Ciberseguridad Nacional

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU·INFO SEGURIDAD DE LA INFORMACION AGASSI

Sobre Cristian Borghello

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate of Cloud Security Knowledge) desde 2014
- Creador y Director de Segu-Info
- Consultor independiente en Seguridad de la Información

Plain: אבגדהוזחטיכלמנסעפצקרשת
Cipher: תשרקצפעסנמלכיטחזוהדגבא

Atbash: cifrado simétrico hebreo (500AC)

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

Julio César (100AC)

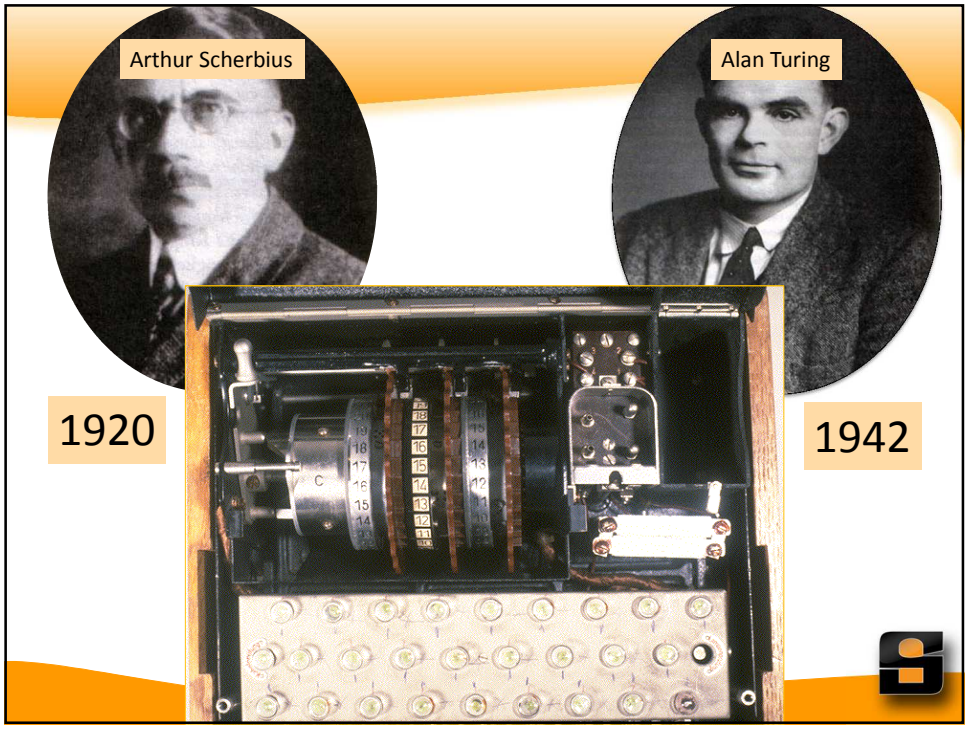
X Y Z A **B** C D E F ...

... A B C D **E** F G H I

Plutarco (50AC) → Escítala

Código Navajo


S.XVI
Johannes Trithemius
Blaise de Vigenère
POLYGRAPHIAE
PLAINTEXT LETTER
KEYWORD LETTER


Arthur Scherbius
Alan Turing
1920
1942


Whitfield Diffie
1976
Martin Hellman
RSA
Ronald Rivest
Adi Shamir
Leonard Adleman


Phil_Zimmermann
PGP
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

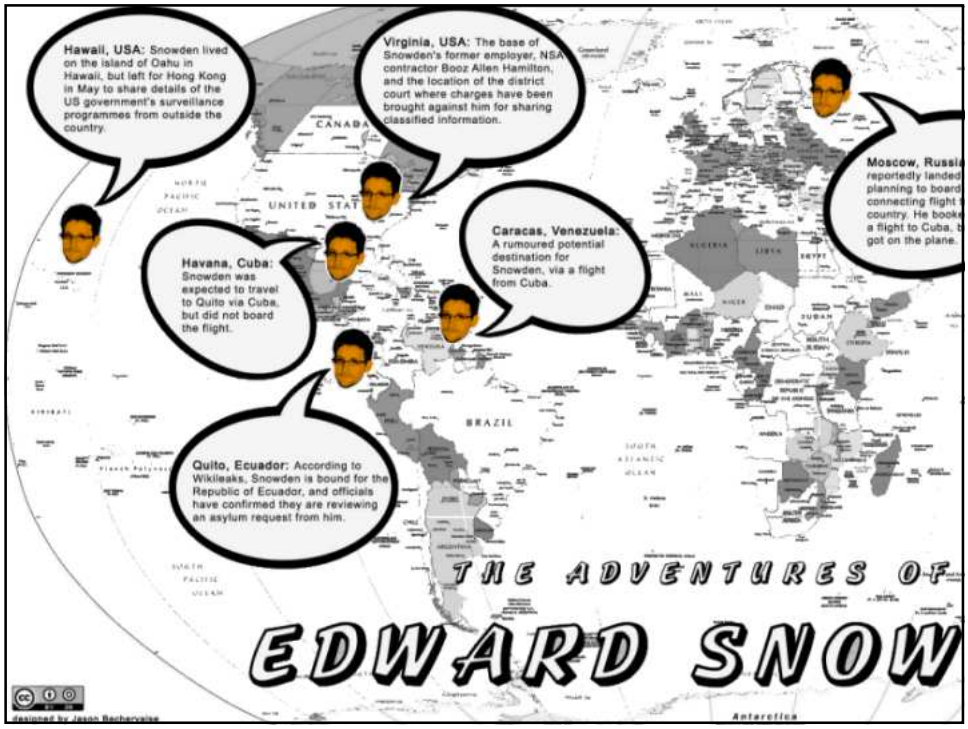
Usos típicos actuales

Correo electrónico seguro
GPG/PGP

Navegación anónima/privada
TOR

Almacenamiento seguro
Truecrypt (y quien le siga)

"No sé con qué armas se librará la Tercera Guerra Mundial, pero en la Cuarta Guerra Mundial usarán palos y piedras"


Hawaii, USA: Snowden lived on the island of Oahu in Hawaii, but left for Hong Kong in May to share details of the US government's surveillance programmes from outside the country.
Virginia, USA: The base of Snowden's former employer, NSA contractor Booz Allen Hamilton, and the location of the district court where charges have been brought against him for sharing classified information.
Moscow, Russia: reportedly landed planning to board connecting flight country. He booke a flight to Cuba, b got on the plane.
Caracas, Venezuela: A rumoured potential destination for Snowden, via a flight from Cuba.
Havana, Cuba: Snowden was expected to travel to Quito via Cuba, but did not board the flight.
Quito, Ecuador: According to Wikileaks, Snowden is bound for the Republic of Ecuador, and officials have confirmed they are reviewing an asylum request from him.
CANADA
UNITED STAT
BRAZIL
THE ADVENTURES OF
EDWARD SNOW

Ciberespacio: alucinación consensual experimentada por operadores en todas las naciones... Una representación gráfica de la información abstraída de los bancos de computadoras del sistema humano. Una complejidad inimaginable.

Neuromante - William Gibson

Ciberespacio

- Ciberespacio: dominio global en el entorno de la información y que consiste en redes dependientes de infraestructuras tecnológicas

  DoD Dictionary of Military Terms (Division, J-7, 10/17/2008)

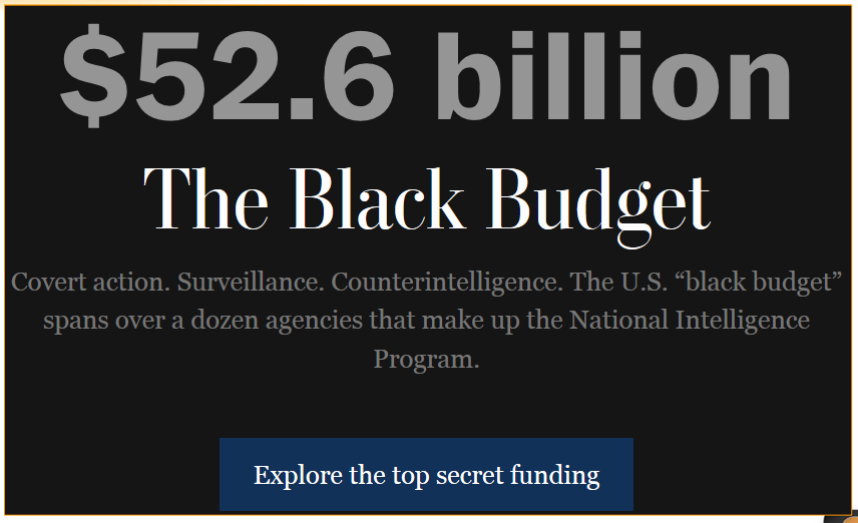
- El ciberespacio se ha convertido en un nuevo campo de batalla. Ha adquirido una importancia similar a la que tienen los otros -tierra, mar, aire y espacio-

La seguridad es un problema real que afecta la vida de los ciudadanos

Lucha en el ciberespacio

Es el uso de hacking para llevar a cabo ataques contra recursos estratégicos y/o tácticos de un blanco, para los propósitos de espionaje o sabotaje

Black Budget (Snowden)



Black Budget (Snowden)

En 2011, los servicios de inteligencia estadounidenses lanzaron 231 ciberataques, principalmente contra Irán, Rusia, China y Corea del Norte

"Se introducen en redes extranjeras para ponerlas bajo un discreto control estadounidense"

http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

Adaptación continua

El desarrollo sistemático y generalizado de aplicaciones y sistemas para la protección surge a principios del siglo XXI, sobre todo a raíz de los atentados de 11 de septiembre en Nueva York y de los posteriores en Madrid, Londres, Bombay

- Recopilar la mayor cantidad de información disponible
- Adaptar la información recogida
- Buscar patrones, coincidencias y seguimientos
- Ayudar a la toma de decisiones y ejecutar operaciones

CiberOperaciones

Según una directiva presidencial emitida en octubre de 2012, las agencias estadounidenses definen Offensive CyberOperation como:

"actividades destinadas a manipular, alterar, bloquear, degradar o destruir información residente en computadoras y redes del adversario (o las mismas computadoras y redes)"

GENIE

- GENIE es un proyecto de EE.UU. que, con un presupuesto de USD 652 millones, implanta programas espías en decenas de miles de sistemas
- A fines de 2013, GENIE controlaba al menos 85.000 programas implantados en máquinas escogidas estratégicamente alrededor del mundo (4 veces más que en 2008)
- Stuxnet, atacó en 2010 el programa nuclear iraní
- Programa “Juegos Olímpicos” de Israel y EE.UU.

Hacktivismo

Date	Notifier	H	M	R	L	Domain	OS	View
2014/07/21	HACKED BY LIBERO	H	M			salsipuedes.gob.ar	Linux	mirror
2014/07/21	Red Eye	H	M			inclusiondigital.gob.ar	Linux	mirror
2014/06/05	SultanHaikal		M	R		www.licencias.lujan.gob.ar/h4x...	Linux	mirror
2014/06/04	DARKWAR2	H	M			www.marcospaz.gob.ar	Linux	mirror
2014/05/21	HACKED BY LIBERO	H		R		intema.gob.ar	Linux	mirror
2014/05/20	Fatal Error	H	M	R		www.ssn.gob.ar	Win 2000	mirror
2014/05/20	Hmei7		M			hcdmarcospaz.gob.ar/qq.htm	Linux	mirror
2014/05/15	DiE_AucH	H	M			www.juzfaltasvalleviejo.catama...	Linux	mirror
2014/05/15	DiE_AucH	H	M			www.pasodesanfrancisco.gob.ar	Linux	mirror
2014/05/14	Bayz96	H				duran.gob.ar	Win 2008	mirror
2014/05/13	HACKED BY LIBERO	H	M			www.villadelasrosas.gob.ar	Linux	mirror
2014/05/07	rooterror					www.semanadelaciencia.mincyt.g...	Linux	mirror
2014/05/05	Hmei7					www.htc.gba.gob.ar/web/images/...	Linux	mirror
2014/05/05	EvreN	H	M			trabajo.salta.gob.ar	Linux	mirror
2014/05/05	palakololo					www.villademerlo.gob.ar/x.txt	Win 2003	mirror
2014/05/03	Tanpa Bicara		M			www.noetinger.gob.ar/0.htm	Linux	mirror
2014/05/03	EvreN	H		R		www.trabajosalta.gob.ar	Linux	mirror
2014/04/17	eRRoR 7rB			R		riogrande.gob.ar/mun/images/jd...	Linux	mirror
2014/04/16	d3b~X		M	R		teatrovera.gob.ar/cartelera/im...	Linux	mirror
2014/04/09	LUN4T1C0		M			web.hospitalgoya.gob.ar/x.txt	Linux	mirror
2014/03/31	LUN4T1C0		M			cruzdelosmilagros.gob.ar/x.txt	Linux	mirror
2014/03/31	LUN4T1C0		M			turismogoya.gob.ar/x.txt	Linux	mirror
2014/03/27	[Nyu]	H		R		www.portena.gob.ar	Linux	mirror
2014/03/23	HACKED BY LIBERO	H	M	R		mariajuana.gob.ar	Linux	mirror
2014/03/23	HACKED BY LIBERO	H		R		www.biblioargentina.gob.ar	Linux	mirror

Ciberespionaje y Ciberterrorismo

Ciberespionaje: medidas adoptadas por un país para penetrar sistemas de otras naciones y robar información

Ciberterrorismo: acción violenta que infunde terror y es realizada a través de Internet

- Es considerado un tipo de guerra asimétrica (relación entre la energía inicial y el posterior daño)
- Rápido
- Bajo costo
- Alcanza a cualquier nación
- Si se ataca infraestructuras críticas, es altamente dañino

Cyberwarfare

Ciberguerra (*cyberwarfare):* conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas propios

- Los ataques estan orientados a bajar sitios y redes oficiales, desactivar servicios críticos, esenciales o vitales, agotar sus recursos o robar información clasificada
- Tiene el adicional que los civiles pueden participar en el ciberataque

Cyber War, 2012 - Richard A. Clarke
http://www.amazon.es/Cyber-War-Threat-National-Security/dp/0061962244
Cyberdeterrence and Cyberwar, 2009 - Martin C. Libicki
http://www.rand.org/pubs/monographs/MG877.html - http://amzn.to/pnYAxe

Historia de la Ciberguerra (I)

- En 1998 EE.UU. ataca sistemas de defensa de Serbia para facilitar un bombardeo posterior
- En 2007 aparece una botnet rusa controlada y dirigida contra sitios de Estonia. *Russian Business Network* (RBN), quizás la más grande red de mafia existente
- En 2008, Georgia y Rusia mantienen sendos ataques sobre sus sitios
- En 2009 se conoce *"GhostNet"* (China), una operación orientada a robar información de 100 gobiernos y empresas
- Se detecta la *"Operación Aurora"*, orientada a robar secretos de una treintena de multinacionales

Historia de las ciberguerras: http://bit.ly/nrYbPa

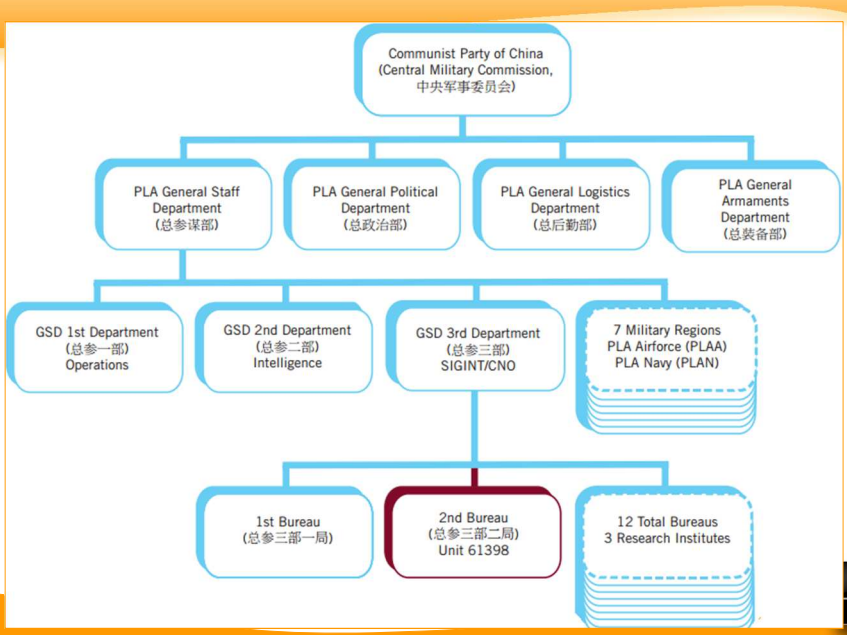
Historia de ciberguerra (II)

- En 2010, Iran es atacado a través del gusano Stuxnet
- India y Pakistan sostienen sus ataques desde finales de 2010
- El DoD EE.UU. anuncia en 2010 la creación del Cibercomando de Fuerzas Armadas (ARFORCYBER)
- La NSA anuncia la creación del centro de ciberseguridad *National Cyber Range*
- En 2011 Alemania inaugura su centro nacional de ciberseguridad (NCA)
- Se conoce *"ShadyRat"*, una operación dirigida a 72 organizaciones públicas y privadas
- En 2012 se descubre Flame

Historia de ciberguerra (III)

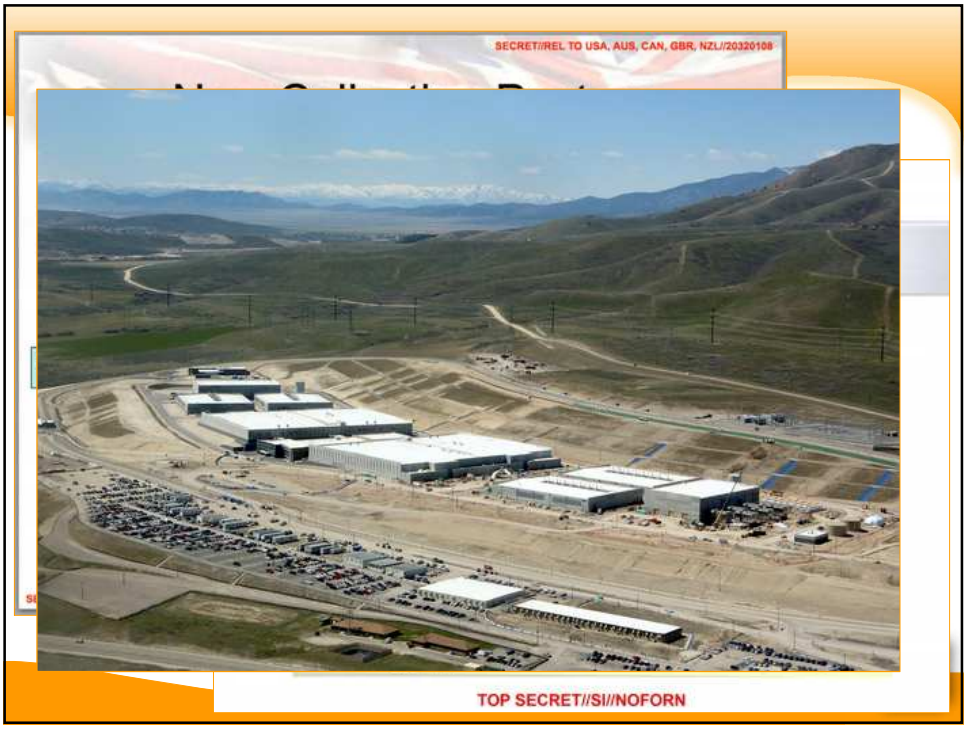
- 02/2013, Israel anuncia su programa nacional contra ciberataques: *"cúpula de acero digital"*
- Se encuentra *"Octubre Rojo"*, el malware diplomático
- En 02/2013, Mandiant publica el informe "APT1" con un estudio sobre ciberespionaje chino
- EE.UU. toma la potestad de ordenar "ciberataques preventivos"
- ENISA actualiza ejercicios para los CERT/CSIRT
- 06/2013, NetTraveler, APT que afecta varios países
- 10/2013, *"Operación Troya"* contra Corea del Sur
- 09/2013, Rusia incorpora unidad de ciberguerra a sus fuerzas armadas
- 11/2013, *"Operación Hangover"* ciberespionaje del gobierno Indio
- 02/2014, aparece The Mask/Careto un APT de ciberespionaje que involucra diarios argentinos y españoles
- 07/2014, Aparece Havex, un RAT que ataca sistemas industriales

Historia de ciberguerra (III)

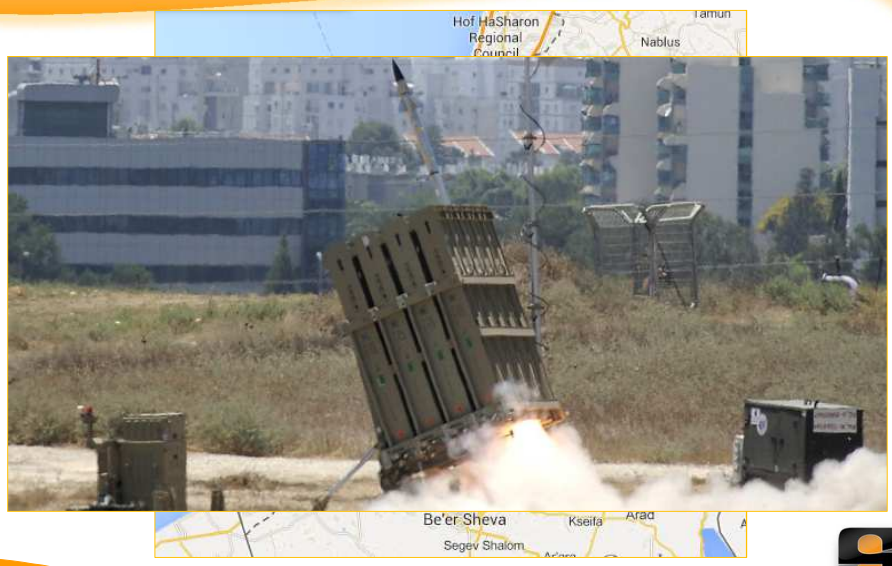


PRISM

- PRISM es un programa “confidencial” de vigilancia a cargo de la Agencia de Seguridad Nacional (NSA), activo desde 2007
- EE.UU. podría estar espiado a más de 35 líderes
- Se conoció en los informes y documentos filtrados por Edward Snowden en junio de 2013 y cada mes se filtra nueva información
- PRISM espía correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, inicio de sesión, llamadas, transferencia de archivos, redes sociales…
- Microsoft, Google, Apple y Facebook eran conscientes a través de *Foreign Intelligence Surveillance Act (*FISA)



Conflicto en Gaza (I)



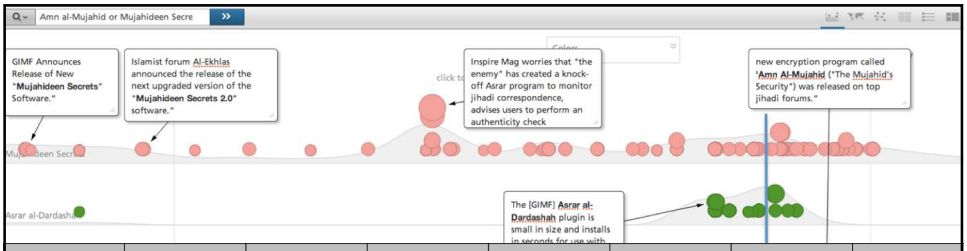
Conflicto en Gaza (II)

¿Todavía se puede dudar que la ciberseguridad afecta a las personas?

- DES, fue modificado y certificado por NIST en 1976 (FIPS PUB 46)
- AES (Rijndael), el estándar actual de cifrado simétrico, fue evaluado y aprobado por NIST (FIPS PUB 197)
- RSA, el algoritmo asimétrico más utilizado en conexiones SSL/TLS/HTTPS, fue validado por NIST (FIPS PUB 186)

National Institute of Standards and Technology
U.S. Department of Commerce

http://es.wikipedia.org/wiki/Instituto_Nacional_de_Normas_y_Tecnolog%C3%ADa



Product	Release Date	Organization	Key Feature	Execution Platform	Messaging Platform	Crypto Method	Delivery
Mujahideen Secrets (Asrar al-Mujahideen)	2007	GIMF (AQ main)	Encryption of messages or file exchange	Windows with recent instructions for Mac porting	Primarily email	Public/Private key, RSA based, 2048 bit	Windows app
Asrar al-Dardashah	February 6, 2013	GIMF (AQ main)	Encryption of instant message traffic	Pidgin platform, Windows installer	Messaging (Pidgin): Yahoo, Google, AOL, etc.	Based on Mujahideen Secrets encryption	Pidgin plugin
Tashfeer al-Jawwal (Mobile Encryption Program)	September 4, 2013	GIMF (AQ main)	Encryption of SMS traffic	Android/Symbian	SMS	Twofish, use SSL for transport	Android/Symbian apps
Asrar al-Ghurabaa	November 27, 2013	ISIS (AQ adversary)	Pure text encryption	Website, accessible via Tor	Platform independent, just encrypts	"A special or unique encryption algorithm"	Website
Amn al-Mujahid	December 10, 2013	Al-Fajr Technical Committee (FTC)	Text encryption	Windows OS	Email, SMS, instant messaging	AES/Twofish	Windows app
Amn al-Mujahid (Mobile)	June 7, 2014	Al-Fajr Technical Committee (FTC)	Text encryption	Android	SMS	AES/Twofish	Android app

http://blog.segu-info.com.ar/2014/08/historia-de-la-criptografia-utilizada.html

Programas internacionales

- Guerra Fría - Wassenaar Arrangement
- 05/2012 - Informe europeo sobre la protección de infraestructuras críticas de información
- 03/2013 - Manual de Tallinn sobre el Derecho Internacional aplicable a los Cyber Warfare
- 02/2014 - Framework for Improving Critical Infrastructure Cybersecurity
- ¿Argentina?

http://www.wassenaar.org/
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
http://ccdcoe.org/tallinn-manual.html

Puntuación de países

Metodología elaborada por Robert Lentz, presidente de *Cyber Security Strategies* del DoD de EE. UU. Es un modelo de madurez de ciberseguridad para gestionar de manera eficaz un ciberataque:

★★★★★	Ningún país consiguió las 5 estrellas
★★★★½	Finlandia, Israel y Suecia
★★★★	Alemania, Dinamarca, España, Estonia, Estados Unidos, Francia, Países Bajos y Reino Unido
★★★½	Australia, Austria y Japón
★★★	Canadá, China, Italia, Polonia y Rusia
★★½	Brasil, India y Rumanía
★★	México

Cyber, Identity and Information Assurance
http://www.dintel.org/Documentos/2011/Foros/ses2Mcafee/lentz.pdf

Por dónde empezar (I)

- Cooperación Internacional
- Definir una estrategia de defensa conjunta
- Definir una estrategia de respuesta conjunta
- Definir una estrategia de comunicación alternativa ante un incidente
- Definir herramientas, controles y métricas regionales
- Estudiar, analizar y crear protocolos de comunicación y herramientas de gestión

Por dónde empezar (II)

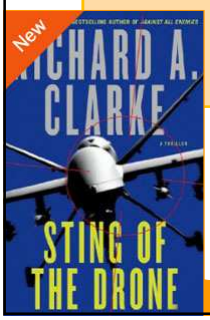
- Investigar tratados actuales
- Crear un "reglamento" gubernamental sobre el uso de Internet y el Ciberespacio
- Aumentar los recursos para la ciberdefensa (públicos y privados)
- Aislar las infraestructuras críticas

Estrategia, políticas a largo plazo, política de estado, recursos

"Si gastas más en café que en seguridad, serás hackeado… Y mereces ser hackeado"

(…y tendrás una úlcera)

Richard A. Clarke



Agradecimientos

A la Comunidad de Segu-Info que todos los días [nos] aporta conocimiento a través de los distintos grupos de discusión

¡GRACIAS!

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU·INFO
SEGURIDAD DE LA INFORMACION

AGASSI