nic.br cgi.br | cert.br

VI Curso Intensivo da Escola de Governança da Internet

Comitê Gestor da Internet no Brasil

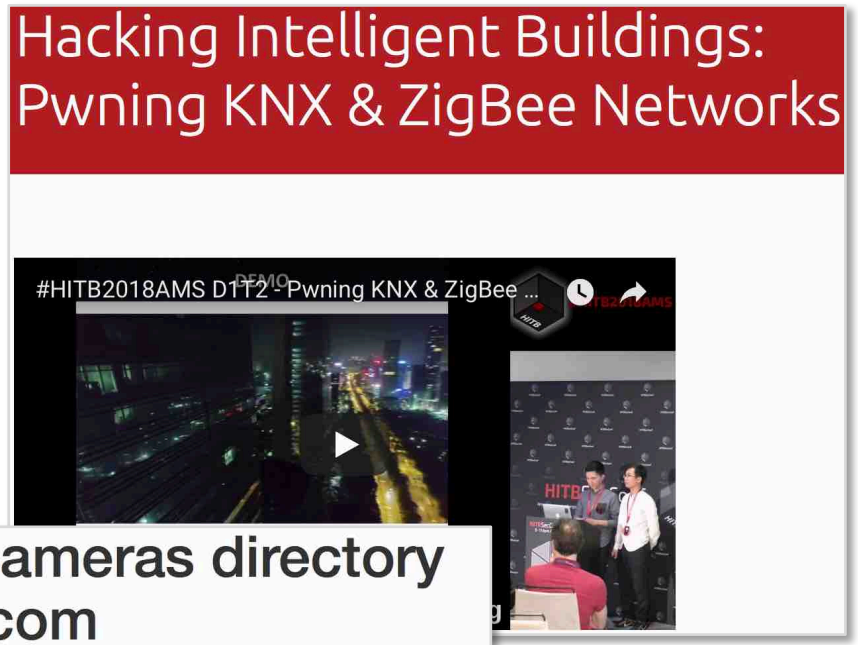
São Paulo, SP | 08/07/2019

Ecossistema da Segurança Cibernética

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br



https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs
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/
http://www.insecam.org

USA TODAY NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 71° INVESTIGATIONS SUBSCRIBE MORE

Why you might want to wrap your car key fob in foil

USA TODAY NETWORK Phoebe Wall Howard, Detroit Free Press Published 6:00 a.m. ET July 8, 2018 | Updated 8:59 a.m. ET July 9, 2018

Even if your keys are right by your side, your car could be at risk from thieves. Some experts say, this household item could protect you. USA TODAY

https://www.usatoday.com/story/money/nation-now/2018/07/08/wrap-car-key-fob-foil/762338002/

Incidentes Públicos em Instituições Focadas em Segurança: **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

- 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

Segurança e Resiliência

cert.br nic.br cgi.br

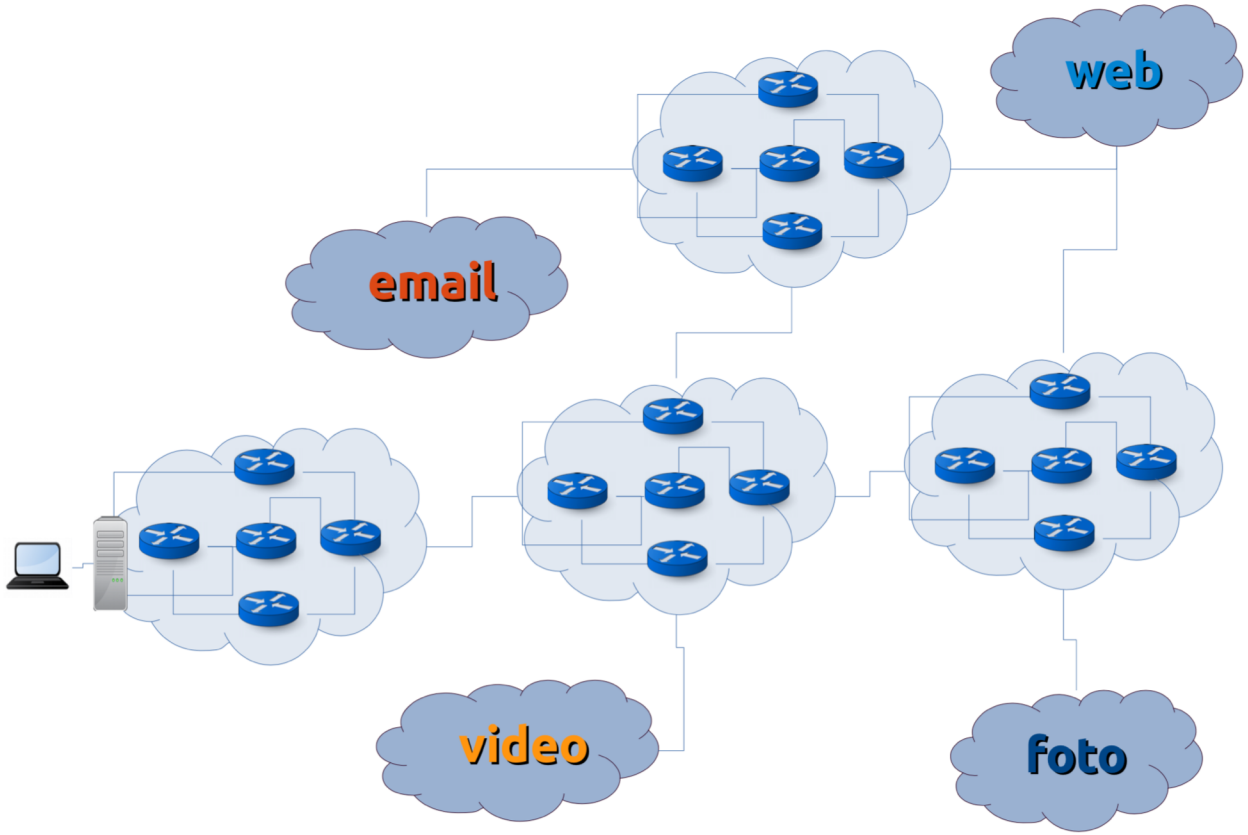
Características da Internet

"Rede de redes"

- Sistema de **redes interconectadas**
- **Sem controle centralizado**

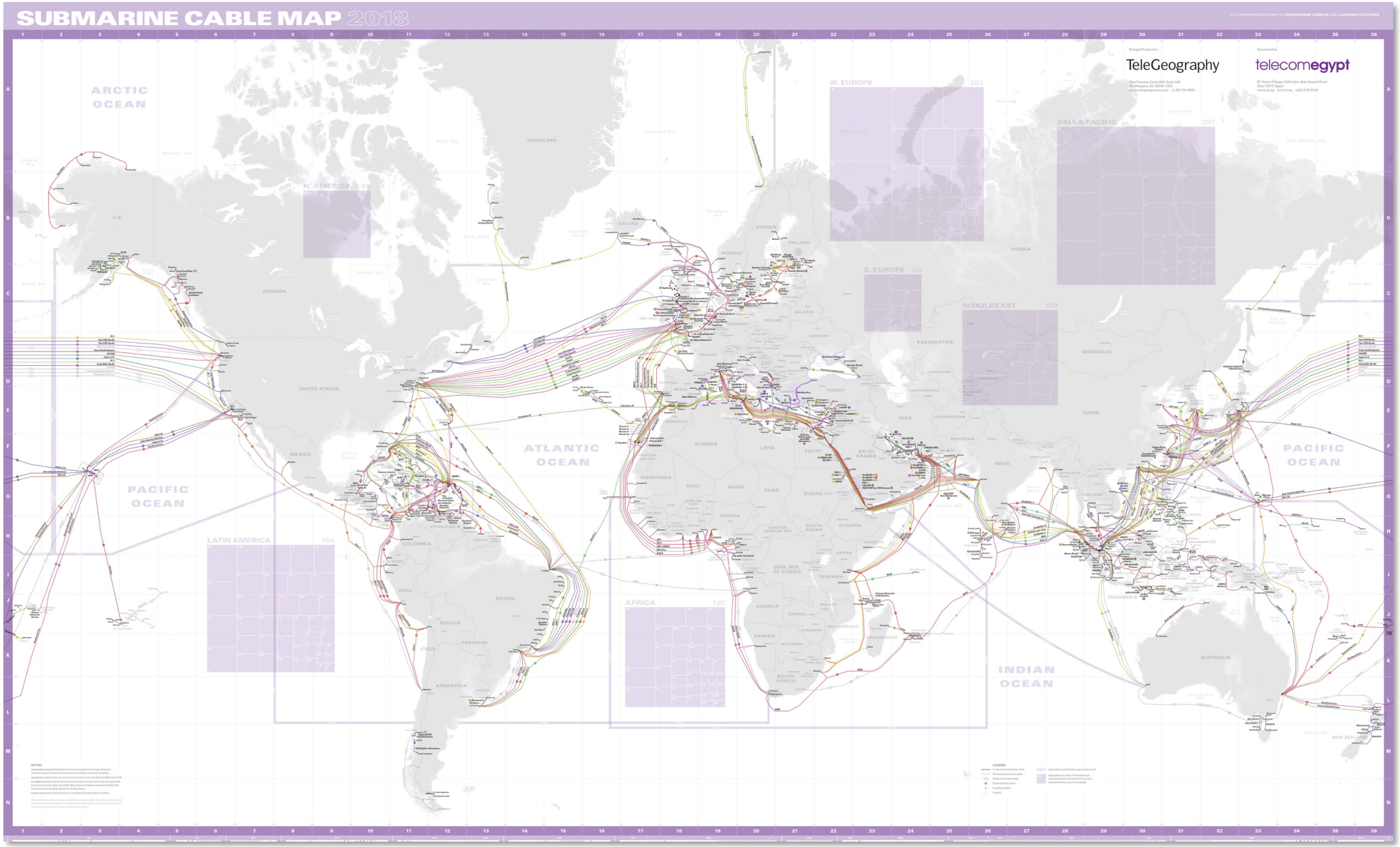
Sistemas Autônomos

- Equipamentos sob uma **mesma administração** e com **políticas de roteamento próprias**
- **Autonomia** em relação aos demais sistemas/redes
- **Identificação única:** ASN (*Autonomous System Number*)
  - Mais de 90 mil ASNs alocados no mundo
  - Mais de 64 mil ASNs na tabela de roteamento
- Brasil: 6.748 Sistemas Autônomos
  - Representatividade no LACNIC: 69,4% dos ASNs, 61% dos blocos IPv4 e 71,7% dos blocos IPv6
  - 6.618 ISPs (estimado)



Fundamentos Técnicos – Arquitetura da Internet, Ricardo Patara
EGI Curso Jurídico, Rio de Janeiro, RJ, 21/11/2016

Fontes das estatísticas (acessadas em 04/07/2019):
https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html
http://www.cidr-report.org/as2.0/
http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion
https://www.cetic.br/pesquisa/provedores/



Fonte: https://www2.telegeography.com/submarine-cable-map

Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

Sistemas na Internet

Riscos

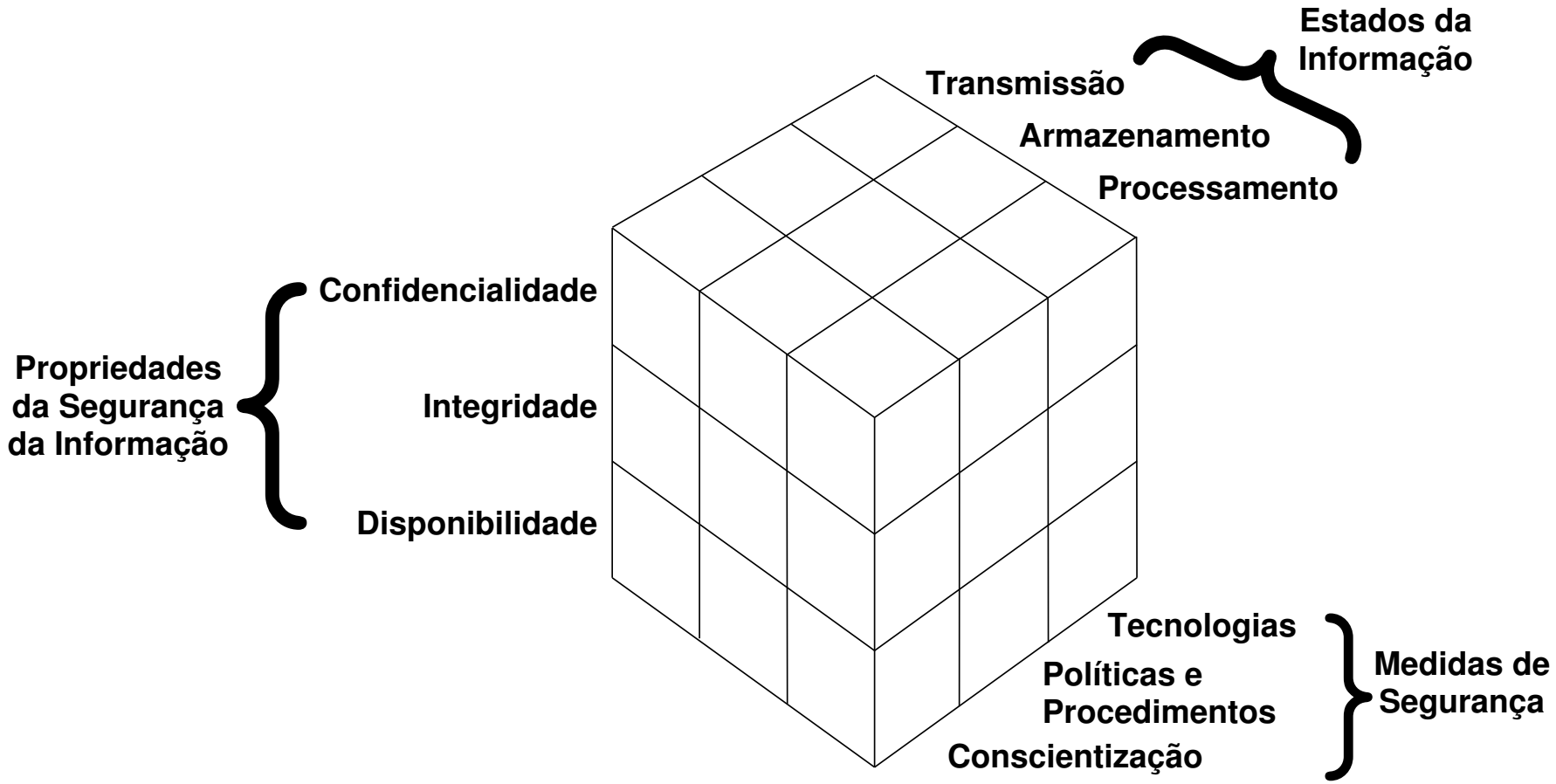
Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

A Segurança Depende de Múltiplos Fatores:
Os Dados e as Informações Estão em Diversos Locais



McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

Resiliência das Organizações:
Resistir e Continuar Operando Mesmo sob Ataque

Nenhum grupo ou estrutura única consegue fazer sozinho a segurança ou a resposta a incidentes - todos tem um papel

- Administradores de redes e sistemas
  - não emanar “sujeira” de suas redes e adotar boas práticas
- Usuários
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções
- Desenvolvedores
  - precisam pensar em segurança desde as etapas iniciais de desenvolvimento

Ainda assim incidentes ocorrerão

- necessário identificar e mitigar mais rapidamente
- necessário ter CSIRTs estabelecidos e profissionais preparados em todas as redes
  - **cooperação depende do estabelecimento de confiança mútua (*trust*)**

CSIRT: Grupo de Tratamento de Incidentes de Segurança em Computadores, do Inglês *Computer Security Incident Response Team*

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

Foco do CERT.br nestes 22 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

A segurança de todos depende de um ecossistema saudável

Comunidade Nacional

- Auxiliar na análise técnica e facilitar o tratamento de incidentes por outros CSIRTs
- Ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (CSIRTs)
- Gerar massa crítica para possibilitar a cooperação e melhora na segurança das redes
- Ter uma visão sobre as principais tendências de ataques no Brasil

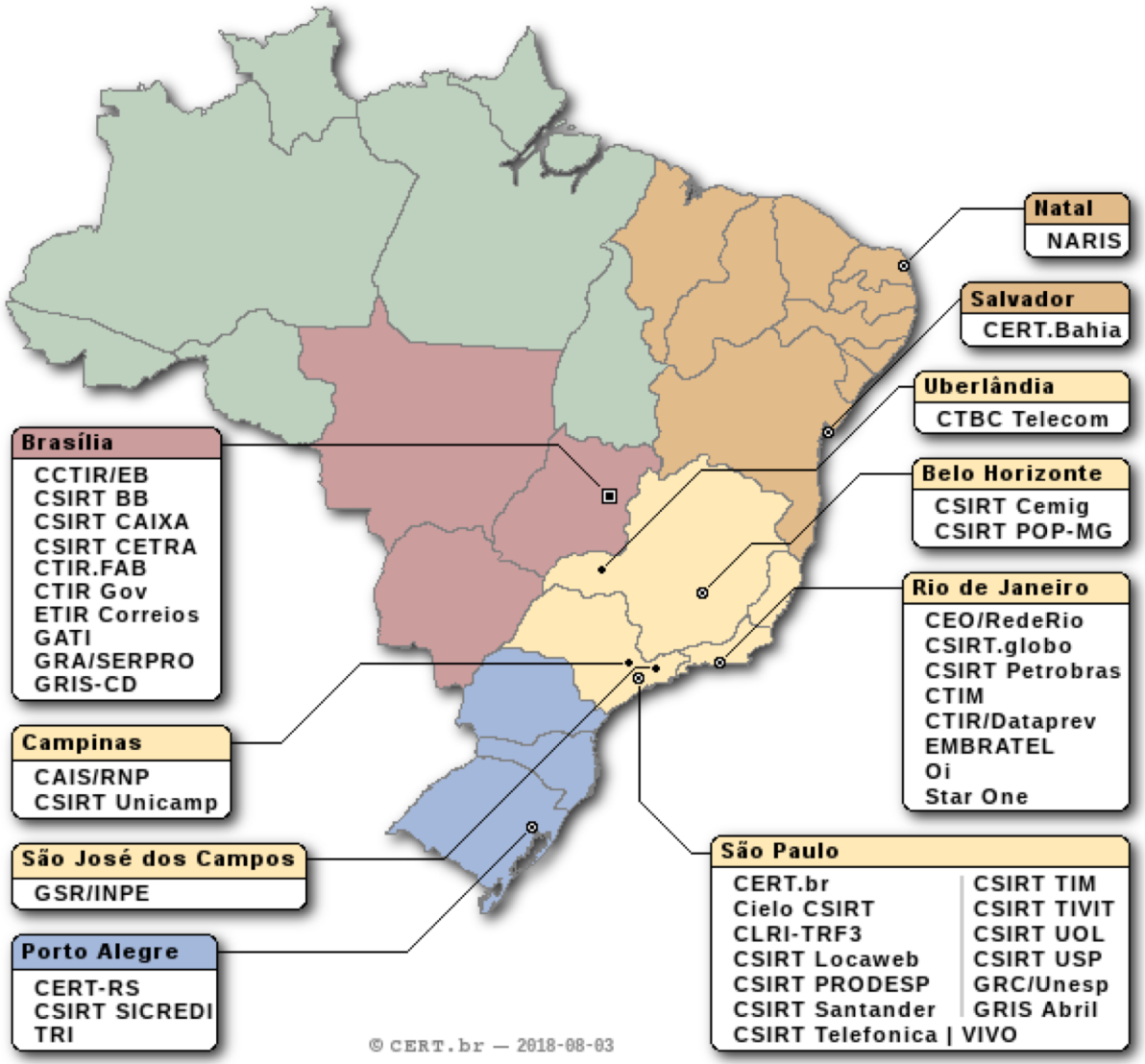
Comunidade Internacional

- Estabelecer relações de confiança
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes

Grupos de Tratamento de Incidentes (CSIRTs) Brasileiros:
42 times com serviços anunciados ao público

Setor	CSIRTs
Nacional – domínios .br, ASNs ou IPs alocados ao Brasil.	CERT.br
Nacional – Administração Pública Federal	CTIR Gov
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energia	CSIRT Cemig, CSIRT Petrobras
Sistema Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Provedores Operadoras Hospedagem	CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Outros	CSIRT.globo, GRIS Abril

https://cert.br/csirts/brasil/



Segurança e Combate a Abusos na Internet:
Fóruns Técnicos Internacionais

FIRST – *Forum of Incident Response and Security Teams*

- Criação: 1990
- Membros: 483 CSIRTs, em 92 países, participantes de todos os setores (dados de 30/06/2019);

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*

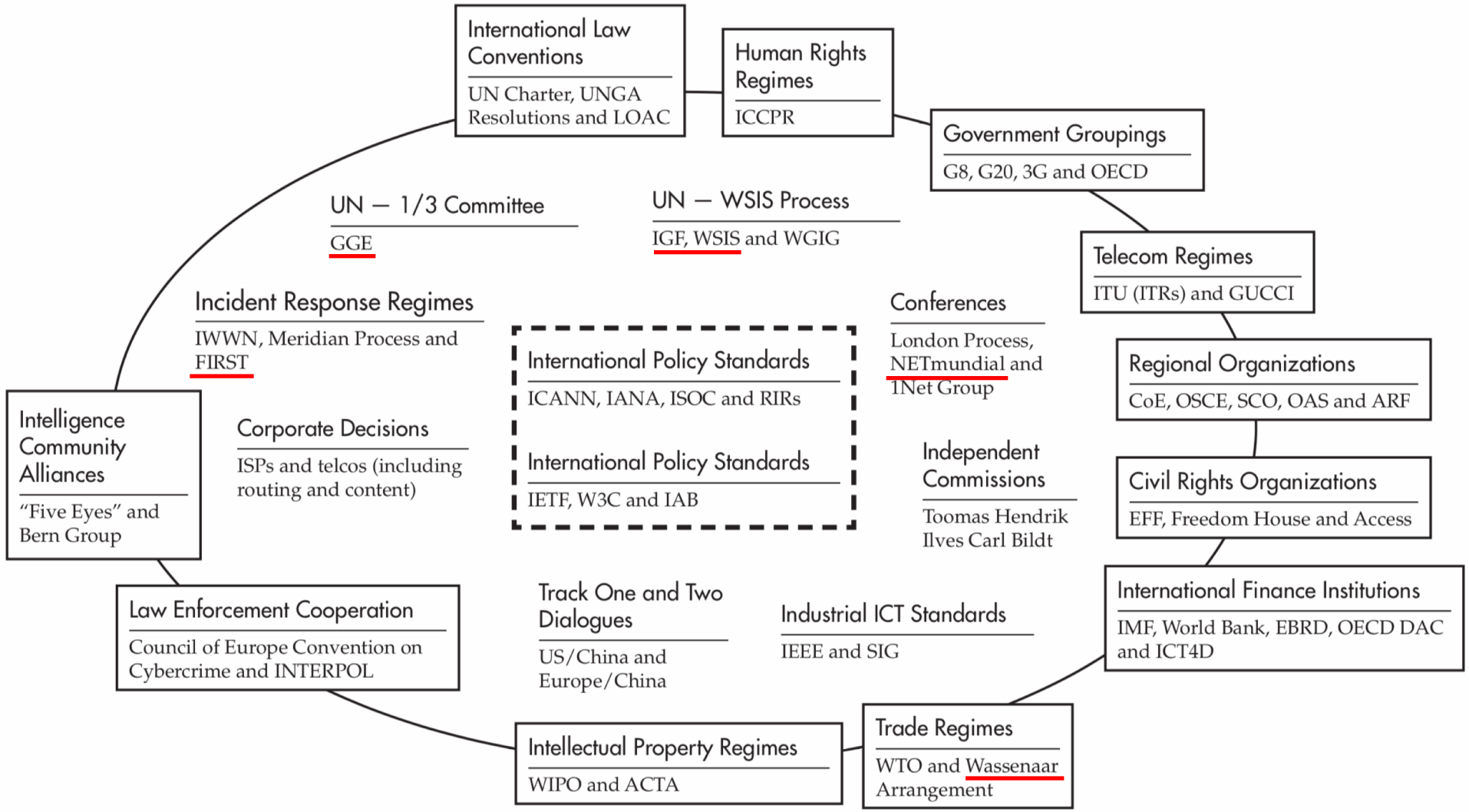
- Criação: 2004
- Membros: mais de 200 membros da Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

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

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

Segurança nos Fóruns Globais

cert.br nic.br cgi.br



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

GCCS – *Global Conference on Cyber Space* (“*London Process*”)

Primeira Conferência em Londres em 2011

- Restrita a Governos
- Objetivo de definir normas de conduta aceitável por Estados no “ciberespaço”

Na Conferência 2015, na Holanda, setor privado foi convidado a participar

- Também foi criado o GFCE – *Global Forum of Cyber Expertise*
  - Grupo formado por Governos, Setor Privado e Organizações Intergovernamentais para focar em “*Capacity Building*”

https://www.thegfce.com/about/gccs

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.

[...]

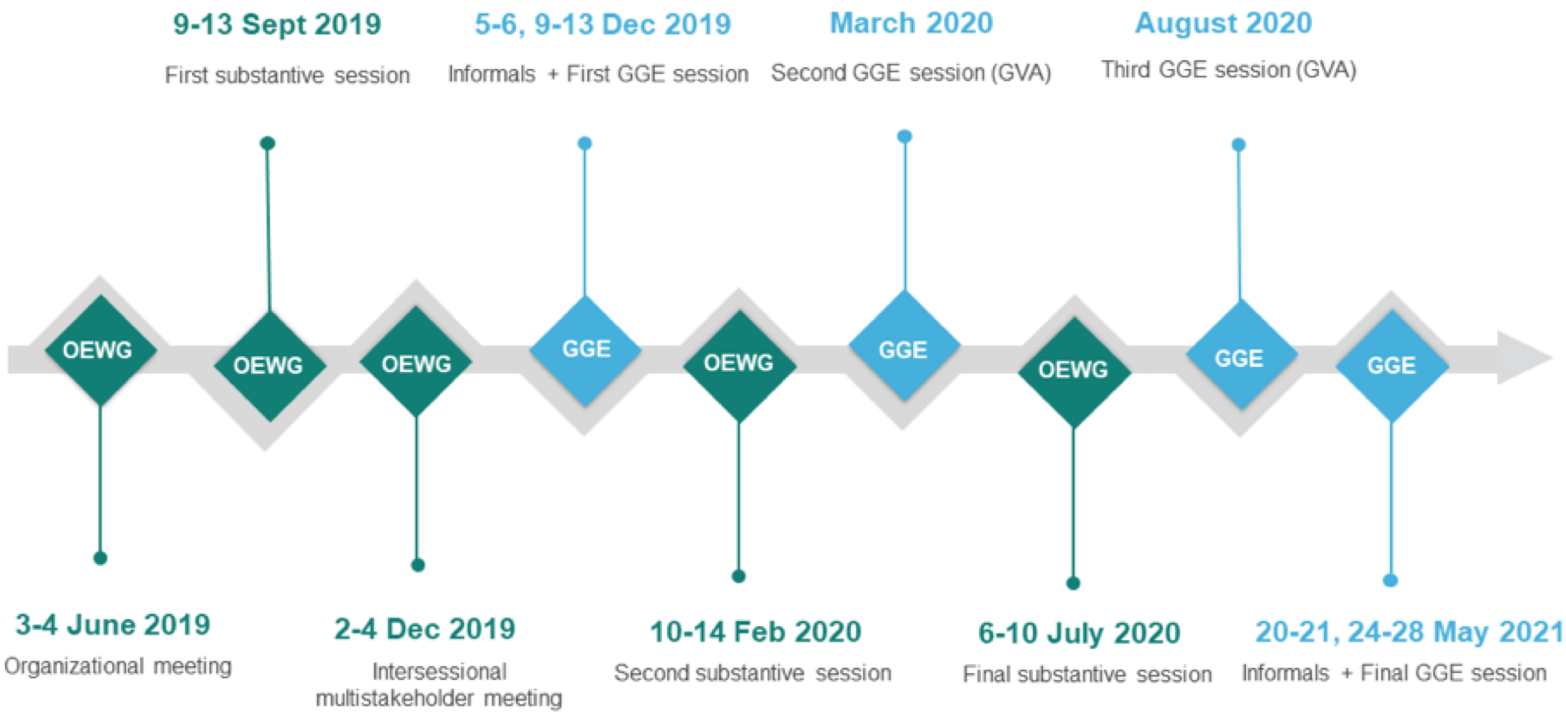
https://undocs.org/A/70/174

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

Desafios

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 ter acesso a estas “armas”

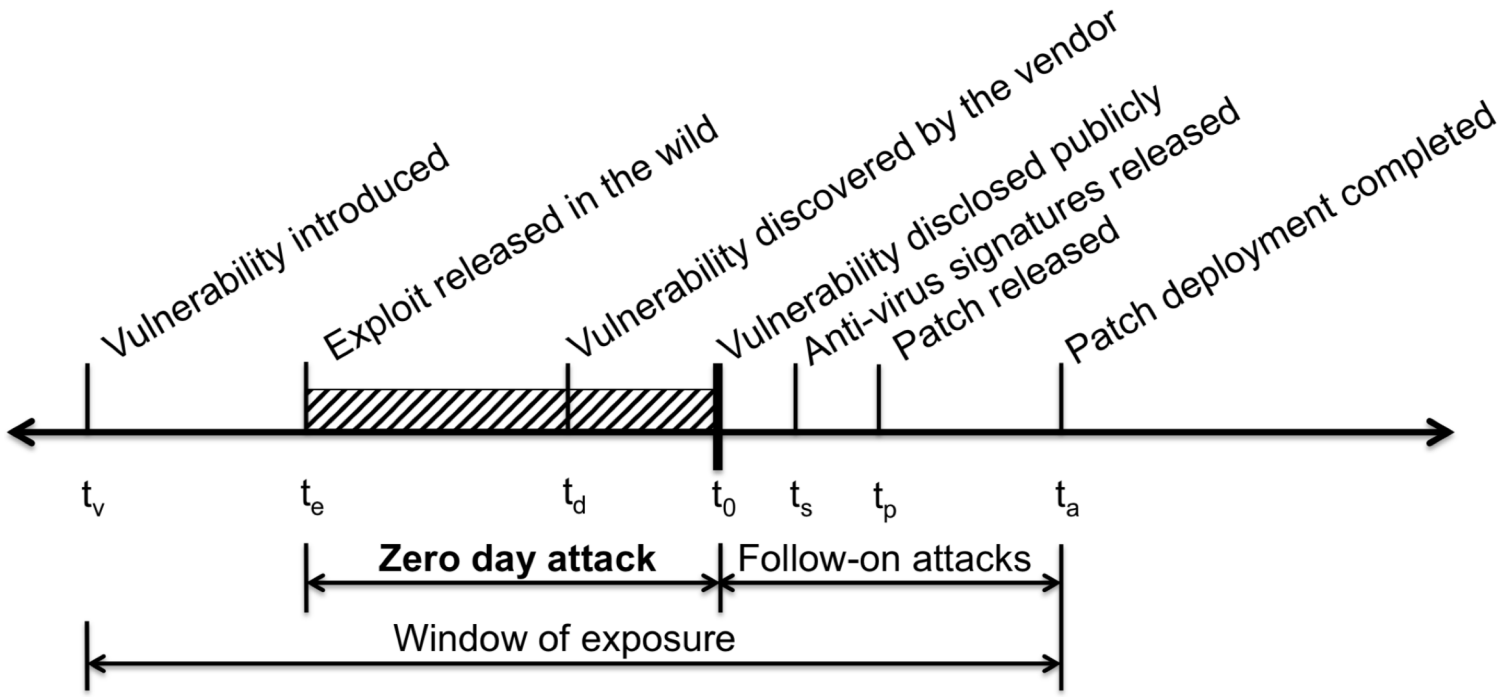
Conseguimos proteger nossos sistemas?
Responsible Disclosure vs. Stock Pilling Vulnerabilities

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 Políticas Públicas

cert.br nic.br cgi.br

"*0-Days*" e governos estocando vulnerabilidades:
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/

Referências Sobre as Discussões Globais

IGF (UN Internet Governance Forum) Best Practices Forums

- 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

- **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

FIRST Internet Governance Initiative

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

FIRST Incident Handling for Policy Makers

https://www.first.org/education/trainings#Incident-Handling-for-Policy-makers

Referências Sobre as Discussões Globais (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/

Questões Persistentes em Fóruns Globais

cert.br nic.br cgi.br

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*"

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**

Acesso Excepcional a Conteúdo Cifrado: **Importância da Criptografia**

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais
- mecanismos de autenticação
- conexão segura na Web (HTTPS)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC)

Cartilha de Segurança para a Internet, Capítulo 9
ISBN: 978-85-60062-54-6 – https://cartilha.cert.br/livro/

Acesso Excepcional a Conteúdo Cifrado: **Referências Recomendadas**

- *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

  "*This report's analysis of law enforcement demands for exceptional access to private communications and data shows that* ***such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend.***"

- *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

  (*Slides*, Áudio e Vídeo disponíveis no *link* acima)

Colocando em Prática os Princípios de Governança Colaborativa para Segurança na Internet

cert.br nic.br cgi.br

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**.

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**.

Redução dos Ataques de Negação de Serviço (DDoS): **Atores e Seus Papéis**

Boas práticas para reduzir o “poder de fogo”:

- **Detentores de Sistemas Autônomos**: implementar *anti-spoofing* (BCP 38)
- **Provedores de Serviços**: (NTP, DNS, etc.): configurar corretamente os serviços para evitar amplificação
- **Usuários**: manter sistemas atualizados, prevenir-se de infecções (*hardening*), “limpar” dispositivos infectados
- **Desenvolvedores de sistemas**: considerar riscos no projeto, desenvolver código mais seguro, configuração padrão mais segura
- **Academia**: formar profissionais de todas as áreas que considerem segurança como essencial

Prevenção por parte das **vítimas**:

- Aumentar os recursos (mais banda, processamento, disco)
- Usar serviços ou ferramentas de mitigação

Repressão por parte dos **operadores da justiça**:

- Investigar e punir os atacantes

Precisamos um Ecossistema mais Saudável:
Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

https://bcp.nic.br/i+seg

Desafios para o Futuro

Qualificação profissional

- Redes, administração de sistemas, segurança, desenvolvimento de *software* seguro

Vulnerabilidades sempre vão existir

- O importante é tratá-las de forma rápida - ter e aplicar correções o mais rápido possívela

Certificação de dispositivos/hardware não faz mais sentido

- Não há como certificar *software* (*firmware* é *software*)
- Precisamos discutir, em nível global, a definição de requisitos de maturidade em segurança para fabricantes (todos) e desenvolvedores de software (incluindo o governo), incluindo:
  - possuir ciclo claro de atualização de *software/firmware*
  - possuir um PSIRT (*Product Security Incident Response Team*) ou ao menos um contato claro para tratar problemas de segurança no produto/*software*

Leitura recomendada:

When safety and security become one
https://www.lightbluetouchpaper.org/2017/06/01/when-safety-and-security-become-one/

Obrigado

cristine@cert.br jessen@cert.br

Notificações para: cert@cert.br @certbr

www.cert.br

08 de julho de 2019

nic.br cgi.br

www.nic.br | www.cgi.br