Infraestructuras críticas y Seguridad de la Información

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

Jornada Regional de Ciberdefensa en Rosario – 11 de agosto de 2014

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

fundación SADOSKY
Investigación y Desarrollo en TIC

cessi ArgenTIna

CICOMRA

Presentación

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.
Primera en desarrollar software comercial para penetration testing (2002, CORE IMPACT)
Hoy: 1600+ clientes de todo el mundo (NASA, Cisco, Apple, Chevron, Lockheed Martin, Raytheon, Boeing, Abbot, Pfizer, GE, Honeywell, AT&T, BT, Qualcomm, US FAA, US NRC…)
150-200 empleados, centro de I+D en Buenos Aires, oficinas comerciales en Boston, EEUU.
9 patentes internacionales otorgadas, 100+ publicaciones técnicas, 100+ vulnerabilidades

http://www.coresecurity.com

2014-2003 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

Qué es la Fundación Sadosky ?

- La Fundación Dr. Manuel Sadosky es una institución público-privada cuyo objetivo es promover la articulación entre el sistema científico - tecnológico y la estructura productiva en todo lo referido a las Tecnologías de la Información y la Comunicación (TIC)

- Formalmente creada por Decreto del Poder Ejecutivo Nacional en Junio de 2009, comenzó a funcionar a fines de 2011

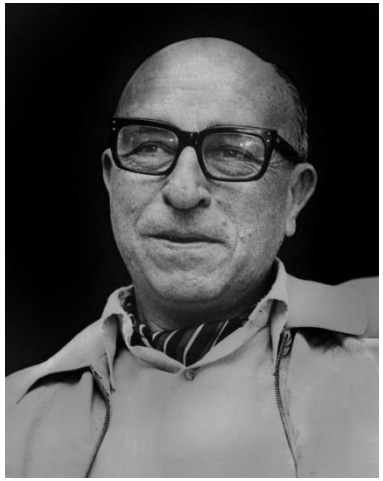
- Lleva el nombre de quien fuera un pionero y visionario de la informática tanto en el país como en la región

- MinCyT, CESSI y CICOMRA

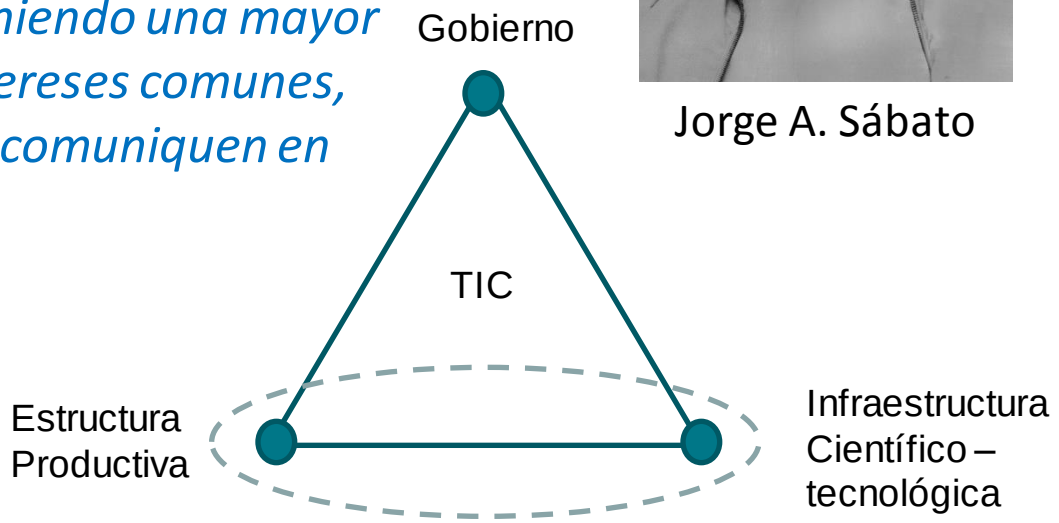
Dr. Manuel Sadosky
(1914-2005)

Tenemos objetivos de mediano y largo plazo

*"La **interacción** necesaria entre el **gobierno**, la **estructura productiva** y la **infraestructura científico-tecnológica** no se alcanza con la sola expresión de deseo, mediante un decreto, sino que es consecuencia de un proceso socio-político que se acelera en la medida en que sus protagonistas vayan teniendo una mayor conciencia de su rol, posean intereses comunes, definan objetivos comunes y se comuniquen en un lenguaje común"*



Jorge A. Sábato



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**

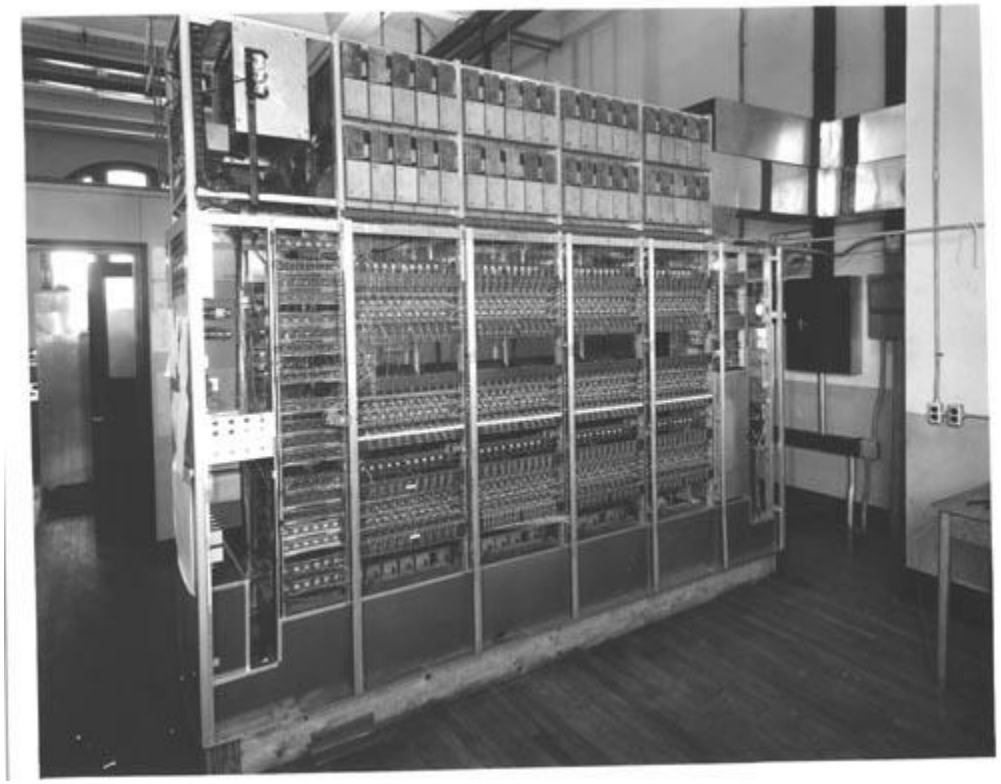
3. **Divulgación, asesoría y capacitación**

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

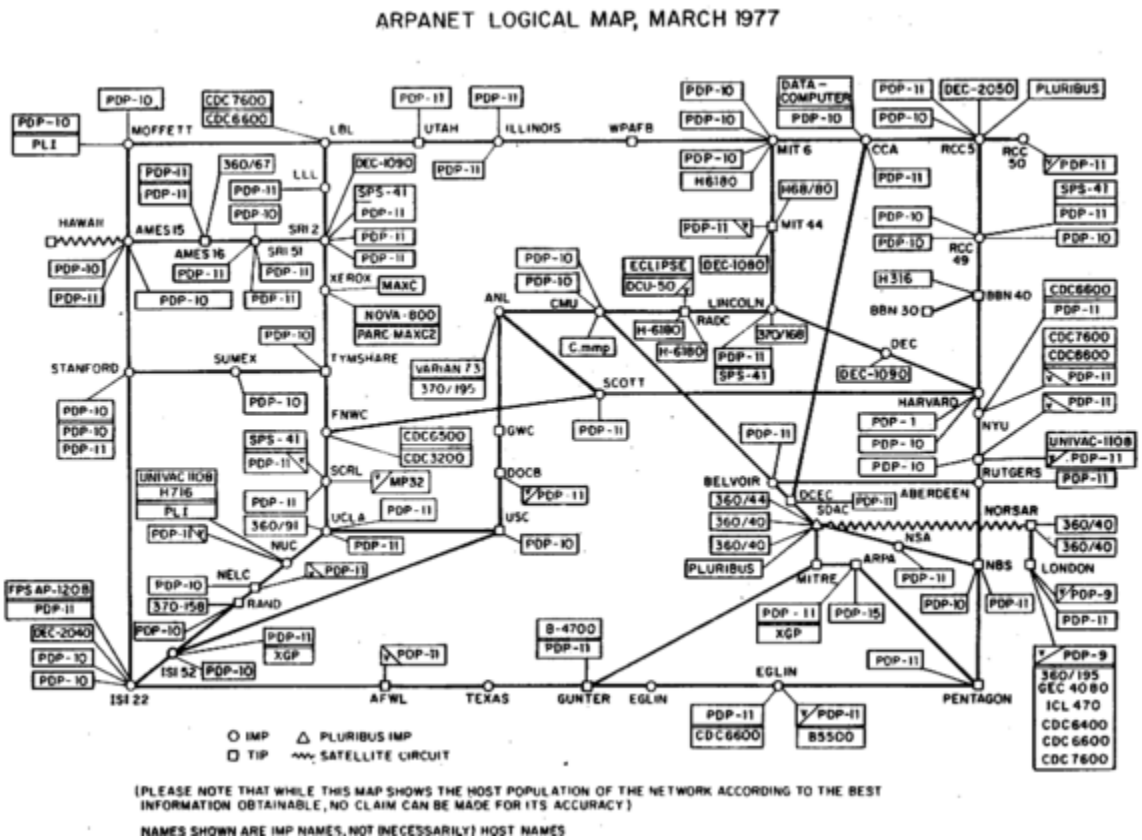
5. **Proyectos Faro de I+D+i**

Seguridad de la Información
Ataque y defensa

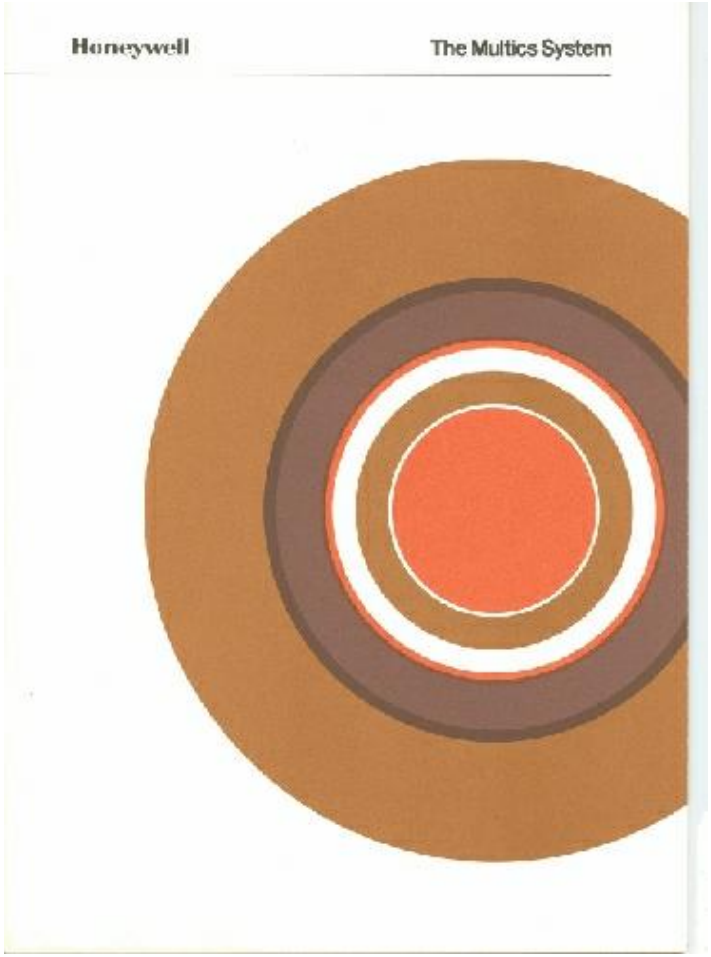
1950-1970

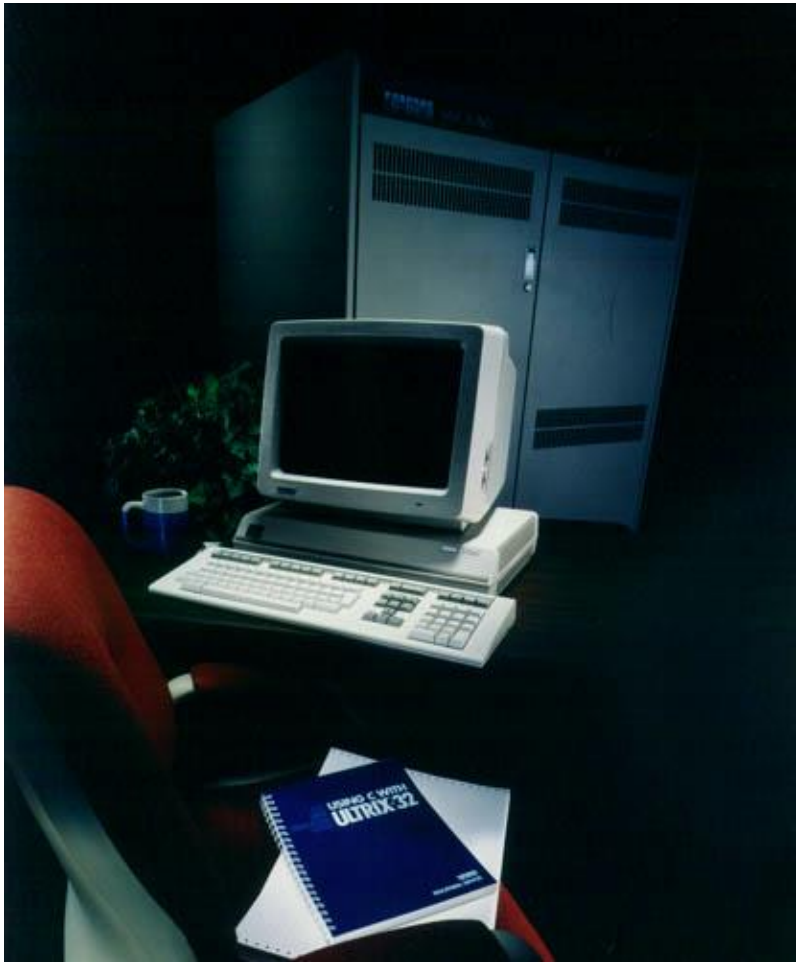


1970-1980

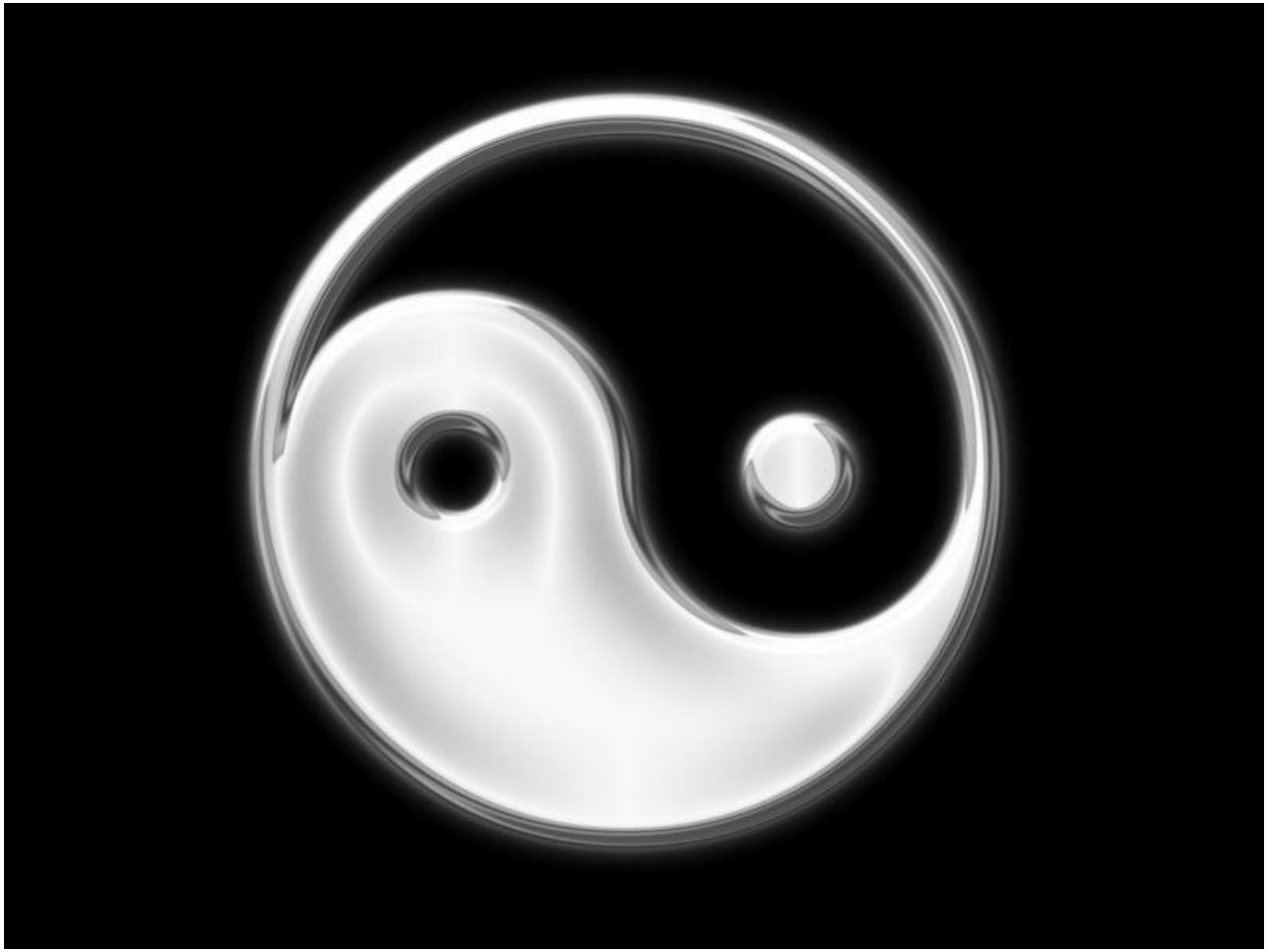

ARPANET LOGICAL MAP, MARCH 1977
MOFFETT
LBL
UTAH
ILLINOIS
WPAFB
MIT 6
CCA
RCC 5
RCC 50
PLURIBUS
HAWAII
AMES 15
AMES 16
SRI 2
SRI 51
XEROX
MAXC
NOVA-800
PARC MAXC2
LLL
360/67
DEC-1090
SPS-41
H68/80
MIT 44
ECLIPSE
DCU-50
DEC-1080
H316
BBN 40
BBN 30
CDC6600
CDC7600
RCC 49
ANL
CMU
C.mmp
LINCOLN
RADC
H-6180
370/168
DEC
DEC-1090
STANFORD
SUMEX
TYMSHARE
VARIAN 73
370/195
SCOTT
HARVARD
NYU
UNIVAC-1108
RUTGERS
FNWC
GWC
CDC6500
CDC3200
DOCB
SCRL
MP32
UNIVAC 1108
H716
PLI
360/91
UCLA
USC
NUC
BELVOIR
360/44
360/40
ABERDEEN
DCEC
SDAC
NSA
NORSAR
LONDON
NELC
RAND
ARPA
MITRE
NBS
FPSAP-120B
DEC-2040
ISI 52
ISI 22
AFWL
TEXAS
GUNTER
EGLIN
B-4700
XGP
PENTAGON
360/195
GEC 4080
ICL 470
CDC6400
CDC 6600
CDC 7600
85500
IMP
TIP
PLURIBUS IMP
SATELLITE CIRCUIT
(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

1970-1980



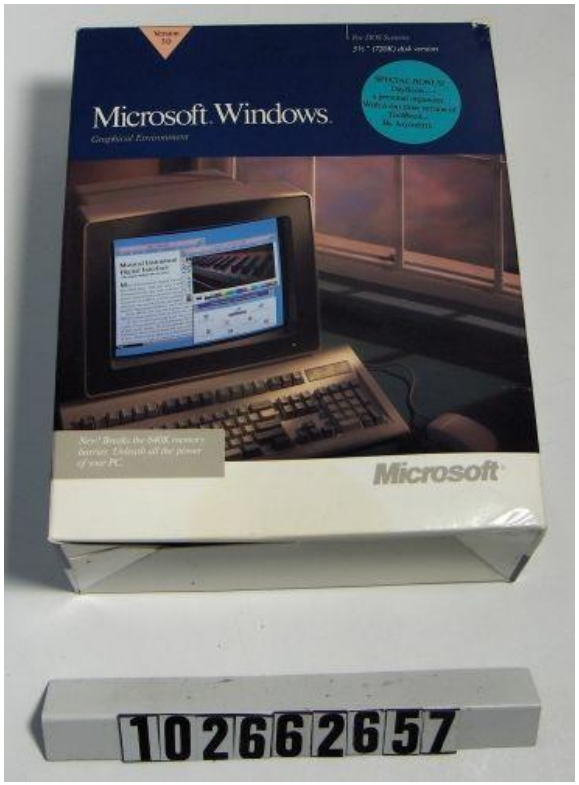


1970-1980



1980-1990

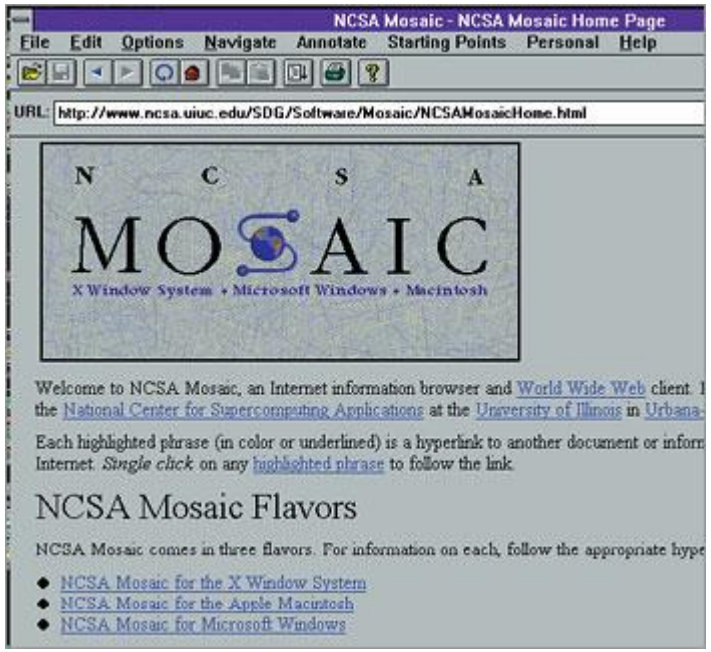

IBM
IBM
102633580


Microsoft Windows
Graphical Environment
Microsoft
102662657

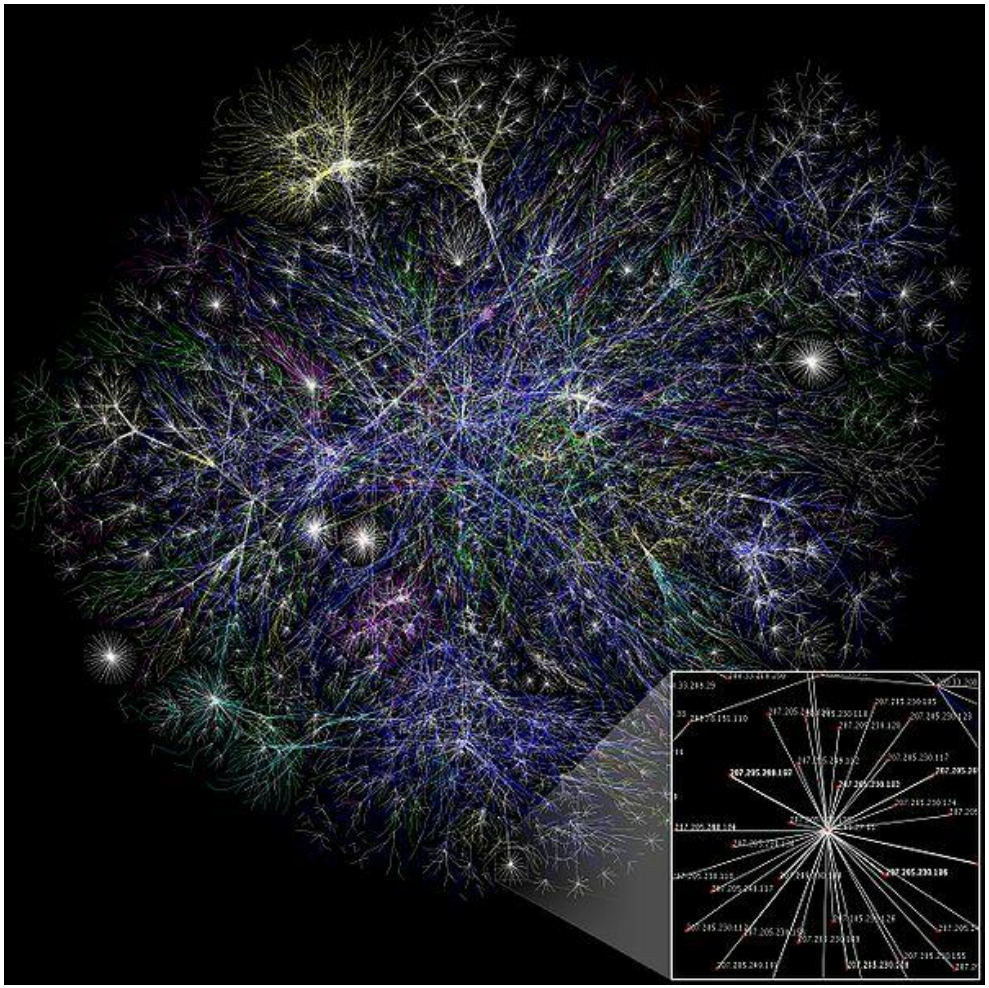
1990-2001

Sun microsystems

We make the net work.



1990-2001



RSA®

VERISIGN™

2001-2010

amazon.com®

ebay®

2010+

STUXNET: Se abre la caja de Pandora

- STUXNET (Junio 2010)
  - Infecta Windows por auto-ejecución usando bug en archivos .LNK
  - Se propaga en red local usando bugs de Windows Print Spooler y Server Service RPC
  - Instala driver (rootkit) firmado con certificados de JMicron o Realtek
  - Determina si el software **Step 7 / WinCC de Siemens** esta instalado
  - Usan interposición de DLLs para capturar llamadas a la API (*API Hooking*)
  - Instala (y oculta) código propio en PLC Siemens S7-300
  - Mas información: "W32.Stuxnet Dossier" de Symantec
    http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

- DUQU (Septiembre 2011)
  - Se propaga vía un documento MS Word
  - Explota vulnerabilidad en kernel de Windows (parser de TTF en win32k.sys)
  - Inyecta código en procesos de ring 3 (Explorer,IExplorer,Firefox,etc)
  - Detecta y evade antivirus
  - Establece canal de control via HTTP GET a servidores usados de proxy
  - Envía información recolectada usando HTTP POST de un archivo .jpg
  - Mas información: "W32.Duqu The precursor to the next Stuxnet"
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Agente del re-contra-espionaje

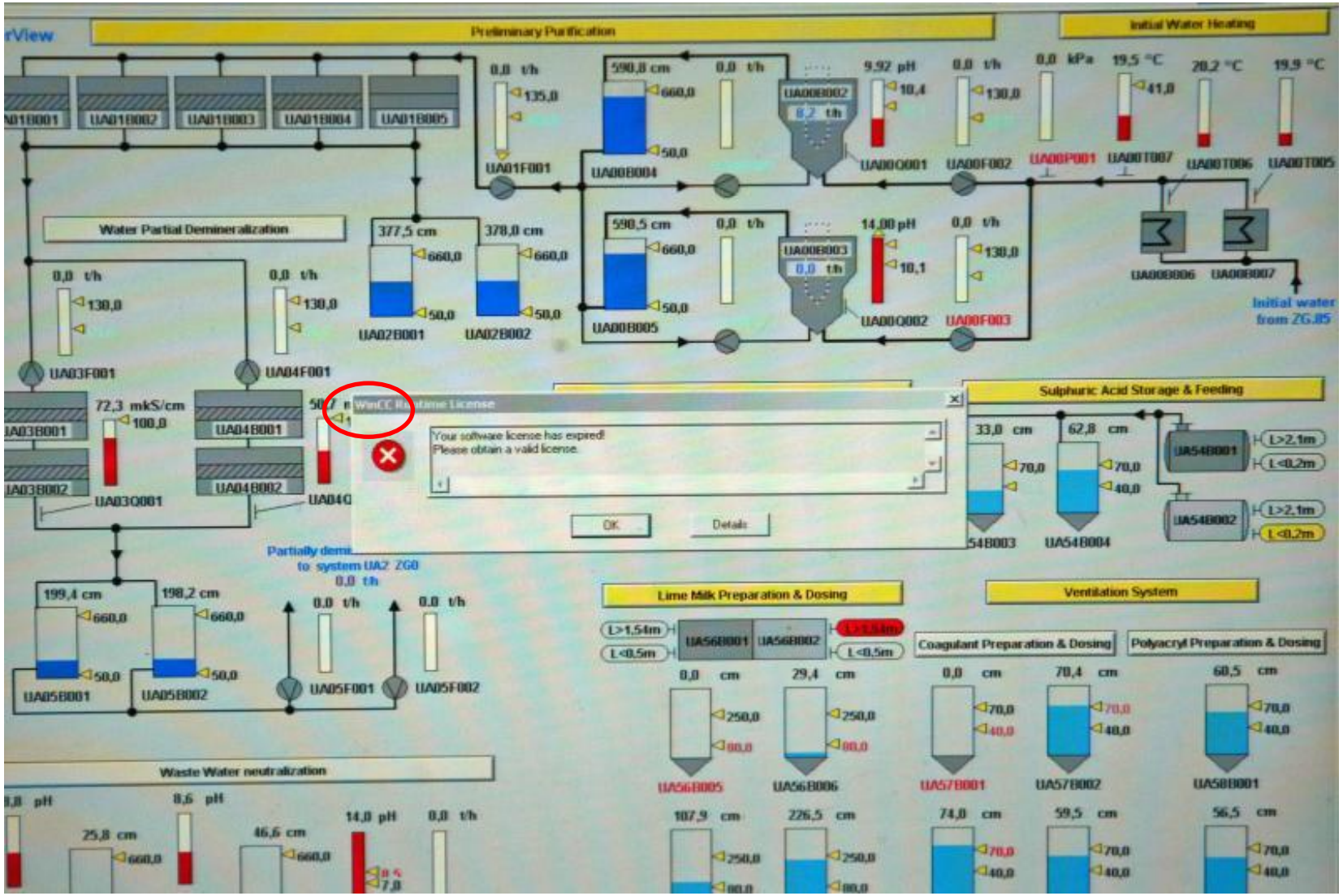
- FLAME (Mayo 2012)
  - Focos de infección: Iran, Israel, Palestina, Sudan, Siria, Libano, Arabia Saudi, Egipto
  - Se propaga vía USB o red local (MITM via WPAD para servir un update de MSFT)
  - Utilizado para recolectar información (AutoCAD, PDF, .doc, audio, screenshots, skype)
  - Diseño modular, programado en lenguaje OO, compilador “raro”
  - Maquina virtual de LUA, base de datos SQLite
  - Detecta y evade anti-virus
  - Firmado con un certificado de MSFT! (Microsoft Terminal Server Licensing Service)
  - Autoridad certificante: “Microsoft Enforced Licensing Intermediate PCA”
  - Cualquiera con un MSFT Terminal Server **activado** puede firmar updates!
  - Usa un ataque de colisión a MD5 nuevo para generar un certificado válido
  - Costo estimado del ataque a MD5: 200K-2MM USD (usando AWS EC2 @ 2008)
  - Mas de 80 servers usados para C&C
  - Mas información: “Analyzing the MD5 collision in Flame” Alex Sotirov http://trailofbits.files.wordpress.com/2012/06/flame-md5.pdf

Agentes del re-contra-espionaje II

- GAUSS (Junio 2012)
  - Usa mismo bug que Stuxnet (.LNK)
  - Instala un Font ?! (Palida Narrow)
  - Utilizado para recolectar información (Líbano, Palestina, Israel, Iran)
  - Código cifrado!
    for(i=0;i<10000;i++) {h = md5(h+%Path%+DIR (%PPROGRAMFILES%))}
    for(i=0;i<10000;i++) {rc4key = md5(h+rc4key)}
  - Mas información: “The Mystery of the encrypted Gauss payload”
    http://www.securelist.com/en/blog/208193781/The_Mystery_of_the_Encrypted_Gauss_Payload
- SHAMOON (Agosto 2012)
  - C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb.
  - Driver firmado por “Eldos Corporation”
  - Borra el Master Boot Record , sobre escribe archivos con una imagen JPEG
  - Reporta victimas via HTTP GET
  - Afectó 30,000 computadoras de ARAMCO (Arabia Saudi) , Rasgas (Qatar)
  - Mas información: “The Shamoon Attacks”
    http://www.symantec.com/connect/blogs/shamoon-attacks

Pero.. qué tan difícil es hacer esto??

Que tan difícil puede ser?



Fuente: http://www.upi.com/enl-win/b00bf188f7671cf2f939d18b1453852f/#axzz2CyOpbFA2

SCADA System SIMATIC Win

www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/pages/default.aspx

Esta página está escrita en inglés ¿Quieres traducirla? No Traducir No traducir nunca del inglés

SIEMENS

Higher visibility in productio
SIMATIC WinCC SCADA s

With the SCADA system SIMATIC Win
Siemens offers an innovative, scalable
visualization system with numerous hig
performance functions for monitoring au
processes. Whether in a single-user sys
distributed multi-user system with redun
servers, the system offers complete fun
for all industries and features optimum

Automation Technology | Deutsch | Contact | Index | Site Explorer

> Automation Technology > Operator control and monitoring systems > HMI Software > SCADA System SIMATIC WinCC

SCADA System SIMATIC WinCC

- SIMATIC WinCC
- WinCC Options
- WinCC Add-ons

Process visualization with Plant Intelligence

Our SCADA system offers maximum functionality and a user-friendly user interface. With this configurable and scalable system, you have the advantage of absolute openness to both the office environment and to production. An integrated process database and Plant Intelligence, for example, ensure transparency in

SCADA System SIMATIC Win | Reference center

https://webservices.siemens.com/referenzen/#produkt=key_517340,language=en,frame=1,OTreg_0=1,regionen=reg_300

Esta página está escrita en inglés ¿Quieres traducirla? No Traducir No traducir nunca del inglés

SIEMENS

Siemens Industry Reference Center

Automation Technology Language Contact

Product
SCADA System SIMATIC WinCC

Enter search term Find Remove all filters

Industry
Please select

Region
Americas

Service
Please select

6 article(s) found

Show 10 | 20 | 50 articles per page

> **Jacksonville water supply project, Florida, USA**
Siemens helps utility JEA keep the waters flowing in Northeast Florida by introducing SINAUT telecontrol

> **Cutting-edge treatment**
Cobb County Georgia taps Siemens automation to improve wastewatertreatment operations

> **Iaco Agrícola – Brazil**

> **New Cycle for Washing Drums**
The Condor industrial laundry in North Buenos Aires increased the efficiency of its machines by using Simatic S7-200 and Micromaster 440 drives. It not only increased the washing quality but also reduced the energy consumption.

Text size

Most viewed

- Building Automation using PROFINET at AZ Sint-Jan - Realized by Actemium Belgium
- Full process automation and control of Vesta Tank Terminal using WinCC and integrated Safety
- More efficiency and flexibility with WinCC at Vopak Leftbank Terminal Antwerp - Realized by Actemium Belgium
- At Kemin, WinCC brings the productivity and quality of feed to a higher level
- Strong stuff
- Wireless waste processing at Vanheede Environmental Group - Realized by CDC Automatisatie
- Water treatment plant Xiangcheng, Suzhou, China
- North China Pharmaceutical Group Corp., China
- Automation of the Oguz-Gabala-Baku water pipeline, Azerbaijan
- Jacksonville water supply project, Florida, USA

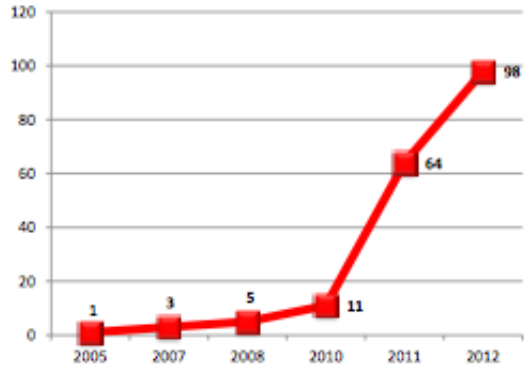


Figure 1. Dynamics of the Number of Vulnerabilities

3.3. The Number of Vulnerabilities in the ICS systems of Various Vendors

The highest number of vulnerabilities for the reporting period (42) was discovered in the components of the ICS developed by Siemens. The second place goes to Broadwin/Advantech (22 vulnerabilities); the third, to Schneider Electric (18 vulnerabilities).

Tab. 2. The Number of Vulnerabilities in the ICS Systems of Various Vendors

Vendor	Vulnerability Total	Vendor	Vulnerability Total
Automated Solutions	2		
Schweitzer Engineering Laboratories	2	WellinTech	9
RuggedCom	2	7-Technologies	12
Lantronix	3	General Electric	15
Progea	3	Invensys Wonderware	15
ABB	3	Schneider Electric	18
Sielco Sistemi	3	Advantech/Broadwin	22
Iconics	5	Siemens	42
Measuresoft	6	Emerson	6
Ecava	5	Rockwell Automation	9
Emerson	6		

Fuente: “SCADA Safety in Numbers”, Gritsai et. al. Positive Technologies http://bit.ly/RI6FtQ

2013+: Programas secretos

“viento plateado del oeste”

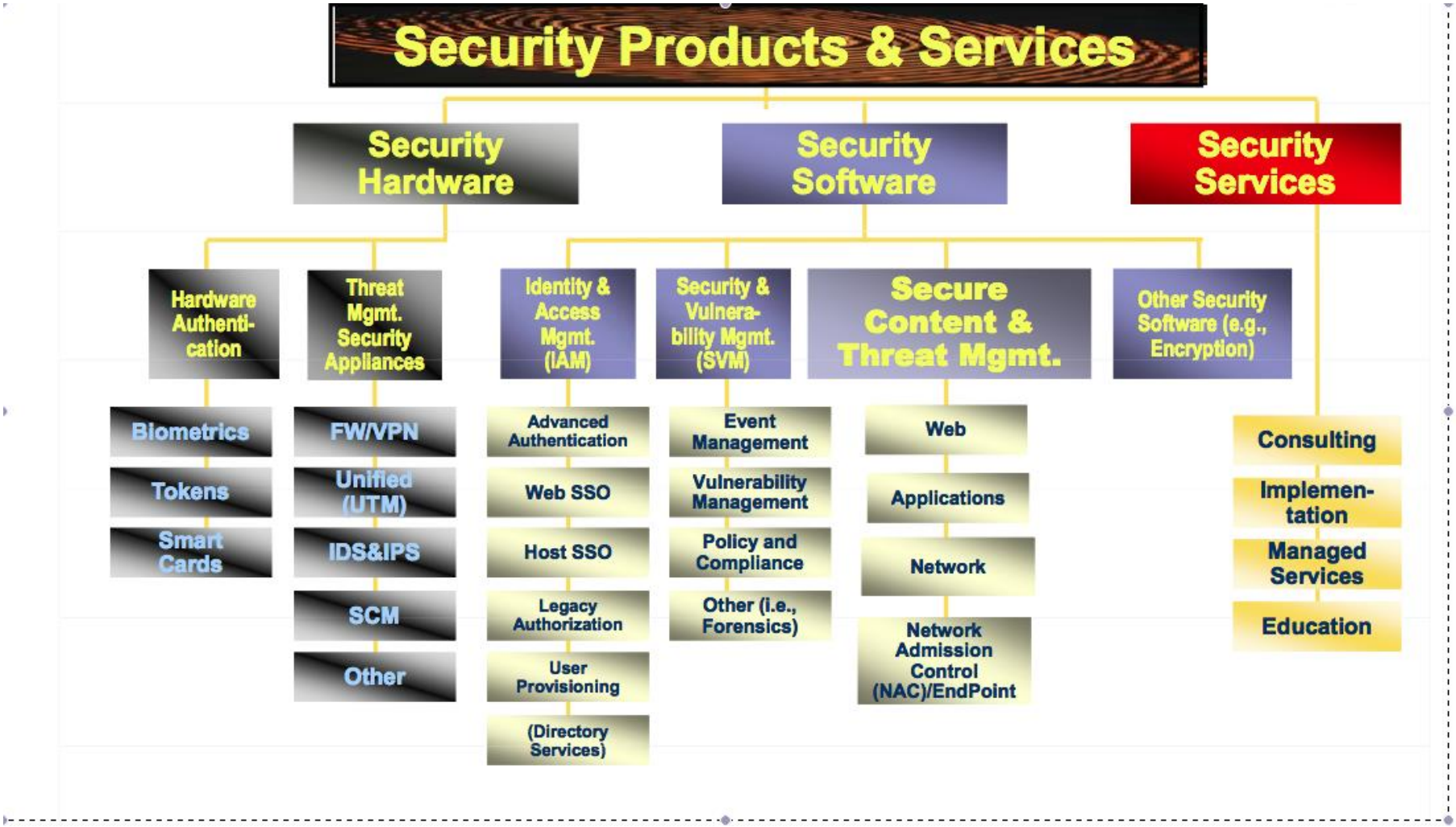
- Captura de comunicaciones en tránsito por EEUU
- Acceso a la red vía “socio” (proveedor de comunicaciones: Verizon? L-3?)
- Específico para Sur y Centro América
- Captura: Metadata, Voz y Fax (DNR)
- Captura: Metadata Y contenido (DNI)

“habilitando inteligencia de señales”

- Busca influir subrepticiamente o modificar activamente el diseño de productos de la industria TIC de EEUU y extranjera para hacerlos susceptibles a actividades de obtención de inteligencia
- Presupuesto 2013: $255mm USD, 141 empleados (personal contratado)
- Insertar vulnerabilidades en sistemas comerciales de cifrado, dispositivos de red, sistemas IT, dispositivos de usuario.
- Influir sobre politicas y estándares técnicos de criptografía
- Subvertir chips de dispositivo comerciales para cifrado de VPN y Web (SSL)
- Captura de comunicaciones VoIP P2P
- Captura y descifrado de comunicaciones 4G/LTE

Seguridad de la Información
El mercado y la industria

Mercado global de seguridad de las TIC



Mercado global de software y servicios de seguridad TIC

- Mercado global > 60.000MM USD* (anual)
  - 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)
- Crecimiento estimado al 2016: 86.000 MM USD* (CAGR 9,4%)
- >1.000 Empresas de Seguridad TIC $10MM/año (< 1% .AR)

* Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update, Agosto 2012, Gartner

Seguridad de la Información
Internet

El gobierno formal y el gobierno real

- Componentes fundamentales
  - Internet Protocol (IP)
  - Domain Name System (DNS)
  - Border Gateway Protocol (BGP)
  - Secure Socket Layer (SSL)
  - Network Time Protocol (NTP)

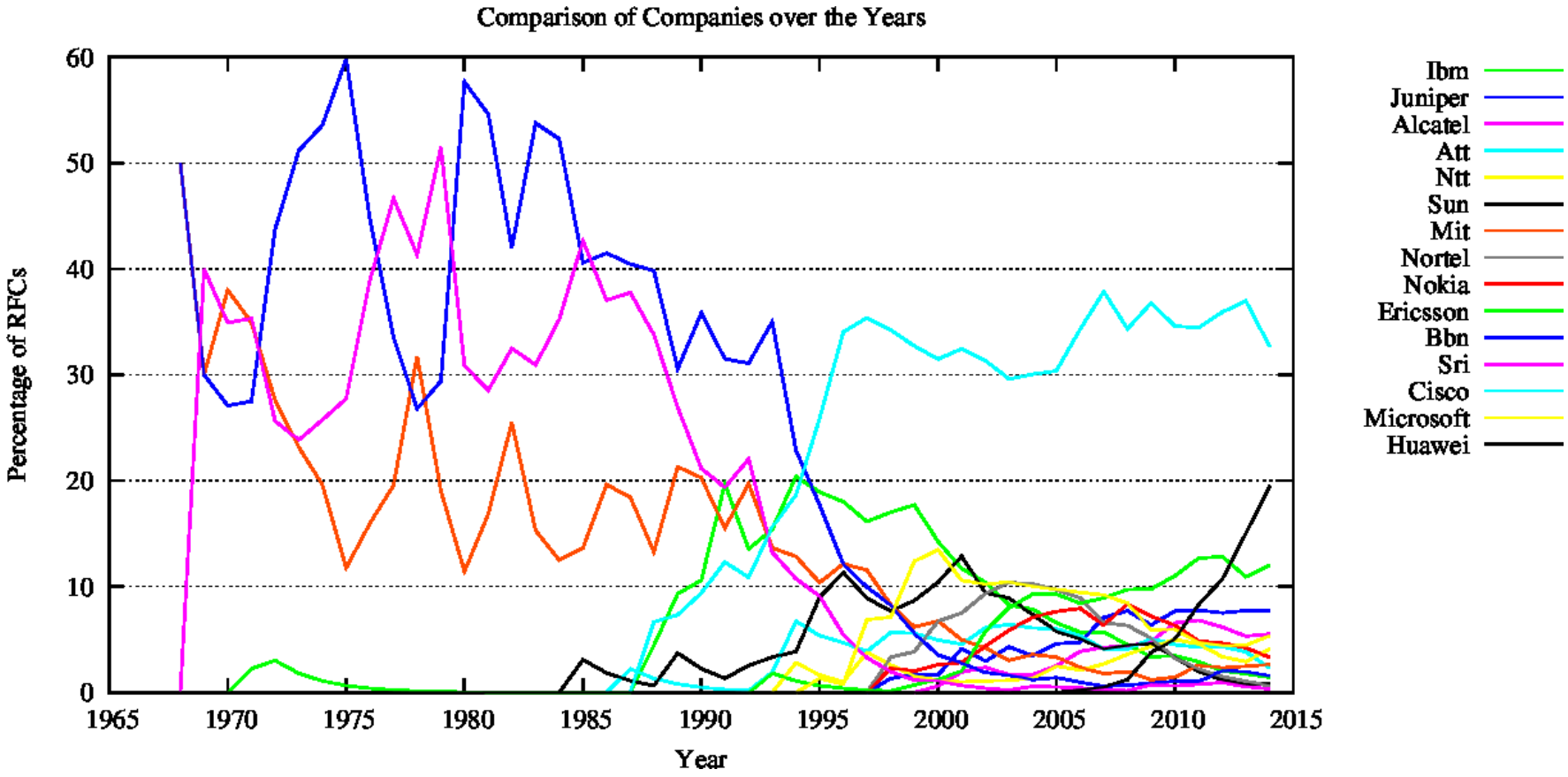
  En los últimos 15 años todos ellos "evolucionaron" hacia la centralización del comando y control de su funcionamiento

- 10 de 13 DNS root servers operan bajo jurisdicción de EEUU
  http://www.iana.org/domains/root/servers

- 3 autoridades certificantes (bajo jurisdicción de EEUU) firman mas del 75% de los certificados SSL
  http://www.netcraft.com/internet-data-mining/ssl-survey

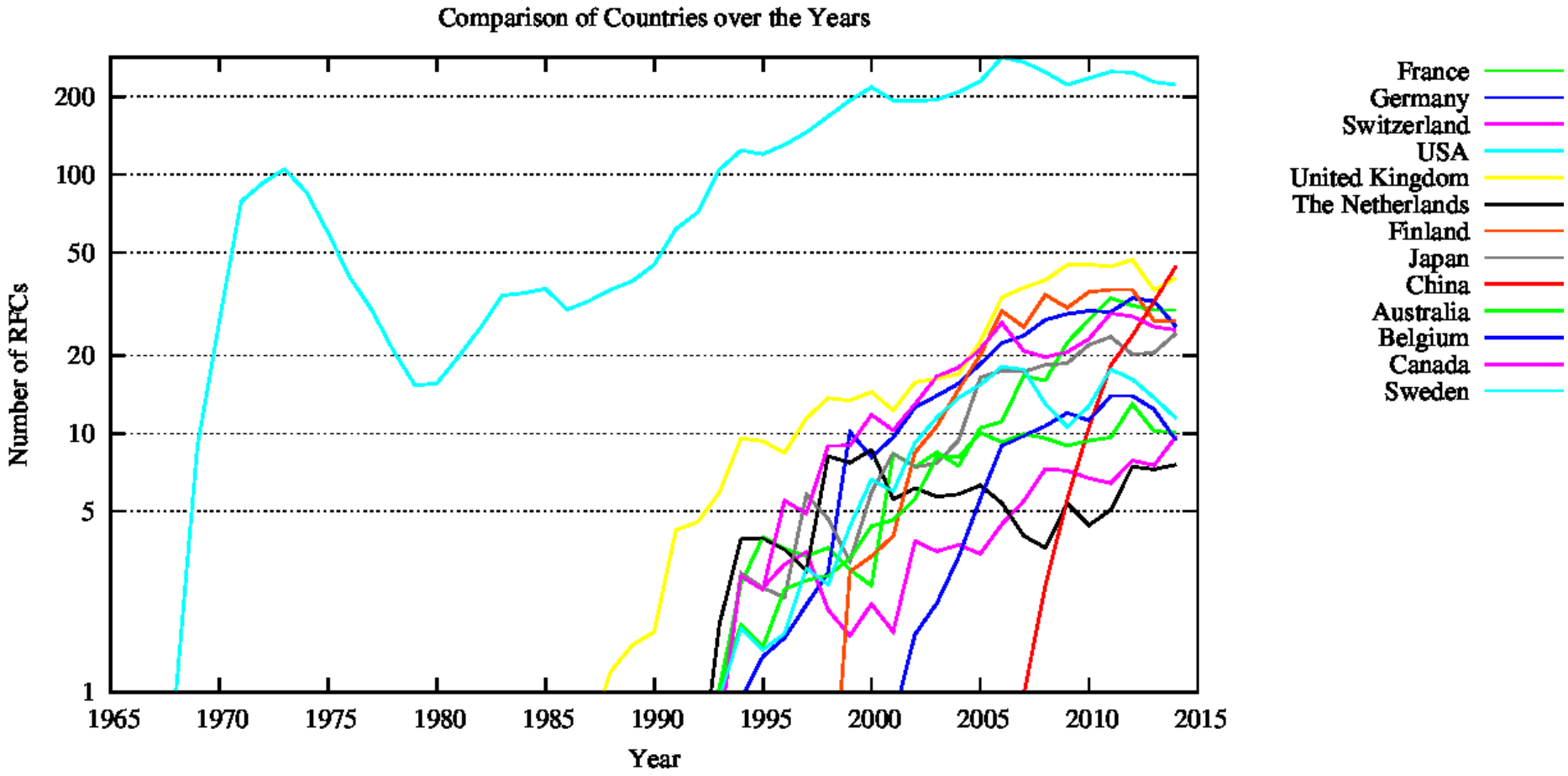
- Los 10 principales proveedores de inter-conectividad en Internet (Tier 1) son extra-regionales
  http://as-rank.caida.org/?mode0=org-ranking

Quienes definen los estándares técnicos ?



Fuente: http://www.arkko.com/tools/rfcstats/companydistrhist_norm.html

De dónde son los autores de los estándares técnicos?



Argentina:30 (0,34%) Brasil:7 (0,08%) México: 3 (0,03%) Colombia: (0,03%)

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

Seguridad de la Información
Herramientas técnico-legales

Algunas consideraciones necesarias

- Espionaje informático (*ciberespionaje*)

  Ley 25.520 "Inteligencia Nacional"

- Delito informático (*ciberdelito)*

  Ley 26.388 "Delito Informático"

  Ley 35.326 "Protección de los datos personales"

  Convenio sobre ciberdelincuencia (Budapest)

  - Panamá y Rep Dominicana, unicos paises signatarios de la región
  - Potencial efecto negativo sobre actividades de I+D (Articulo 6)

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

- Guerra cibernética (*ciberguerra*)

  - Wassenaar Arrangement (Dic. 2013)

  El "software de intrusión" agregado a la lista de tecnologías de uso dual con controles de exportación (Categoría 4)

  http://www.wassenaar.org/controllists/index.html

Guerra cibernética: Cuestiones no resueltas

- Qué es? Hace falta una definición precisa?
  La teoría del efecto cinético
  La teoría de la velocidad de la luz
  El 5to dominio
  Cuestiones Operativas, Tácticas y Estratégicas

- Disuación
- No proliferación
- Atribución

- Reglas del juego
  Jus ad Belum
  Jus in Bello

Tallinn Manual on International Law applicable to Cyber Warfare (OTAN)

Conclusiones

Claves para una estrategia nacional

- Tiene relevancia estratégica para nuestro país y nuestra región
- 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
- **Investigación, Desarrollo e Innovación**
  Claves para la soberanía tecnológica
  Ataque y Defensa son complementarios, ambos necesarios.
- Es necesario pero no suficiente:
  Políticas nacionales, regulación e implementación de controles
  Desarrollo del sector productivo
  Crear y robustecer un ecosistema sustentable

Email: stic@fundacionsadosky.org.ar

GRACIAS!