ArgenTIna

CICOMRA

Qué es la Fundación Dr. Manuel Sadosky?

- La Fundación Dr. Manuel Sadosky es una institución público-privada cuyo objetivo es favorecer y promover la articulación entre el sistema científico - tecnológico y la estructura productiva en todo lo referido a las Tecnologías de la Información y Comunicación (TIC)
- Fue formalmente creada por Decreto del Poder Ejecutivo Nacional en Junio de 2009, y comenzó a funcionar en 2011
- Lleva el nombre quien fuera un pionero y visionario de la Informática en el País y la región

Manuel Sadosky
(1914-2005)


Gobierno
TIC
Estructura Productiva
Infraestructura Científico-Técnica

Cuál es el propósito del Programa STIC?

Visión

“Las TIC como factor transformador para una sociedad con un cultura emprendedora que promueve e impulsa la creación de conocimiento, la innovación productiva y sustentable, la competitividad de la economía y la mejora de la calidad de vida de la población **sin que ello redunde en un aumento de la dependencia tecnológica o de la vulnerabilidad de la infraestructura crítica**“

Funciones del Programa STIC

1. **Desarrollar y robustecer capacidades de I+D+i**

2. **Articulación Academia-Industria-Estado**

3. **Divulgación, asesoría y capacitación**

4. **Vinculación regional y extra-regional con centros de I+D de Seguridad TIC**

5. **Proyectos Faro de I+D+i**

Que temas le interesan al Programa STIC?

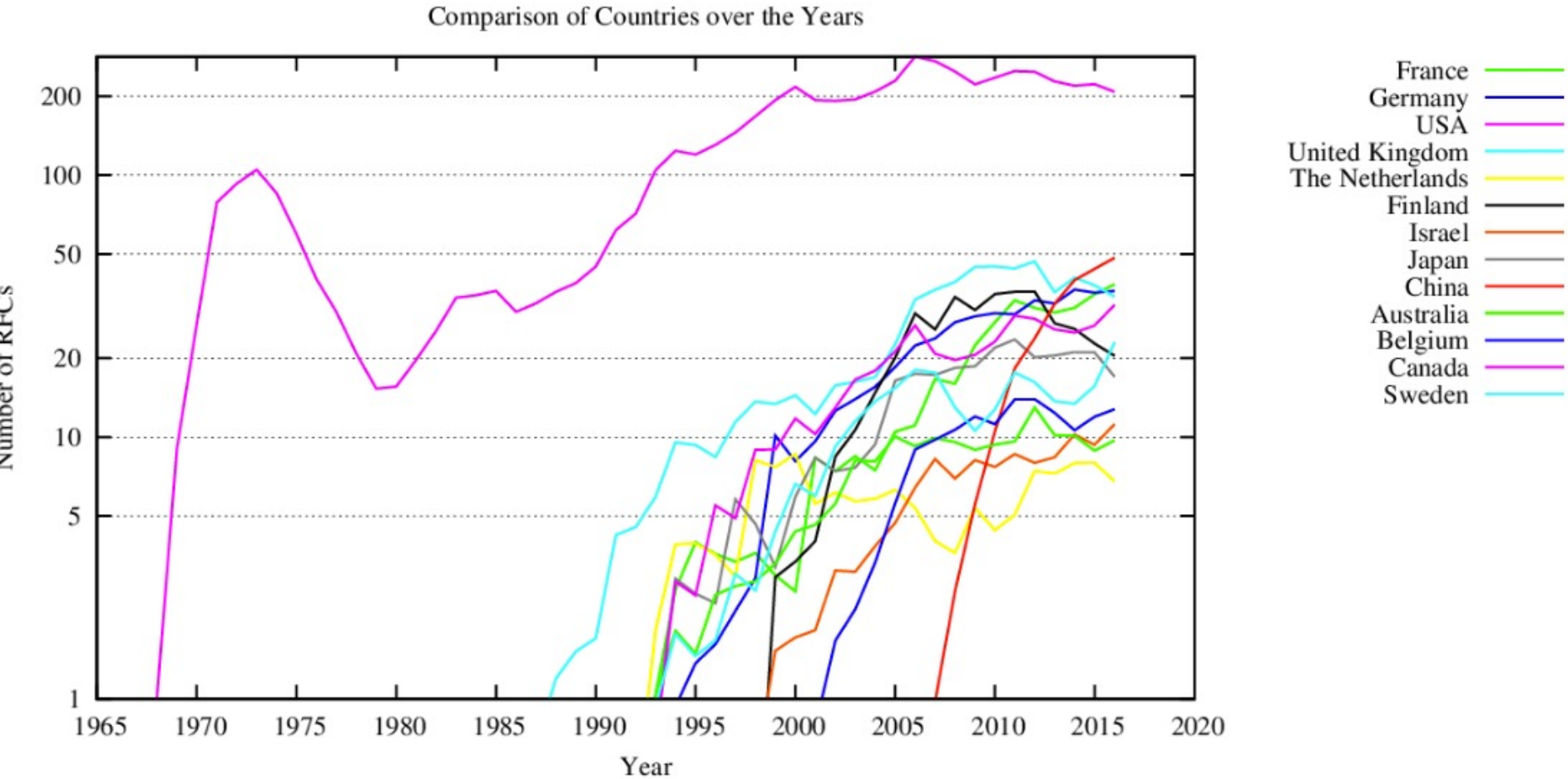
- Seguridad de Aplicaciones
- Ingeniería de Software
- Análisis estático|dinámico de código
- Software y Sistemas Embebidos
- Comunicaciones Inalámbricas
- Dispositivos Móviles
- Seguridad en Redes Avanzadas
- Sistemas de Control de Procesos Industriales y SCADA
- Métricas y modelos para la gestión de riesgo
- Arquitecturas de Seguridad Innovadoras
- Bioinformática

I+D de Seguridad en TIC
¿Por qué hablar de esto acá?

Porqué hablar de Seguridad de las TIC ?

- Tiene relevancia estratégica a nivel nacional y regional
- Problemática real con impacto directo sobre todos los habitantes
- **Sin seguridad no hay privacidad ni posibilidad de garantizar otros derechos fundamentales.**
- Seguridad de las TIC es transversal, el software es omnipresente
- La Seguridad de las TIC se convirtió en una herramienta de geopolítica
- Tendencia inexorable (?) hacia la “balcanización” y nacionalización de la comunidad internacional de seguridad informática

De dónde salen los estándares técnicos de Internet?



Argentina:34 (0,36%) Brasil:9 (0,09%) México: 3 (0,03%) Colombia: (0,03%)

Fuente: http://www.arkko.com/tools/allstats/d-countrydistr.html

De dónde salen los estándares técnicos de Internet?

Documents come from these countries, 74 different countries in total.

- 7247 documents (76.12%) have authors from USA.
- 810 documents (8.51%) have authors from United Kingdom.
- 706 documents (7.42%) have authors from China.
- 653 documents (6.86%) have authors from Germany.
- 586 documents (6.15%) have authors from France.
- 529 documents (5.56%) have authors from Canada.
- 489 documents (5.14%) have authors from Finland.
- 417 documents (4.38%) have authors from Sweden.
- 380 documents (3.99%) have authors from Japan.
- 229 documents (2.41%) have authors from India.
- 219 documents (2.30%) have authors from Belgium.
- 203 documents (2.13%) have authors from Australia.
- 176 documents (1.85%) have authors from The Netherlands.
- 172 documents (1.81%) have authors from Italy.
- 164 documents (1.72%) have authors from Spain.
- 151 documents (1.59%) have authors from Switzerland.
- 150 documents (1.58%) have authors from Israel.
- 144 documents (1.51%) have authors from Norway.
- 90 documents (0.95%) have authors from South Korea.
- 73 documents (0.77%) have authors from Austria.
- 55 documents (0.58%) have authors from New Zealand.
- 49 documents (0.51%) have authors from Ireland.
- 34 documents (0.36%) have authors from Argentina.
- 30 documents (0.32%) have authors from Russia.
- 28 documents (0.29%) have authors from Hungary.
- 26 documents (0.27%) have authors from Denmark.
- 23 documents (0.24%) have authors from Thailand.
- 19 documents (0.20%) have authors from Singapore.
- 18 documents (0.19%) have authors from Greece.
- 16 documents (0.17%) have authors from Luxembourg.
- 15 documents (0.16%) have authors from Turkey.
- 15 documents (0.16%) have authors from Slovakia.
- 13 documents (0.14%) have authors from Portugal.
- 9 documents (0.09%) have authors from Brazil.

RFCs come from these countries, 48 different countries in total.

- 1081 RFCs (69.47%) have authors from USA.
- 204 RFCs (13.11%) have authors from United Kingdom.
- 159 RFCs (10.22%) have authors from France.
- 148 RFCs (9.51%) have authors from Germany.
- 148 RFCs (9.51%) have authors from Finland.
- 126 RFCs (8.10%) have authors from Canada.
- 119 RFCs (7.65%) have authors from China.
- 104 RFCs (6.68%) have authors from Japan.
- 70 RFCs (4.50%) have authors from Sweden.
- 61 RFCs (3.92%) have authors from Belgium.
- 49 RFCs (3.15%) have authors from Australia.
- 43 RFCs (2.76%) have authors from Israel.
- 39 RFCs (2.51%) have authors from Italy.
- 34 RFCs (2.19%) have authors from India.
- 34 RFCs (2.19%) have authors from The Netherlands.
- 31 RFCs (1.99%) have authors from Switzerland.
- 27 RFCs (1.74%) have authors from Spain.
- 21 RFCs (1.35%) have authors from New Zealand.
- 18 RFCs (1.16%) have authors from Norway.
- 14 RFCs (0.90%) have authors from South Korea.
- 13 RFCs (0.84%) have authors from Thailand.
- 11 RFCs (0.71%) have authors from Argentina.
- 9 RFCs (0.58%) have authors from Hungary.
- 9 RFCs (0.58%) have authors from Austria.
- 7 RFCs (0.45%) have authors from Turkey.
- 6 RFCs (0.39%) have authors from Russia.
- 6 RFCs (0.39%) have authors from Denmark.
- 5 RFCs (0.32%) have authors from Ireland.
- 5 RFCs (0.32%) have authors from Greece.
- 4 RFCs (0.26%) have authors from Singapore.
- 3 RFCs (0.19%) have authors from Ukraine.
- 2 RFCs (0.13%) have authors from Czech Republic (rfc6110, rfc6594).
- 2 RFCs (0.13%) have authors from Croatia (rfc6273, rfc6572).
- 2 RFCs (0.13%) have authors from Poland (rfc5643, rfc6334).
- 2 RFCs (0.13%) have authors from Romania (rfc6356, rfc6824).

Fuente: http://www.arkko.com/tools/allstats/d-countrydistr.html

Mercado global de software y servicios de seguridad TIC

- Mercado global: 71.100MM USD* (2014)

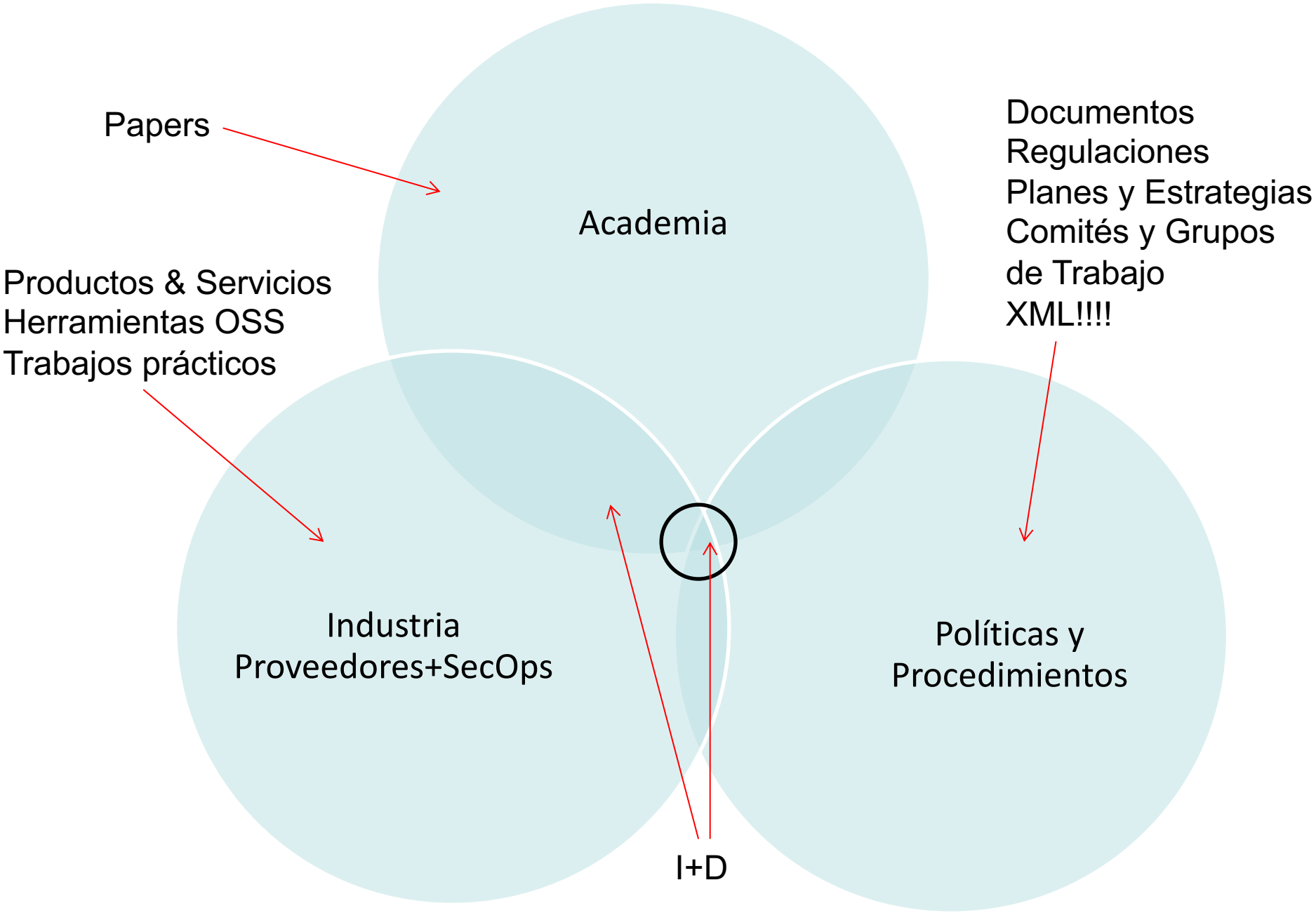
  - Seguridad Computadoras de Escritorio y Servers: $7.170 MM USD (2010)
  - Seguridad de Redes: $7.540MM USD (2010)
  - Gestión de Identidades y Accesos: $4.450MM USD (2010E)
  - Gestión de Seguridad y Vulnerabilidades : $3.400MM USD (2010)
  - Seguridad Web: $1.700MM USD (2010)
  - Protección contra Filtración de Datos (DLP): $680MM (2013)
    Crecimiento estimado > 18% para el 2014

- Crecimiento estimado al 2015: 76.900 MM USD* (8,2%)

- >1.000 Empresas de Seguridad TIC $10MM USD/año
- **Menos del 2% son de capitales o tecnología desarrollada en LatAm**

* Forecast Overview: Information Security, Worldwide, 2012-2018, 2Q14 Update, Agosto 2014, Gartner

¿Qué es hacer I+D en Seguridad de TIC?


Papers
Academia
Documentos
Regulaciones
Planes y Estrategias
Comités y Grupos
de Trabajo
XML!!!!
Productos & Servicios
Herramientas OSS
Trabajos prácticos
Industria
Proveedores+SecOps
Políticas y
Procedimientos
I+D

“Llamaremos Tecnología al conjunto ordenado de los conocimientos empleados en la producción y comercialización de bienes y servicios, y que esta integrado no sólo por los conocimientos científicos sino también por los conocimientos empíricos que resultan de observaciones, experiencias, aptitudes específicas, tradición oral o escrita, etc.”

- Jorge Sábato, *El comercio de Tecnología*,1972

"Déjenme decir que toda persona que se incorpora a esta organización sabe porqué hacemos investigación: Para darle ganancias a la General Electric"

- Arthur M. Bueche, Vice President of Research & Development, General Electric, 1972

“Yo soy yo y mi circunstancia”
– Ortega Y Gasset
(YMMV)


commodore
VIC 20
POWER
CTRL
RESTORE
RUN STOP
SHIFT LOCK
RETURN
SHIFT
CLR HOME
INST DEL
BLK
WHT
RED
CYN
PUR
GRN
BLU
YEL

```
**** COMMODORE 64 BASIC V2 ****

 64K RAM SYSTEM  38911 BASIC BYTES FREE

READY.
LOAD"*",8,1

SEARCHING FOR *
LOADING
READY.
RUN
```

In the future, being able to "speak" a computer language will give you a tremendous advantage over those who can't, <u>not because you can write a computer program but because you'll have a better understanding of what a computer is and does</u>, and you will make better use of computing at the school, on the job and at home…"

Commodore VIC-20 Programmer's Reference Guide


commodore
REVS

Sobre el orador (o.. quién es este tipo???)

…… - 2012 PROGRAMA STIC – Fundación Dr. Manuel Sadosky

Organización sin fines de lucro público-privada dedicada a promover, robustecer y articular las actividades de investigación, desarrollo e innovación en TIC entre el sector privado, sistema científico-tecnológico y estado argentino.

http://www.fundacionsadosky.org.ar

2011-1996 CORE SECURITY TECHNOLOGIES – Fundador & CTO

Empresa de software y servicios de seguridad informática fundada en 1996 en Argentina.

>20MM USD/año, >100 empleados, centro de I+D en Buenos Aires, oficinas comerciales en EEUU.

>15 patentes internacionales otorgadas, 100+ publicaciones técnicas, 100+ vulnerabilidades

http://www.coresecurity.com

1996-1993 VirtualFon– Director R&D, Líder del equipo técnico

Diseño, Implementación y despliegue de soluciones de Computer Telephony Integration (CTI) LatAm

2015-2003 IEEE Security & Privacy Magazine – Editor Asociado / Miembro del Consejo Editorial

Revista especializada en seguridad y privacidad de la Sociedad de Computación del IEEE

http://www.computer.org/portal/web/computingnow/securityandprivacy

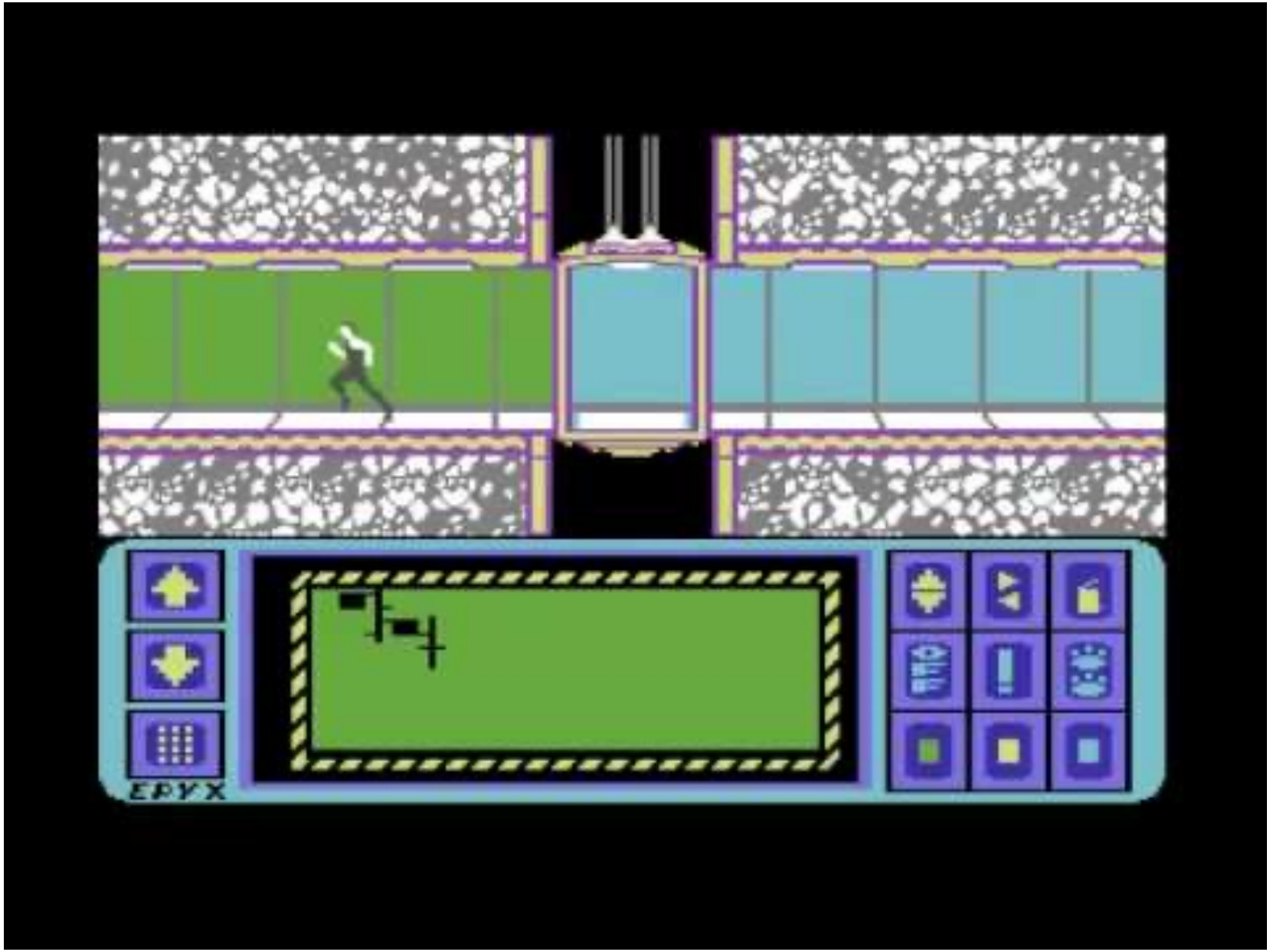
2014 – Miembro fundador del Center for Secure Design de IEEE-CS

http://cybersecurity.ieee.org/center-for-secure-design.html

Todos te dicen “qué”
Nadie te dice “cómo”

Ataque y Defensa son parte de la misma disciplina

I+D de Seguridad en TIC: Actividad Lúdica

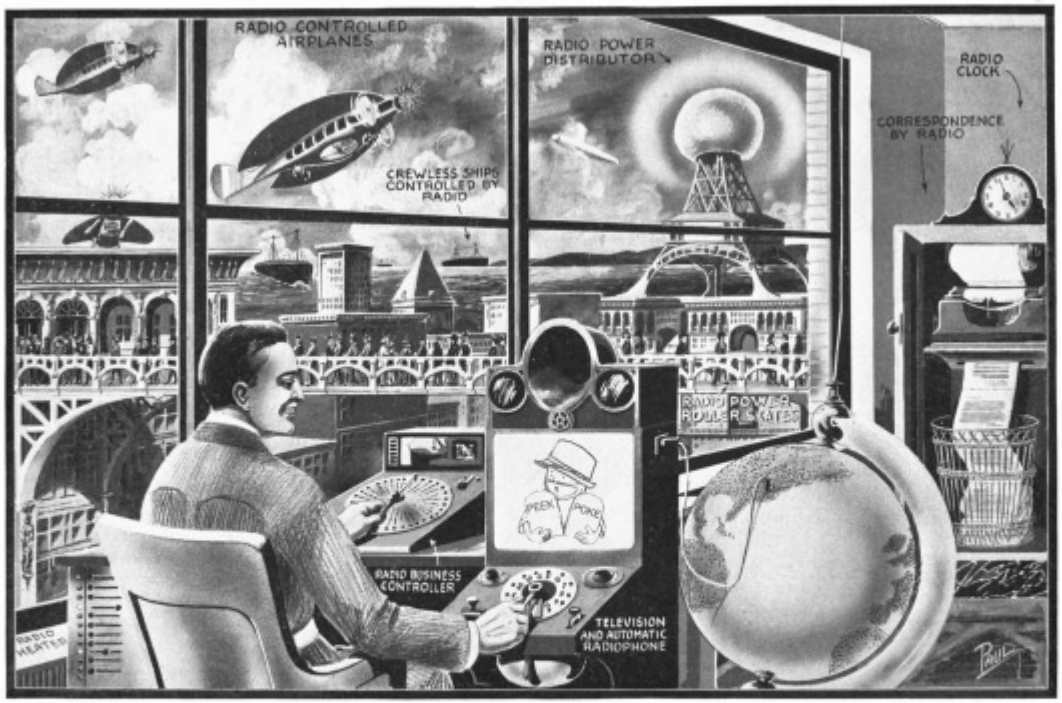


Adversarios vs. Enemigos

NO es la batalla entre El Bien y El Mal

POC || GTFO

PoC || GTFO



IN THE THEATER OF LITERATE DISASSEMBLY,

PASTOR MANUL LAPHROAIG

AND HIS MERRY BAND OF

REVERSE ENGINEERS

LIFT THE WELDED HOOD FROM

THE ENGINE THAT RUNS THE WORLD!

“Hacer predicciones es muy difícil, especialmente cuando se trata del futuro”

-Niels Bohr, Premio Nobel de Física , 1887-1962

“La mejor forma de predecir el futuro es inventarlo (uno mismo)”

-Alan Kay, 1971

Cómo estructurar un equipo de I+D en Seguridad de TIC ?

Heinlein – Specialization is for Insects

> *A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly. Specialization is for insects.*
>
> –Robert A. Heinlein

Sin embargo, la tendencia es hacia la especialización

- Formación Académica
  - Cómo funciona una computadora?
  - Como funciona un sistema operativo?

- Experiencia Práctica
  - Programación en lenguaje de bajo nivel (C , asm, C++)
  - Programación en lenguaje de alto nivel (Java, Python, Ruby)
  - OOP, Funcional (+)
  - Implementación de protocolos de red (+)
  - Ingeniería Inversa (+)
  - Certificaciones de Seguridad (-)
  - Resolución de problemas (+)

- Proyectos de código abierto, competencia de programación
- Videojuegos, sistema operativo, algoritmo criptográfico

- Capacitación
  - Corrupción de Memoria
  - Ingeniería Criptográfica (Construir y Romper)
  - Aplicaciones Web
  - Ingeniería Inversa, Auditoría de código, Logs
  - Seguridad de protocolos de red
  - Modelado de Amenzas (+)
  - Patrones de diseño (+)
  - Lenguages de programación (++)
  - Virtualización (++)

- Es más fácil que un desarrollador “aprenda” de seguridad
- Es más fácil generalizar a partir de la experiencia

- Gestión de la innovación
  - Actividad colectiva vs. Individual
  - Equipos interdisciplinarios, rotación.
  - Revisión de pares
  - Actividades programadas (bugweek, burst, BDLV)
  - Actividades exploratorias
  - Documentación y comunicación
  - Transferencia de conocimiento
  - *“working code”*

- Gestión del equipo
  - Remuneración
  - Incentivos intrínsecos
  - Crecimiento profesional

Output

“Entregables” de proceso de I+D

- Papers
  - Resultados reproducibles
  - Con ejemplos de la vida real
  - Citar fuentes no-académicas
  - Delimitar el alcance de los resultados
  - Código fuente, datos.
- “White papers”, boletines de seguridad, documentos técnicos
  - Metodología y terminología
  - Fuente de datos, alcance de los resultados
- Herramientas
  - Prueba de concepto vs. Prototipo Funcional
  - Código fuente, pruebas, compilación, integración
  - Licencia de uso
- Tecnología patentable

Investigación y Reporte de Vulnerabilidades

Por qué vale la pena hacerlo?

- Ayudar a usuarios/organizaciones a entender y mitigar riesgo
- Adquisición y transferencia de conocimientos
- Mejorar el estado del arte de la disciplina científica
- Imperativo profesional
- Reconocimiento de los pares
- Remuneración, marketing, crecimiento profesional

Pautas a seguir

- Siempre notificar al fabricante y darle oportunidad de arreglar
- Siempre trabajar con una fecha de publicación
- Mantener transparencia sobre el proceso
- Documentar quién dijo qué, cuando.
- Intentar publicación coordinada
- Asumir que descubrimiento simultáneo
- Minimizar plazo de publicación
- Por defecto, todo es explotable si no hay evidencia de lo contrario
- No hay recetas genéricas
- Buscar soluciones alternativas (configuración, mitigación)

Qué publicar?

- Resumen
  Alcance
  Impacto
  Solución oficial
  Mitigación

- Identificador único por cada vulnerabilidad

- Clasificación por tipo, métricas

- Descripción técnica, pasos para reproducir

- Referencias

- Cronología del proceso

Patente ?

Patentar o no patentar?

- Se patenta una implementación de “una idea”
- Novedosa y no obvia (ni derivada de combinar otras)
- Proceso de patentamiento
  - Redacción (descripción técnica, claims)
  - EPO, USPTO: Fecha de entrada (protección temporaria)
  - Búsqueda de trabajos previos
  - Revisión formal, publicación
  - Objeciones de forma y de contenido
  - Correción, ortorgamiento (o no)
  - Incorporación a oficinas regionales, nacionales (PCT)
- 3-5+ años
- >= 30,000 USD
- Desincentiva uso u adopción por 3ros
- Utilizable como mecanismo defensivo

Contexto legal y regulatorio

Computer Fraud and Abuse Act (CFAA) 1986, EEUU

www.justice.gov/sites/defa

www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Chapter 1

Computer Fraud and Abuse Act

In the early 1980s law enforcement agencies faced the dawn of the computer age with growing concern about the lack of criminal laws available to fight emerging computer crimes. Although the wire and mail fraud provisions of the federal criminal code were capable of addressing some types of computer-related criminal activity, neither of those statutes provided the full range of tools needed to combat these new crimes. *See* H.R. Rep. No. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692.

In response, Congress included in the Comprehensive Crime Control Act of 1984 provisions to address the unauthorized access and use of computers and computer networks. The legislative history indicates that Congress intended these provisions to provide "a clearer statement of proscribed activity" to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access." *Id.* Congress did this by making it a felony to access classified information in a computer without authorization and making it a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer. In so doing, Congress opted not to add new provisions regarding computers to existing criminal laws, but rather to address federal computer-related offenses in a single, new statute, 18 U.S.C. § 1030.

Even after enacting section 1030, Congress continued to investigate problems associated with computer crime to determine whether federal criminal laws required further revision. Throughout 1985, both the House and the Senate held hearings on potential computer crime bills, continuing the efforts begun the year before. These hearings culminated in the Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986, which amended 18 U.S.C. § 1030.

In the CFAA, Congress attempted to strike an "appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses." *See* S. Rep. No. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482. Congress addressed federalism concerns in the CFAA by limiting federal jurisdiction to

www.justice.gov/sites/defa

www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

cases with a compelling federal interest—i.e., where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature. *See id.*

In addition to clarifying a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. For example, Congress added a provision to penalize the theft of property via computer that occurs as a part of a scheme to defraud. Congress also added a provision to penalize those who intentionally alter, damage, or destroy data belonging to others. This latter provision was designed to cover such activities as the distribution of malicious code and denial of service attacks. Finally, Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.

As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008. The 2008 amendments made the following changes to section 1030:

- Eliminated the requirement in 18 U.S.C. § 1030(a)(2)(C) that information must have been stolen through an interstate or foreign communication, thereby expanding jurisdiction for cases involving theft of information from computers;
- Eliminated the requirement in 18 U.S.C. § 1030(a)(5) that the defendant's action must result in a loss exceeding $5,000 and created a felony offense where the damage affects ten or more computers, closing a gap in the law;
- Expanded 18 U.S.C. § 1030(a)(7) to criminalize not only explicit threats to cause damage to a computer, but also threats to (1) steal data on a victim's computer, (2) publicly disclose stolen data, or (3) not repair damage the offender already caused to the computer;
- Created a criminal offense for conspiring to commit a computer hacking offense under section 1030;
- Broadened the definition of "protected computer" in 18 U.S.C. § 1030(e)(2) to the full extent of Congress's commerce power by including those computers used in or affecting interstate or foreign commerce or communication; and

Convención sobre “delito cibernético” (Budapest, 2001)

Full list - Council of Europe

www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

WWW.COE.INT | HUMAN RIGHTS | DEMOCRACY | RULE OF LAW | EXPLORE | EN | CONNECT

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

Treaty Office

Home | General Information | Full list | Recent changes | Search | Partial Agreements | Translations | Notifications | Contact

You are here: Conventions > Full list

Full list

Details of Treaty No.185

Convention on Cybercrime

Title	Convention on Cybercrime
Reference	CETS No.185
Opening of the treaty	Budapest, 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
Entry into Force	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe
Summary	IT DE EN RU FR The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and ... of network security. It also contains a series of powers and procedures such as the search of

TREATY OFFICE

- Home
- General Information
- Full list
- Recent changes
- Search
- Partial Agreements

www.coe.int

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Wassenaar Arrangement

on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

Home | Sitemap | Contact Us | Search

- Introduction
- F.A.Q.
- Participating States/Links
- Guidelines & Procedures incl. Initial Elements
- Control Lists
- All Public Documents
- Secretariat
- Related Links

Latest Additions

2015

March

List of Dual Use Goods and Technologies and Munitions List

Summary of Changes to the List of Dual Use Goods and Technologies and Munitions List

January

Basic Documents - Compilation

2014

December

Statement by the Plenary Chair on 2014 Outcomes

Guidelines for Applicant Countries

Tratado de Wassenaar

"The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of ***conventional arms and dual-use goods and technologies****, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the* ***development or enhancement of military capabilities*** *which undermine these goals, and are not diverted to support such capabilities."*

41 paises signatarios:
UE, EEUU, Canada, Japón, México, Korea, Rusia, Sudafrica, Australia, Nueva Zelanda, Argentina

Paises NO signtarios: Brasil, China, Israel, Iran, India, Pakistan,Vietnam…

Controles de exportación implementados (o en proceso):
Alemania, UK, Italia, Australia, Canada, Japon, EEUU

Motivación: Evitar el uso de "software de intrusion" y "sistem ade vigilancia" por parte de gobiernos opresivos

4. D. 3. Not used since 2009

N.B. *See Category 5–Part 2 for "software" performing or incorporating "information security" functions.*

4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".

4. E. TECHNOLOGY

4. E. 1. "Technology" as follows:

a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D.

b. "Technology", other than that specified by 4.E.1.a., specially designed or modified for the "development" or "production" of equipment as follows:

1. "Digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 1.0 Weighted TeraFLOPS (WT);
2. "Electronic assemblies" specially designed or modified for enhancing performance by aggregation of processors so that the 'APP' of the aggregation exceeds the limit in 4.E.1.b.1.

c. "Technology" for the "development" of "intrusion software".

Cat 4 "Intrusion software"

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:

a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes

1. *"Intrusion software" does not include any of the following:*
   a. *Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;*
   b. *Digital Rights Management (DRM) "software"; or*
   c. *"Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.*
2. *Network-capable devices include mobile devices and smart meters.*

Technical Notes

1. *'Monitoring tools': "software" or hardware devices, that monitor system behaviours or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.*
2. *'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.*

Conclusiones

Email: stic@fundacionsadosky.org.ar

GRACIAS!