nic.br cgi.br | cert.br

Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSeg 2019

São Paulo, SP

04 de setembro de 2019

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

The Honeynet PROJECT

Criação:

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Foco das Atividades

- Atuar como ponto de contato nacional para notificação de incidentes
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências
- Transferir o conhecimento adquirido através de cursos, boas práticas e materiais de conscientização

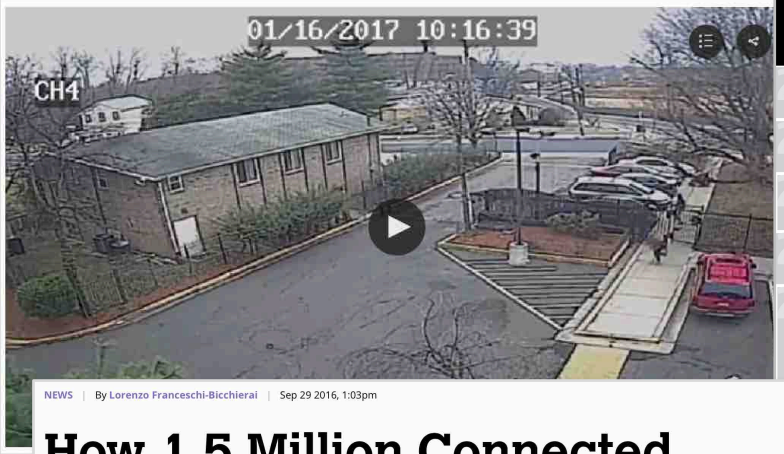
Segurança, Privacidade, Ética e Geopolítica: Como Isso Pode Afetar Minha Pesquisa?

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

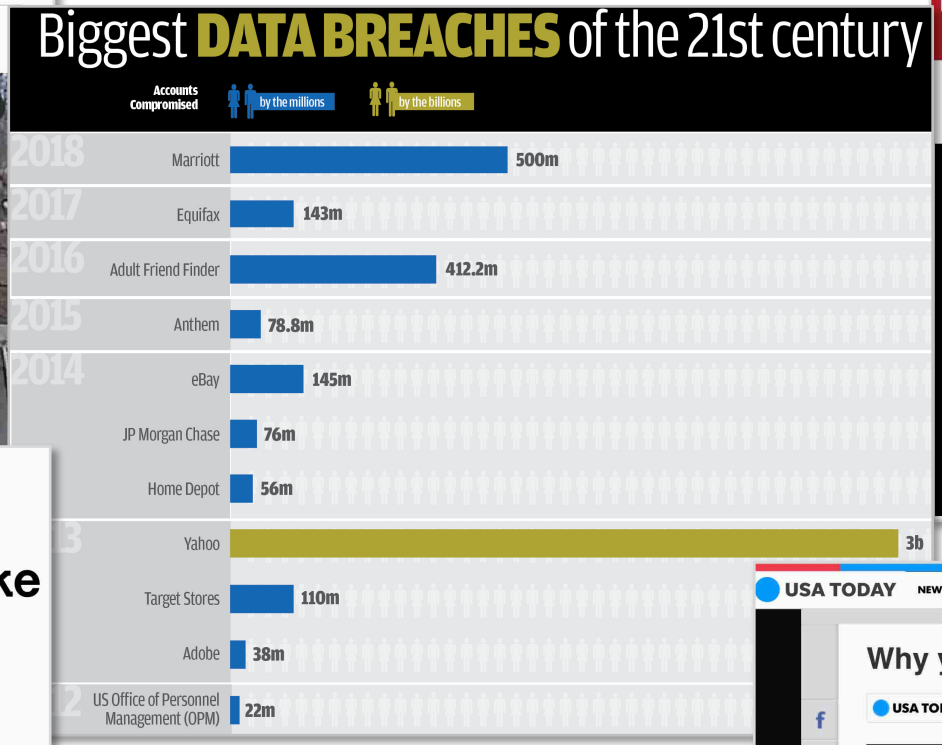
cert.br nic.br cgi.br

Officials: DC security cameras hacked 8 days before inauguration by man, woman in London

by John Gonzalez/ABC7 | Friday, February 3rd 2017



Biggest DATA BREACHES of the 21st century



Hacking Intelligent Buildings: Pwning KNX & ZigBee Networks

NEWS | By Lorenzo Franceschi-Bicchierai | Sep 29 2016, 1:03pm

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

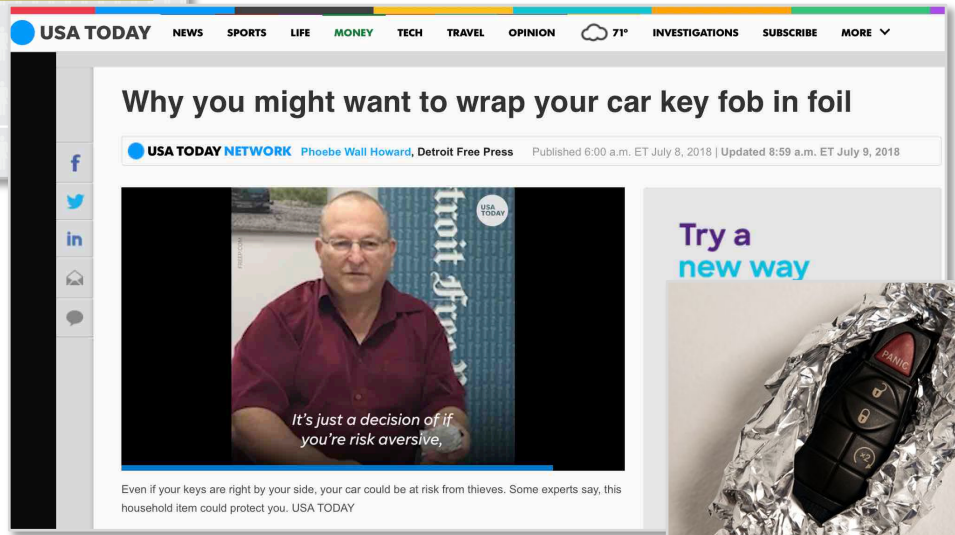
Ad closed by Google

Report this ad | Why this ad?

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.

SHARE | TWEET

Last week, hackers forced a well-known security journalist to take down his site after hitting him for more than two days with an unprecedented flood of traffic.



https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
https://wjla.com/news/local/officials-dc-security-cameras-hacked-8-days-before-inauguration-by-man-woman-in-london
https://conference.hitb.org/hitbsecconf2018ams/sessions/hacking-intelligent-buildings-pwning-knx-zigbee-networks/
https://www.usatoday.com/story/money/nation-now/2018/07/08/wrap-car-key-fob-foil/762338002/

Instituições Focadas em Segurança não estão Melhores: **Invasão de Sistemas Altamente Protegidos**

- Comprometimento da RSA/EMC, para furto de material criptográfico – levou ao comprometimento do DoD (*US Department of Defense*)
  https://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex991.htm

- Comprometimento do *Office of Personnel Management*, para furto dos antecedentes de todos os funcionários do Governo Americano
  https://www.opm.gov/cybersecurity/cybersecurity-incidents

- Caso DigiNotar: Comprometimento da Autoridade Certificadora da Holanda – usada para gerar chaves falsas do Google, usadas em espionagem no Irã
  http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html

- Alegado comprometimento da empresa Kaspersky para acesso a documentos em sua nuvem – vazamento de documentos da NSA para a Rússia – em tese, a NSA foi alertada por Israel (que admitiu publicamente ter invadido a Kaspersky)
  https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

ShadowHammer Targets Multiple Companies, ASUS Just One of Them

By Sergiu Gatlan — April 23, 2019 — 09:40 AM — 0

ASUS was not the only company targeted by supply-chain attac
ShadowHammer hacking operation as discovered by Kaspersky
organizations having been infiltrated by the attackers.

As further found out by Kaspersky's security researchers, ASUS
successfully compromised by trojanizing one of the company's
named ASUS Live Updater which eventually was downloaded a
of tens of thousands of customers according to experts' estimati

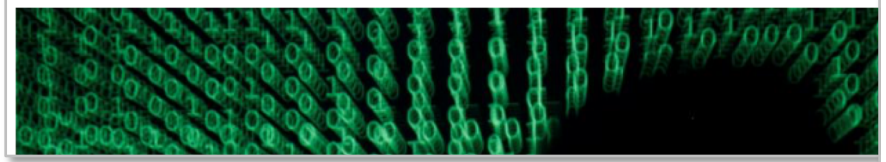
The tampered with binaries were signed using a legitimate certi
attackers avoid breaking the digital signature and having the ma

CYBER RISK AUGUST 5, 2019 / 3:28 PM / A MONTH AGO

North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report

Michelle Nichols — 4 MIN READ

UNITED NATIONS (Reuters) - North Korea has generated an estimated
for its weapons of mass destruction programs using "widespread and inc
sophisticated" cyberattacks to steal from banks and cryptocurrency exch
according to a confidential U.N. report seen by Reuters on Monday.



28 AUG 2019 NEWS

NATO: Attack Like WannaCry Could Prompt "Collective Defense Commitment"

Michael Hill
Editor , Infosecurity Magazine
Email Michael
Follow @MichaelInfosec

NATO secretary general Jens Stoltenberg has gone on record to state that a cyber-attack - such as the WannaCry outbreak of 2017 - would prompt a "collective defense commitment" from the intergovernmental military alliance between 29 North American and European countries.

https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyber-attacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX
https://www.bleepingcomputer.com/news/security/shadowhammer-targets-multiple-companies-asus-just-one-of-them/
https://www.infosecurity-magazine.com/news/nato-security-general-collective/

Enquanto isso Fóruns de Governança Refletem a Confusão: **Segurança vs. Privacidade**

"*Para ter segurança é preciso abrir mão da privacidade*"

"*Na Internet, não se deve analisar nem os cabeçalhos dos pacotes*"

"*Órgãos investigativos precisam ter acesso a comunicações criptografadas para serem efetivos*"

"*Para ter privacidade deve-se eliminar*

- *logs*
- *cookies*"

"*Usar criptografia em todas as comunicações garante privacidade*"

Algumas Agências e Governos Exploram a Confusão: **Controle vs. Segurança vs. Privacidade**

Medidas de Segurança

- criptografia
- controle de acesso
  - garantir que só você acessa sua conta de *e-mail*; que ninguém invade seu perfil do *twitter,* etc
  - garantir que só você acessa seu *Internet banking*
- amazenar *logs* de acordo com políticas bem definidas e para fins específicos de segurança e funcionamento da rede

Medidas de Controle

- acesso excepcional a conteúdo criptografado
- armazenar 100% do tráfego
- armazenar, inspecionar e processar de forma centralizada *logs*, consultas DNS, acessos, conteúdo, etc
  - de múltiplas redes
  - correlacionando estas informações
  - com **motivações diversas e difusas**

Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications
http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Ecossistema Global de Governança do “Espaço Cibernético”

cert.br nic.br cgi.br

Segurança e Combate a Abusos na Internet:
Fóruns Técnicos Internacionais

FIRST – *Forum of Incident Response and Security Teams*

- Criação: 1990
- Membros: 492 CSIRTs, em 92 países, participantes de todos os setores (dados de 01/09/2019);

APWG – (originalmente *AntiPhishing Working Group*)

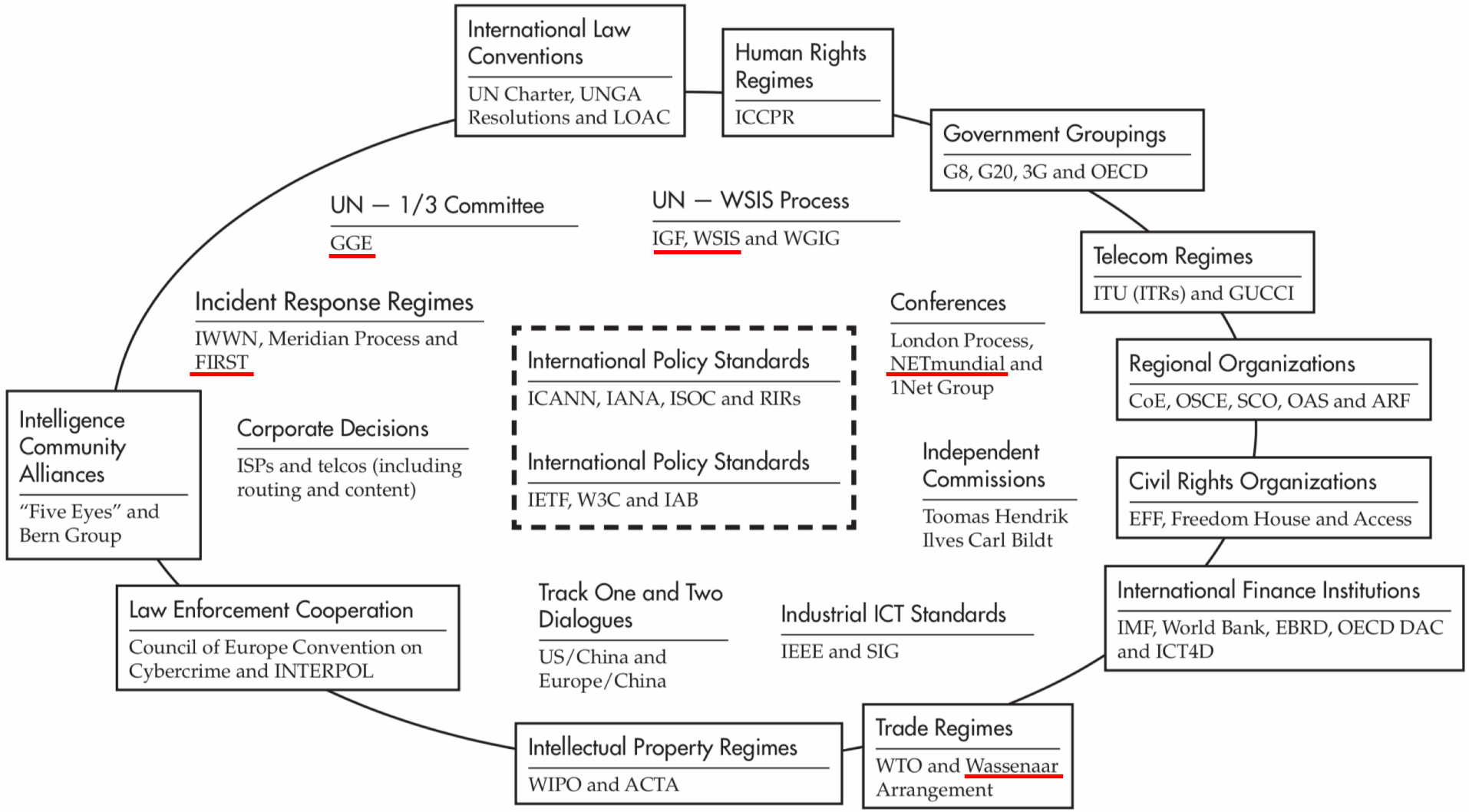
- Criação: 2003
- Membros: mais de 2.000 organizações, participantes de todos os setores, incluindo organizações internacionais;

M^{3}AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group*

- Criação: 2004
- Membros: mais de 200 membros da Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Criação: 2017
- Membros: Comunidade Internet em Geral; mantido pelo LACNOG e M^{3}AAWG.



The Regime Complex for Managing Global Cyber Activities
Global Commission on Internet Governance Paper Series No. 1
May 20, 2014, Joseph S. Nye Jr.
https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

WSIS:
Declaration of Principles

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) **Building confidence and security in the use of ICTs**

35. Strengthening the trust framework, **including information security and network security, authentication, privacy and consumer protection**, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

CGI.br:
Princípios para a Governança e Uso da Internet no Brasil

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

Fevereiro de 2009

[...]

8. **Funcionalidade, segurança e estabilidade**

A **estabilidade, a segurança e a funcionalidade** globais da rede devem ser preservadas de forma ativa **através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas**.

[...]

http://www.cgi.br/resolucoes/documento/2009/003

NETmundial:
Internet Governance Principles

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, **the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness** in addressing risks and threats to security and stability of the Internet **depends on strong cooperation among different stakeholders**.

[...]

http://netmundial.br/netmundial-multistakeholder-statement/

UN GGE

UNODA
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS

UN General Assembly, Group of Governmental Experts, Document A/70/174

22 July 2015

[...]

> **States should not** conduct or knowingly support activity to **harm the information systems of the authorized emergency response teams** (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

[...]

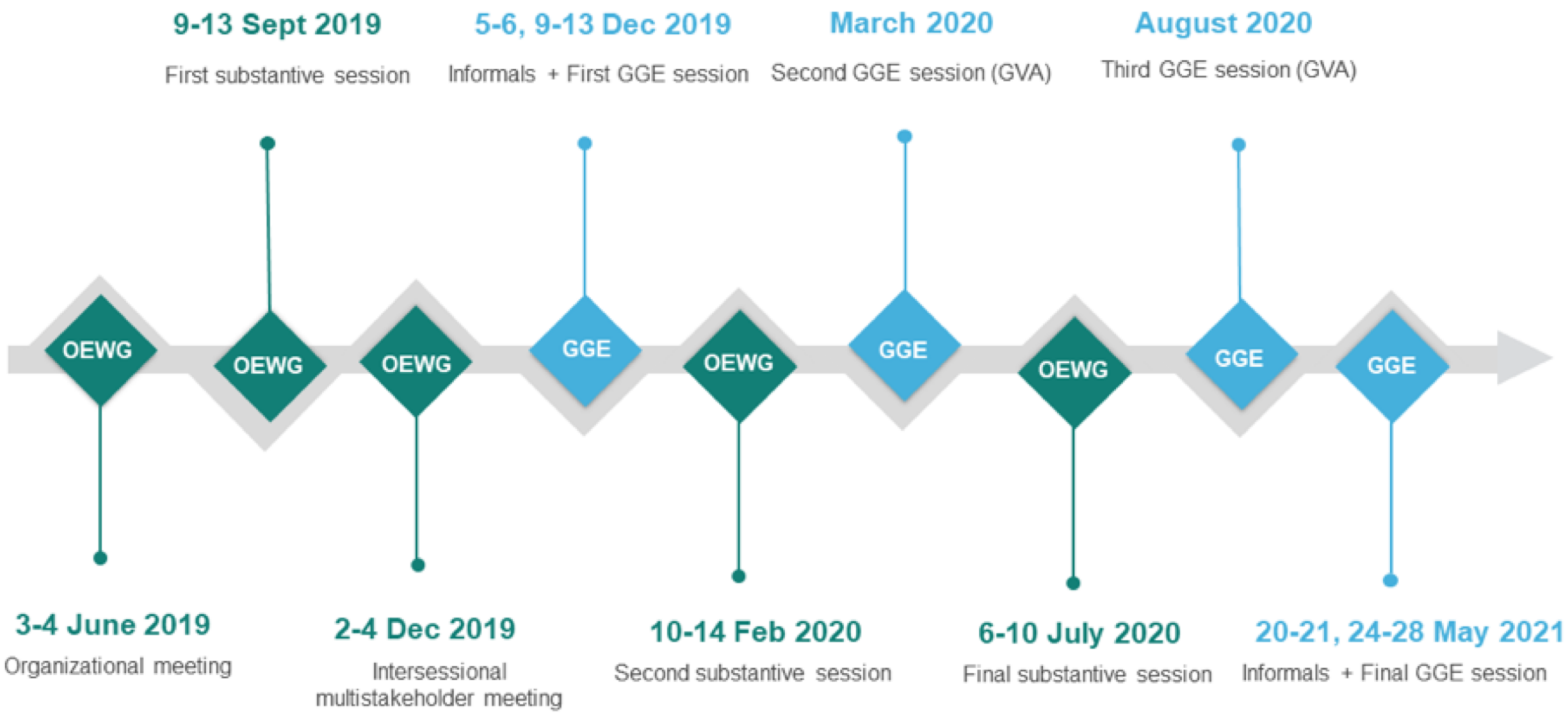
https://undocs.org/A/70/174

UN GGE

UNODA
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS

“In December 2018, the General Assembly established two processes to discuss the issue of security in the use of ICTs during the period of 2019-2021, an Open-ended Working Group and a Group of Governmental Experts.”

Tentative GGE and OEWG timeline (2019-2021)



https://www.un.org/disarmament/ict-security/

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

- Grupo de 42 países criado após o final da Guerra Fria para controlar a exportação de armas e tecnologias de uso dual

  Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

- 2013 – inserção de "*intrusion software*" na lista de itens controlados
  - ***Scope of the New Entries***

    Systems, equipment, components and software specially designed for the ***generation, operation or delivery of, or communication with, intrusion software*** *include* ***network penetration testing products*** *that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software* ***includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices****.*

https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies – December 2017

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.

[...]

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

Note 1 **4.E.1.a. and 4.E.1.c. do not apply to 'vulnerability disclosure' or 'cyber incident response'.**

Note 2 Note 1 does not diminish national authorities' rights to ascertain compliance with 4.E.1.a. and 4.E.1.c.

Technical Notes

1. **'Vulnerability disclosure' means** the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.
2. **'Cyber incident response' means** the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident.

[...]

https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

GCSC - *Global Commission on the Stability of Cyberspace*

"[...] ***Conflict between states*** *will take new forms* [...] *increasing* ***the risk of undermining the peaceful use of cyberspace*** *to facilitate the economic growth and the expansion of individual freedoms.*

In order to counter these developments*, the Global Commission on the Stability of Cyberspace* ***will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace****.* [...]

- "*Call to Protect the Public Core of the Internet*"

  "state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."

  https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf

- "N*orm Package Singapore*

  Norm to Avoid Tampering

  Norm Against Commandeering of ICT Devices into Botnets

  Norm for States to Create a Vulnerability Equities Process

  Norm to Reduce and Mitigate Significant Vulnerabilities

  Norm on Basic Cyber Hygiene as Foundational Defense

  Norm Against Offensive Cyber Operations by Non-State Actors"

  https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

https://cyberstability.org

Plenary Panel: Cyberstability and the Future of the Internet – NATO CCDCOE CyCon 2017, https://youtu.be/FDBTtawj6Ms

Como Conciliar um Sistema de Normas Territoriais às Realidades de um Cenário Digital e Interconectado?

- A Internet realmente não tem fronteiras
- Ocultar a fonte dos ataques é muito fácil
- “Atribuição” é muito difícil
- Sistemas críticos e sistemas de uso geral compartilham o mesmo *software*
  - todos os países usam o mesmo *software*
- Aumentar a segurança depende de as vulnerabilidades serem descobertas, conhecidas e corrigidas
- As leis e normas são territoriais
- Governos historicamente não confiam uns nos outros
- Forças Militares e de Segurança Nacional aplicam a lógica da dissuasão (*deterrence*) no cenário digital
  - “estocar armas” (i.e. vulnerabilidades)
  - [tentar] impedir “inimigos” de ter acesso a estas “armas”

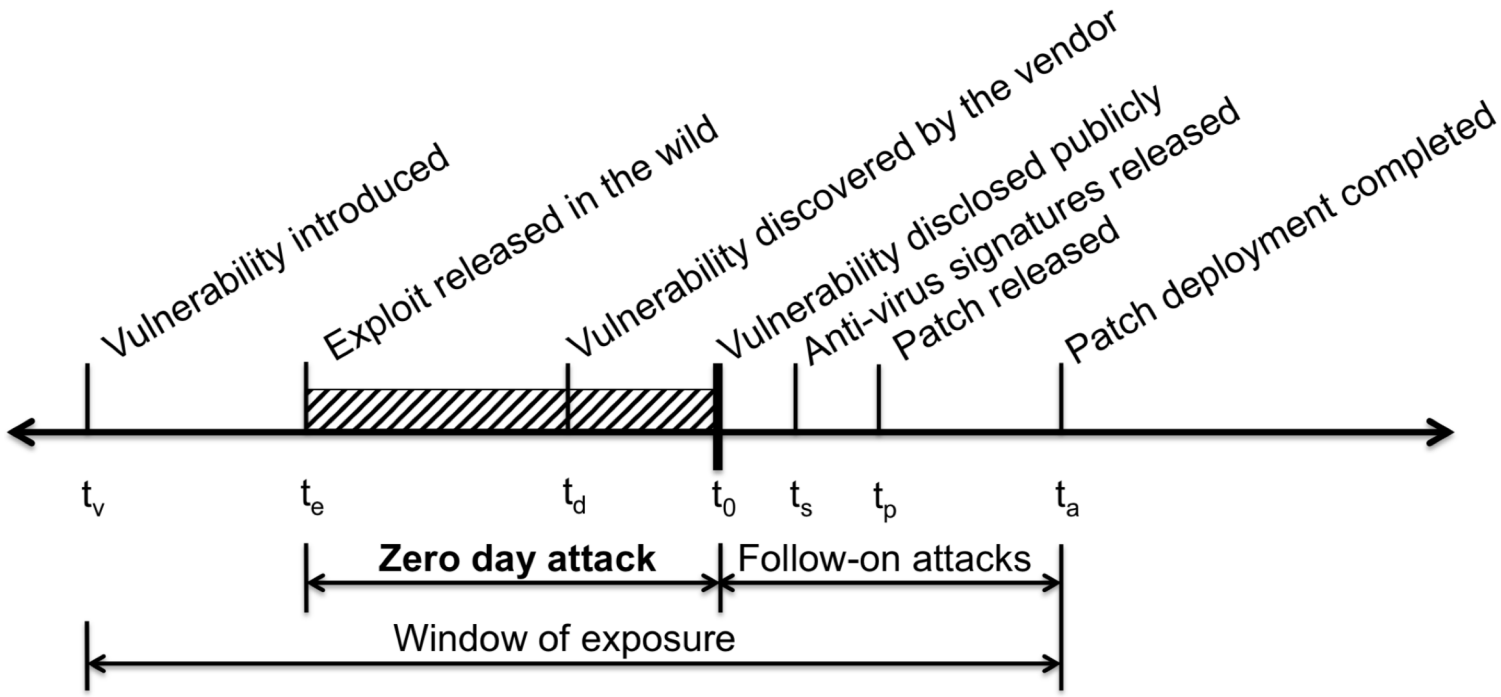
Estocar “armas” nos ajuda proteger os sistemas e redes?
Responsible Disclosure vs. Stock Pilling Vulnerabilities

Complicadores do cenário

- Vulnerabilidades descobertas pelos governos e mantidas em “segredo”
- Mercado de compra e venda (*brokering*) de *zero days*
  - Ex.: *Zerodium* e *Absolute Zero-Day™*
  - Governos são os principais compradores dos *brokers* legítimos
  - “Pesquisadores” tendem a vender para quem pagar mais
  - Programas de *Bug Bounty* dos fabricantes não conseguem competir

► **Dura verdade: só há *patches* se o fabricante conhece a vulnerabilidade, fora isso, todos estamos vulneráveis**

Attack Timeline



Fonte: ***Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World Proceedings of the 2012 ACM Conference on Computer and Communications Security***
http://doi.acm.org/10.1145/2382196.2382284

Consequências Não Intencionais de Estados Estocando “Armas”: Do *EternalBlue* ao *WannaCry*

2012 (ou antes) – NSA descobre uma vulnerabilidade grave nos sistemas Windows, que permite comprometimento remoto. Dá o nome de *EternalBlue* e não divulga a ninguém.

1º Semestre de 2016 – um grupo chamado *The Shadow Brokers* ganha acesso a dados da NSA, que incluem diversas vulnerabilidades, entre elas o *EternalBlue*.

Agosto de 2016 – *The Shadow Brokers* começa a colocar publicamente na Internet algumas das ferramentas da NSA.

07 de janeiro de 2017 – *The Shadow Brokers* começa a vender algumas das ferramentas, incluindo o *EternalBlue*.

Janeiro/Fevereiro de 2017 – NSA contata a Microsoft com detalhes sobre a vulnerabilidade.

14 de março de 2017 – Microsoft lança a correção MS17-010, que corrige a vulnerabilidade identificada como CVE-2017-0144 – o *EternalBlue*.

14 de abril de 2017 – O grupo *The Shadow Brokers* dilvulga 300MB de materiais da NSA no Github, incluindo o *EternalBlue*.

12 de maio de 2017 – Tem início a propagação do *Ransomware WannaCry* explorando o *EternalBlue*.

https://boot13.com/windows/timeline-nsa-hacking-tool-to-wannacry/
https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

"Hacking Back" e *"Active Defense"*: **Ataque é a melhor defesa na Internet?**

Plenary Panel: Cyberstability and the Future of the Internet - CyCon 2017

Discussão sobre militarização, sanções e normas de comportamento responsável de Estados no Evento "NATO CCDCOE CyCon 2017" – *Plenary Panel: Cyberstability and the Future of the Internet*
https://youtu.be/FDBTtawj6Ms?t=4559

MIT Technology Review

Sign in | Subscribe

Topics | Magazine | Newsletters | Events

Computing / Cybersecurity

Five reasons "hacking back" is a recipe for cybersecurity chaos

A new US bill would make it legal for private companies to chase hackers across the internet. It's a terrible idea that simply will not die.

by **Martin Giles** Jun 21, 2019

https://www.technologyreview.com/s/613844/cybersecurity-hackers-hacking-back-us-congress/

Over 100 companies committed to protecting cyberspace:

The Cybersecurity Tech Accord

TECH ACCORD

SIGNATORIES

ABB • ACCESS SMART • ALITER TECHNOLOGIES • ANCHORFREE • ANOMALI • APP DETEX • ARCHIVE360 • ARM • ATLASSIAN • AVAST • AVEPOINT • BALASYS • BILLENNIUM • BINARY HOUSE • BITDEFENDER • BT • CAPGEMINI • CARBON BLACK • CISCO • CLOUDFLARE • COGNIZANT • CONTRAST SECURITY • CSC • CYBER SERVICES • CYBER TRUST ALLIANCE • DATASTAX • DELL • DOCUSIGN • DOGTOWN MEDIA • DOMAIN TOOLS • DYNAMIC CONSULTING • EBRC • ENTEL • EPRIVACY • ESET • EXELTEK CONSULTING GROUP • EYEO • FACEBOOK • FASTLY • FIREEYE • FLOWMON NETWORKS • FRACTAL INDUSTRIES • F-SECURE • G DATA • GIGAMON • GITHUB • GITLAB • GLOBANT • GREYCORTEX • GUARDTIME • HITACHI • HMATIX • HP INC • HPE • IMPERVA • INDRA • INTEGRITY PARTNERS • INTERNATIONAL SOFTWARE SYSTEMS • INTUIT • JUNIPER NETWORKS • KOOLSPAN • KPN • LAWTOOLBOX • LINKEDIN • LIREX • MARK MONITOR • MEDIAPRO • MERCADO LIBRE • MICROSOFT • NETCOM LEARNING • NIELSEN • NOKIA • NORTHWAVE • NTT • ORACLE • ORANGE • PALADION • PANASONIC • PANDA • PERCIPIENT.AI • PREDICA • PROFESSIONAL OPTIONS • REVEAL DATA • ROCKWELL AUTOMATION • RSA • SAFETICA • SALESFORCE • SAP • SECUCLOUD • SHARP • SILENT BREACH • SONDA • STACKPATH • STRIPE • STRONG CONNEXIONS • SWISSCOM • TAD GROUP • TANIUM • TELECOM ITALIA • TELEFONICA • TELELINK • TENABLE • THREATMODELER SOFTWARE INC • TREND MICRO • UNISYS • US LICENSING GROUP • US MEDICALIT • VMWARE • VU SECURITY • WIPFLI • WISEKEY

Signatories of the Cybersecurity Tech Accord are united by common values as reflected in four core principles:

- Strong defense: We believe everyone deserves equal protection online irrespective of technical acumen, culture, location or motive for any malicious attack.
- No offense: We are committed to not knowingly undermining the security of the online environment, and to protecting against efforts to tamper with our products and services.
- Capacity building: We see cybersecurity as a shared responsibility and work to improve both the ability of everyone to act securely and safely online and the diversity of the security practitioner community.
- Collective response: We believe we can achieve more together and will partner within the group and more broadly to address critical cybersecurity challenges.

https://cybertechaccord.org

Coordinated Vulnerability Disclosure (CVD)

- The CERT® Guide to Coordinated Vulnerability Disclosure
  https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
- Global Good Practices - Coordinated Vulnerability Disclosure (CVD)
  https://www.thegfce.com/good-practices/documents/publications/2017/11/21/coordinated-vulnerability-disclosure
- The Cybersecurity Tech Accord supports the GFCE's call for industry-wide adoption of transparent policies for coordinated vulnerability disclosure (CVD)
  https://cybertechaccord.org/supports-gfce-call-for-cvd/

Ainda assim nem todas as vulnerabilidades serão compartilhadas com os desenvolvedores:

- Vulnerabilities Equities Policy and Process for the United States Government
  https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
- Equities Process operated on behalf of the UK Government by GCHQ
  https://www.gchq.gov.uk/information/equities-process

E Aspectos Legais?

cert.br nic.br cgi.br

Aspectos Legais:
Lei nº 12.737/12

"Art. 2º[...] **Invadir dispositivo** informático **alheio**, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações **sem autorização** expressa ou tácita **do titular do dispositivo** ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§1º Na mesma pena incorre quem **produz**, **oferece**, **distribui**, vende ou **difunde** dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput."

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Aspectos Legais:
Lei nº 13.709/18 (LGPD)

“Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;”

“Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;”

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Segurança, Privacidade, Ética e Geopolítica: Como Isso Pode Afetar Minha Pesquisa?

cert.br nic.br cgi.br

Algo afeta minha pesquisa e vice-versa?
Checklist

Levar sempre em conta
- ética
- consequências dos testes e tecnologias para a sociedade e os cidadãos

Respeitar confidencialidade
- minimizar quem tem acesso e em quais sistemas o dado estará
- segurança extra dos sistemas
- honrar NDA e seguir o TLP definido pela fonte https://www.first.org/tlp/

Para qualquer atividade que envolva tecnologias ofensivas
- checar se é legal
- ter tudo documentado
- assinar contratos, seguir normas, formalizar autorizações, etc

Pesquisas sobre vulnerabilidades e *pen test* precisam:

- **Seguir os padrões de *Coordinated Vulnerability Disclosure* (CVD)**
  - ACM explicita que é o modo compatível com o código de ética https://ethics.acm.org/integrity-project/ask-an-ethicist/ask-an-ethicist-vulnerability-disclosure/
  - Usenix WOOT (*Workshop on Offensive Technologies*) requer CVD antes da submissão https://www.usenix.org/conference/woot19/call-for-papers
- **Verificar se há algo que impeça pesquisa com outros países**
  - ex.: *Wassenar Arrengement* permite a comunicação apenas para quem está conduzindo ou coordenando as atividades relacionadas com a resolução da vulnerabilidade ou com o tratamento do incidente.

Algumas Áreas de Pesquisa Pouco Exploradas

- *Extrusion Detection*
  - foco no que sai da rede, incluindo ataques
  - permite detecção de exfiltração de dados e comunicação de C2
- Uso de *Netflow* para Segurança
  - *FloCon Conference, FIRST Conference*
- Anonimização de Dados
- Auditoria e segurança de código, mitigação de vulnerabilidades, segurança de auto-updates
- Requisitos mínimos de segurança vs. certificação
- Impactos de novos protocolos
  - ex.: HTML5, DOH, DOT, QUIC, etc

Referências:
Palestras que você DEVE assistir

- Usenix Security'18, James Mickens, Associate Professor of Computer Science at Harvard University
  https://www.usenix.org/conference/usenixsecurity18/presentation/mickens

- The Second Crypto War—What's Different Now
  Susan Landau, Bridge Professor of Cyber Security and Policy, Tufts University
  https://www.usenix.org/conference/usenixsecurity18/presentation/landau

- Privacy for Tigers, Ross Anderson, Professor of Security Engineering at Cambridge University
  https://www.usenix.org/conference/usenixsecurity18/presentation/anderson

- Plenary Panel: Cyberstability and the Future of the Internet – NATO CCDCOE CyCon 2017
  https://youtu.be/FDBTtawj6Ms

Em breve *online*:

- Tackling the Trust and Safety Crisis, Alex Stamos, Adjunct Professor, Stanford University
  https://www.usenix.org/conference/usenixsecurity19/presentation/stamos

- The Spies Hacking our Phones are Going Dark, and We're All in Trouble, Citizen Lab
  https://www.usenix.org/presentation/scott-railton

- Security Educational Panel, Usenix 2019
  https://www.usenix.org/conference/usenixsecurity19/presentation/panel-security-educational

Referências:
Discussões nos Fóruns de Governança da Internet

IGF (UN Internet Governance Forum) Best Practices Forums

- **Fórum ativo** no IGF é o "*Best Practices Forum on Cybersecurity*". O foco deste ano é: "***Exploring best practices in relation to recent international cybersecurity initiatives***"

  2016–2019: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

- Relatórios finais das discussões dos fóruns sobre "*Establishing and supporting CSIRTs*" e "*Fighting Spam*"

  2015: http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs

  2014: http://www.intgovforum.org/cms/best-practice-forums/igf-2014-best-practices-forums

FIRST Internet Governance Initiative

https://www.first.org/global/governance/

FIRST Incident Handling for Policy Makers

https://www.first.org/education/trainings#t5

Referências:
Discussões nos Fóruns de Governança da Internet (cont.)

Cadernos CGI.br

https://www.cgi.br/publicacoes/indice/livros/

- Documentos da Cúpula Mundial sobre a Sociedade da Informação: Genebra 2003 e Túnis 2005
  https://www.cgi.br/publicacao/cadernos-cgi-br-documentos-cmsi/

- Fórum de Governança da Internet: Relatórios dos dez primeiros anos do IGF
  https://www.cgi.br/publicacao/cadernos-cgibr-forum-de-governanca-da-internet/

- Declaração Multissetorial do NETmundial
  https://www.cgi.br/publicacao/cadernos-cgi-br-declaracao-multissetorial-do-netmundial/

Precisamos um Ecossistema mais Saudável: **Faça a sua parte!**

PROGRAMA INTERNET +SEGURA

Iniciativa conjunta: ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee – https://bcp.nic.br/i+seg

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

04 de setembro de 2019

nic.br cgi.br

www.nic.br | www.cgi.br