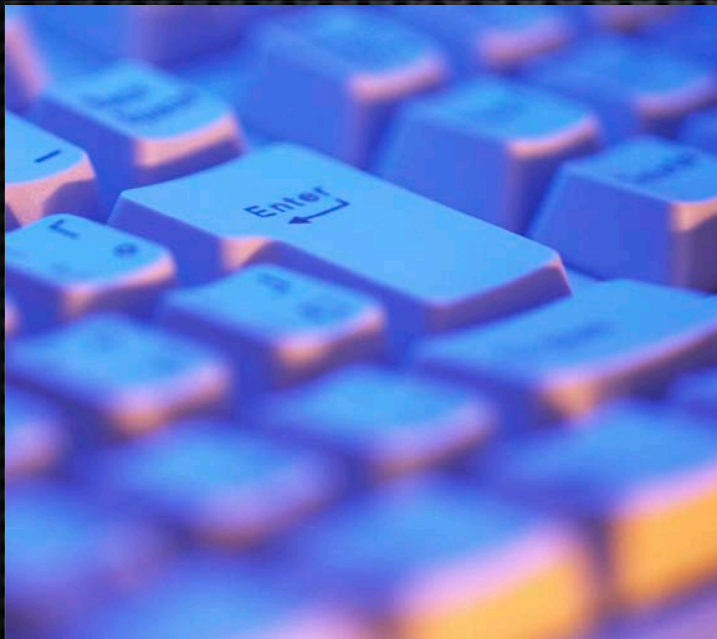
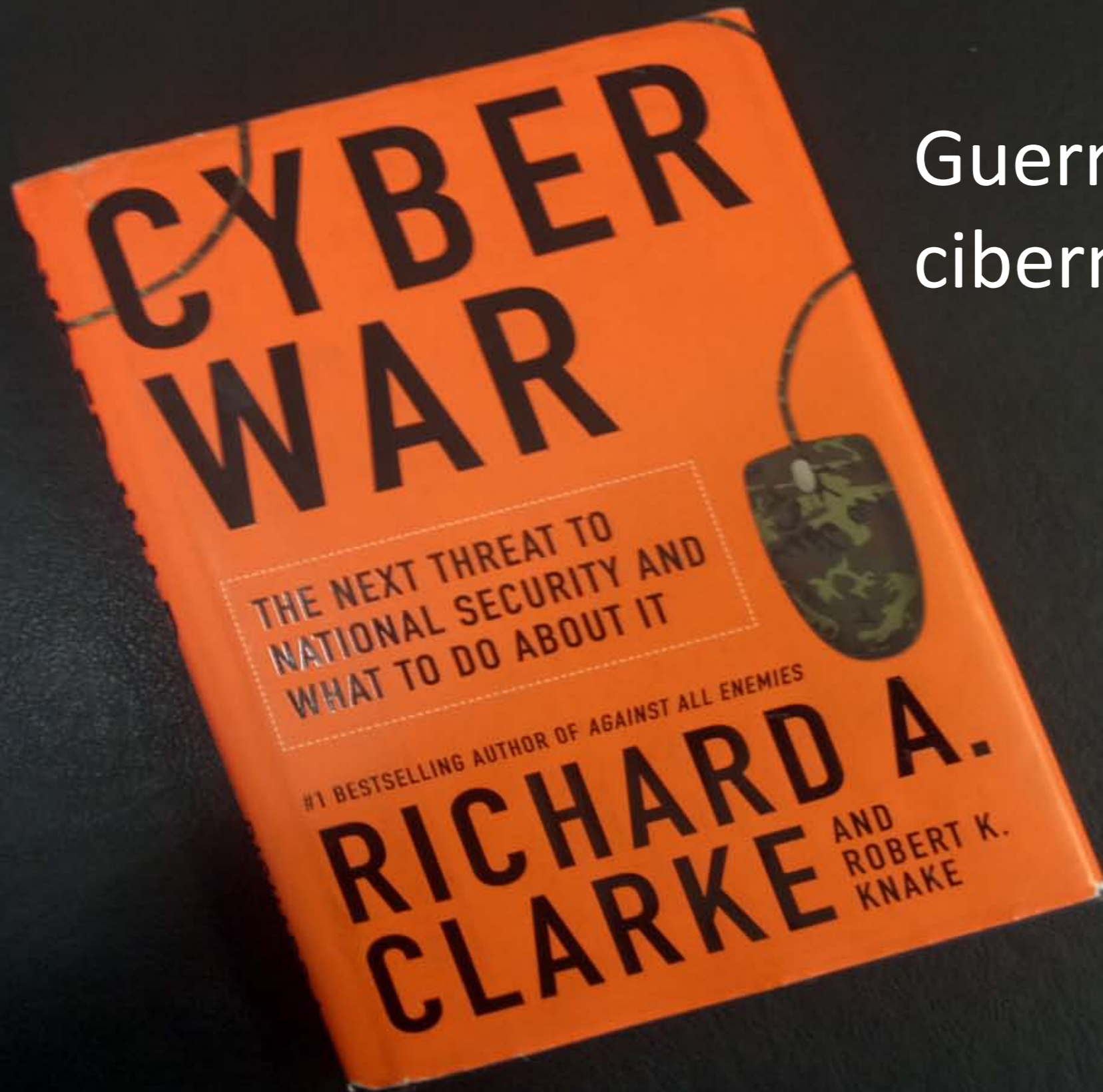




Sumário

- Introdução
- Desenvolvimento
 - O setor cibernético no Exército
 - C&T no Brasil
 - Jornadas de Trabalho MCTI-EB
 - Framework
 - Pij Ap Grandes Eventos
 - Eventos futuros
- Conclusão

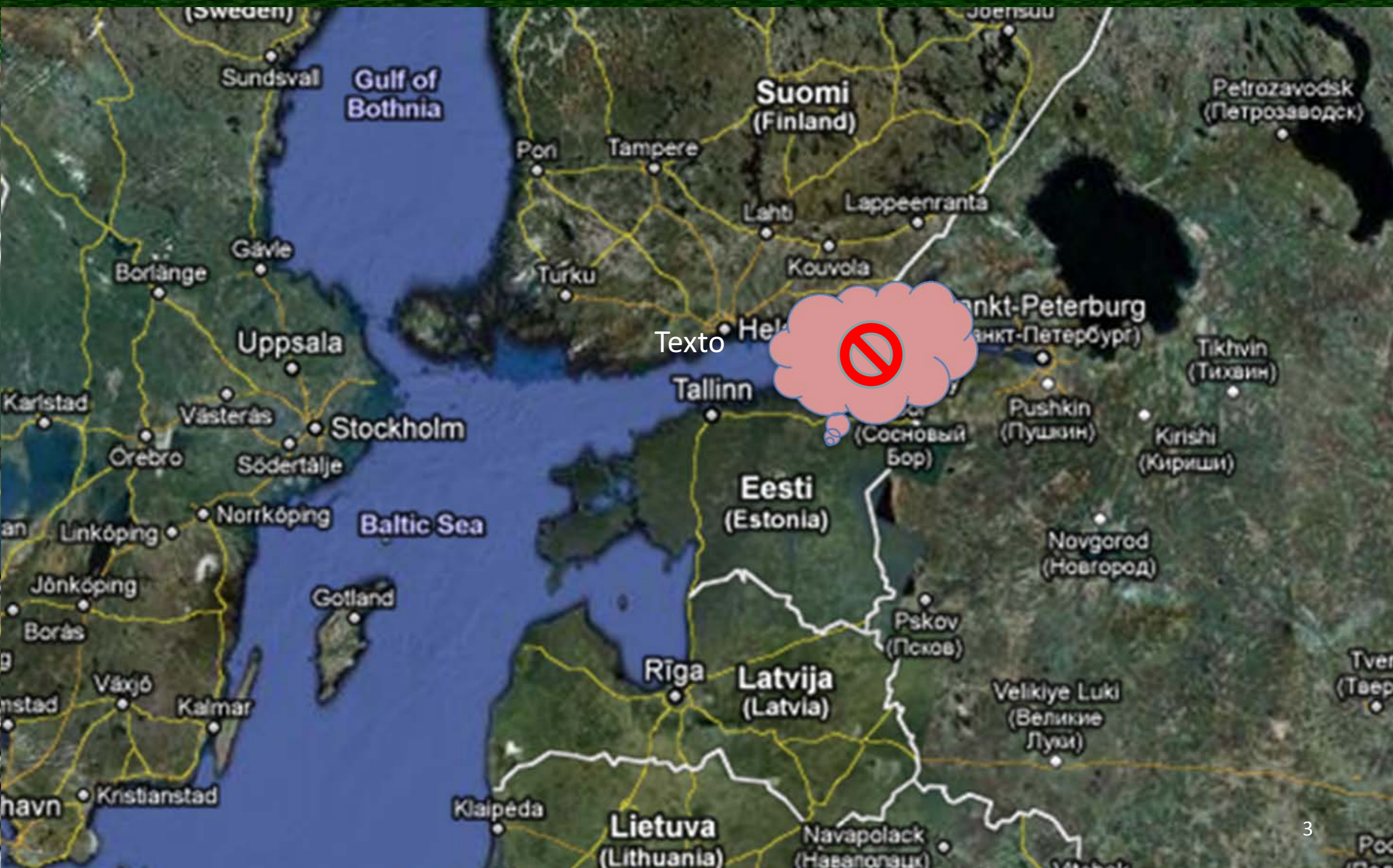




Guerra
cibernética?



ESTÔNIA, Abr 2007





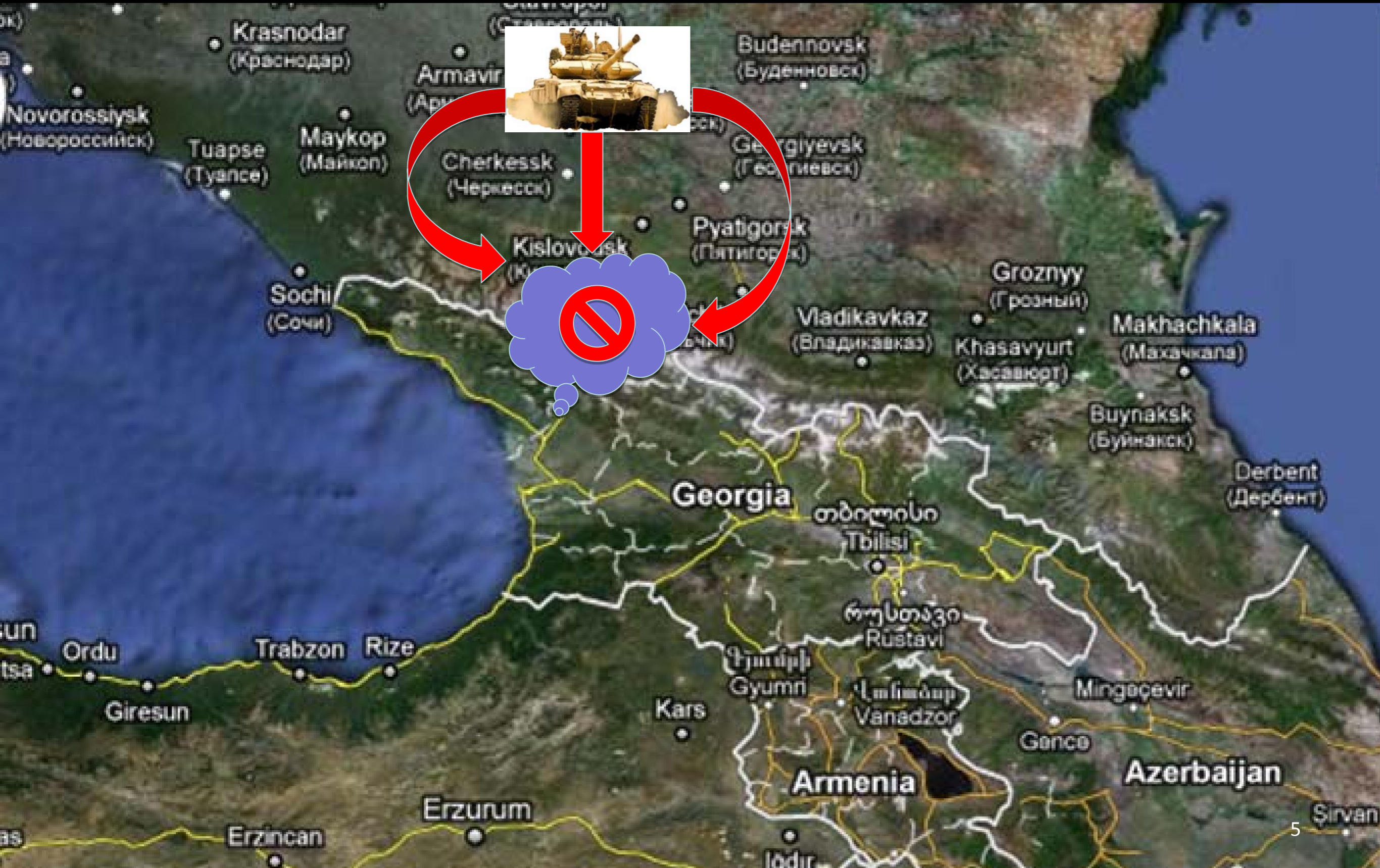
SÍRIA, 06 Set 2007





Centro de Defesa Cibernética

Georgia, 08 Ago 2008





Natanz, IRAN, Jul 2010



Book 3 nights and get the 4th for free! Book Online Now! Premier Party hostel in Argentina. Hostel Buenos Aires MiHOUSE



Advertise on NYTimes.com

U.S. Debated Cyberwarfare in Attack Plan on Libya

By ERIC SCHMITT and THOM SHANKER
Published: October 17, 2011

WASHINGTON — Just before the American-led strikes against [Libya](#) in March, the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyberoffensive to disrupt and even disable the Qaddafi government's air-defense system, which threatened allied warplanes.

While the exact techniques under consideration remain classified, the goal would have been to break through the firewalls of the Libyan government's computer networks to sever military communications links and prevent the early-warning radars from gathering information and relaying it to missile batteries aiming at NATO warplanes.

But administration officials and even some military officers balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such

offensives of their own, and questioning whether the attack could be mounted on such short notice. They were also unable to resolve whether the president had the power to proceed with such an attack without informing Congress.

In the end, American officials rejected cyberwarfare and [used conventional aircraft, cruise missiles and drones](#) to strike the Libyan air-defense missiles and radars used by Col. [Muammar el-Qaddafi's](#) government.

This previously undisclosed debate among a small circle of advisers demonstrates that cyberoffensives are a growing form of warfare. The question the United States faces is whether and when to cross the threshold into overt cyberattacks.

Last year, a [Stuxnet](#) computer worm apparently [wiped out a part of Iran's nuclear centrifuges](#) and delayed its ability to produce nuclear fuel. Although no entity has acknowledged being the source of the poisonous code, some evidence suggests that the

- RECOMMEND
- TWITTER
- LINKEDIN
- COMMENTS (67)
- SIGN IN TO E-MAIL
- PRINT
- REPRINTS
- SHARE



Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This? Log In With Facebook

What's Popular Now f
Notes From a Dragon Mom
In California, Going All Out to Bid Adieu to Foie Gras

Connect With Us on Twitter
Follow @nytimesworld for international breaking news and headlines.



Readers' Comments
Share your thoughts.
Post a Comment »
Read All Comments (67) »

Claro DDD Empresas
A partir de R\$ 29,90/mês.
Saiba mais >>
Claro logo
Compartilhe cada momento.

TimesLimited E-Mail
Sign up to receive exclusive products and experiences featuring NYTimes.com's premier advertisers.
[input] Sign Up
Privacy Policy

MOST E-MAILED MOST VIEWED
1. Amazon Signs Up Authors, Writing Publishers Out of Deal
2. OP-ED COLUMNIST Losing Their Immunity
3. EDITORIAL Elizabeth Warren's Appeal





O Setor Cibernético no EB

A Estratégia Nacional de Defesa

Setores de importância estratégica: o espacial, o **cibernético** e o nuclear.

As capacitações cibernéticas incluirão, como parte prioritária, as tecnologias de comunicação. de modo a assegurar sua capacidade para **atuar em rede** .

● Aperfeiçoamento. que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra **ataques cibernéticos**.

CDCiber

Criação: 02 de agosto de 2010

Missão:

● Coordenar as atividades do Setor Cibernético no Exército.

● Promover ações que atendam ao preconizado na **Estratégia Nacional de Defesa**, com ênfase na **atuação em rede** e na redução das vulnerabilidades **contra ataques cibernéticos**.





O Setor Cibernético no EB

• A Estratégia Nacional de Defesa

Resguardados os interesses de segurança do Estado quanto ao acesso a informações, serão estimuladas **iniciativas conjuntas** entre organizações de pesquisa das Forças Armadas, **instituições acadêmicas** nacionais e **empresas privadas** brasileiras. O objetivo será fomentar o desenvolvimento de um **complexo militar-universitário-empresarial** capaz de atuar na fronteira de tecnologias que terão quase sempre utilidade **dual**, militar e civil.

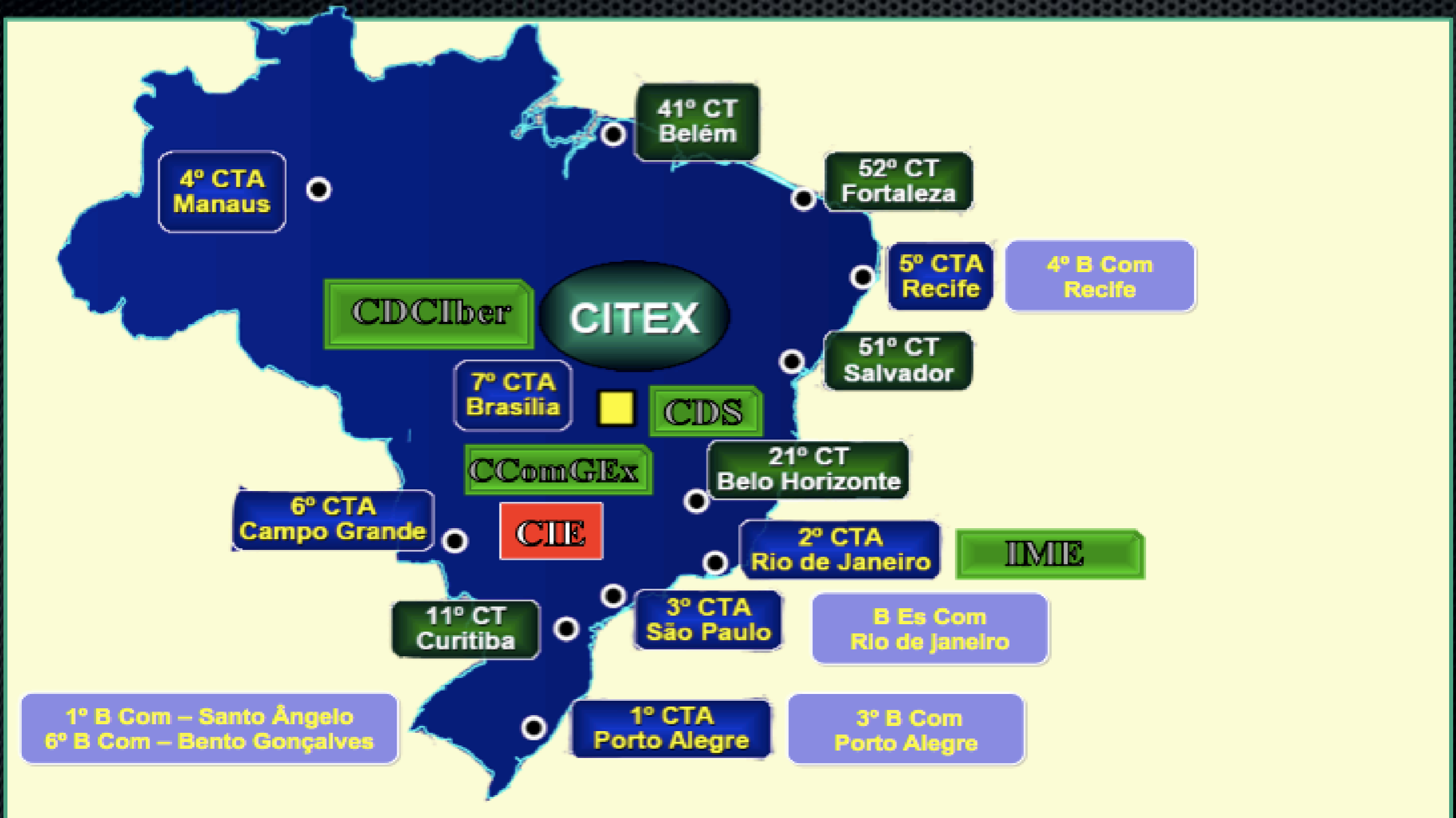


O Setor Cibernético no EB

Nível de decisão	Designação	Estrutura
Político	Segurança Cibernética	Gabinete de Segurança Institucional
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Componentes das Forças Armadas
Tático		

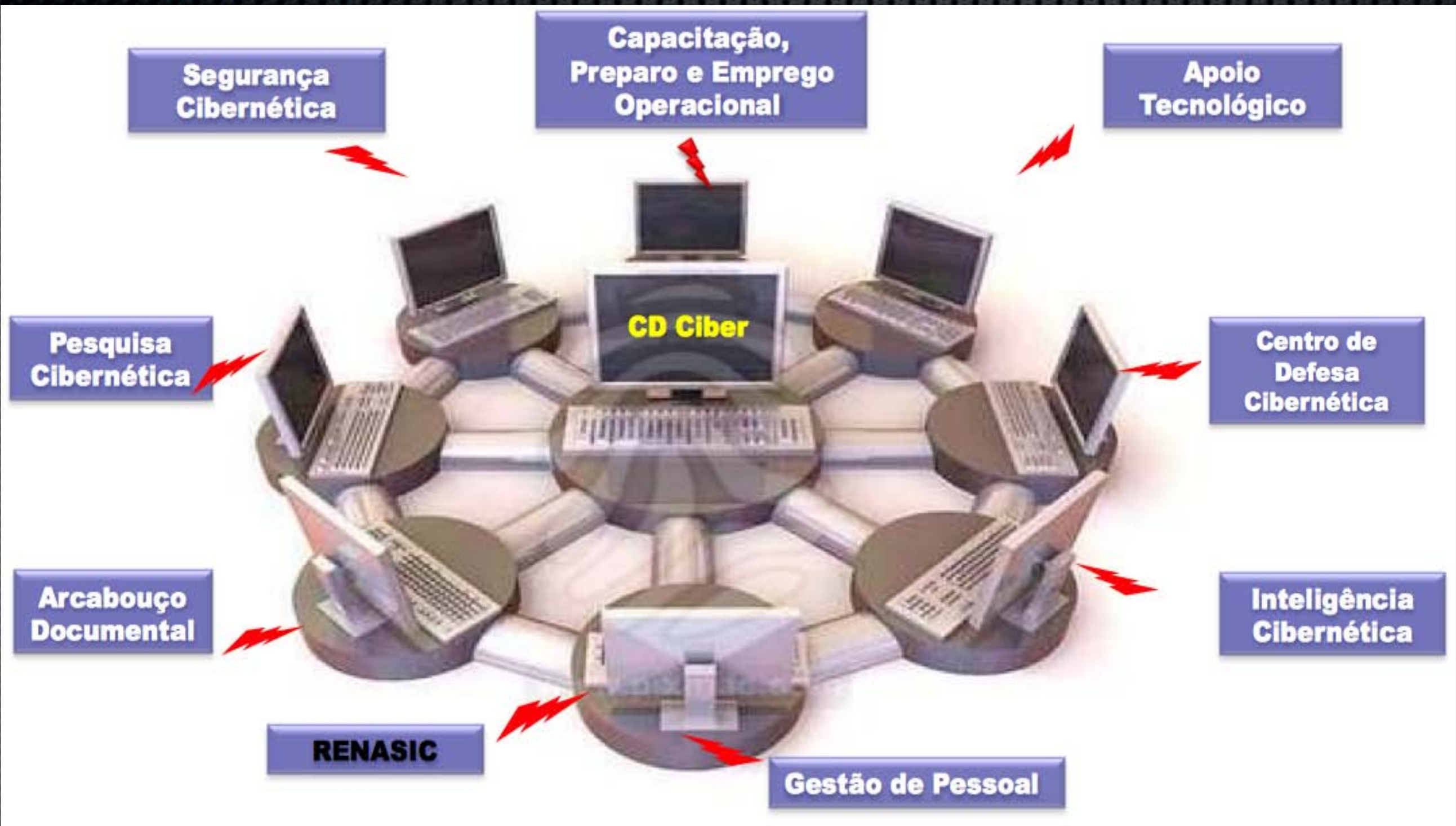


O Setor Cibernético no EB





O Setor Cibernético no EB

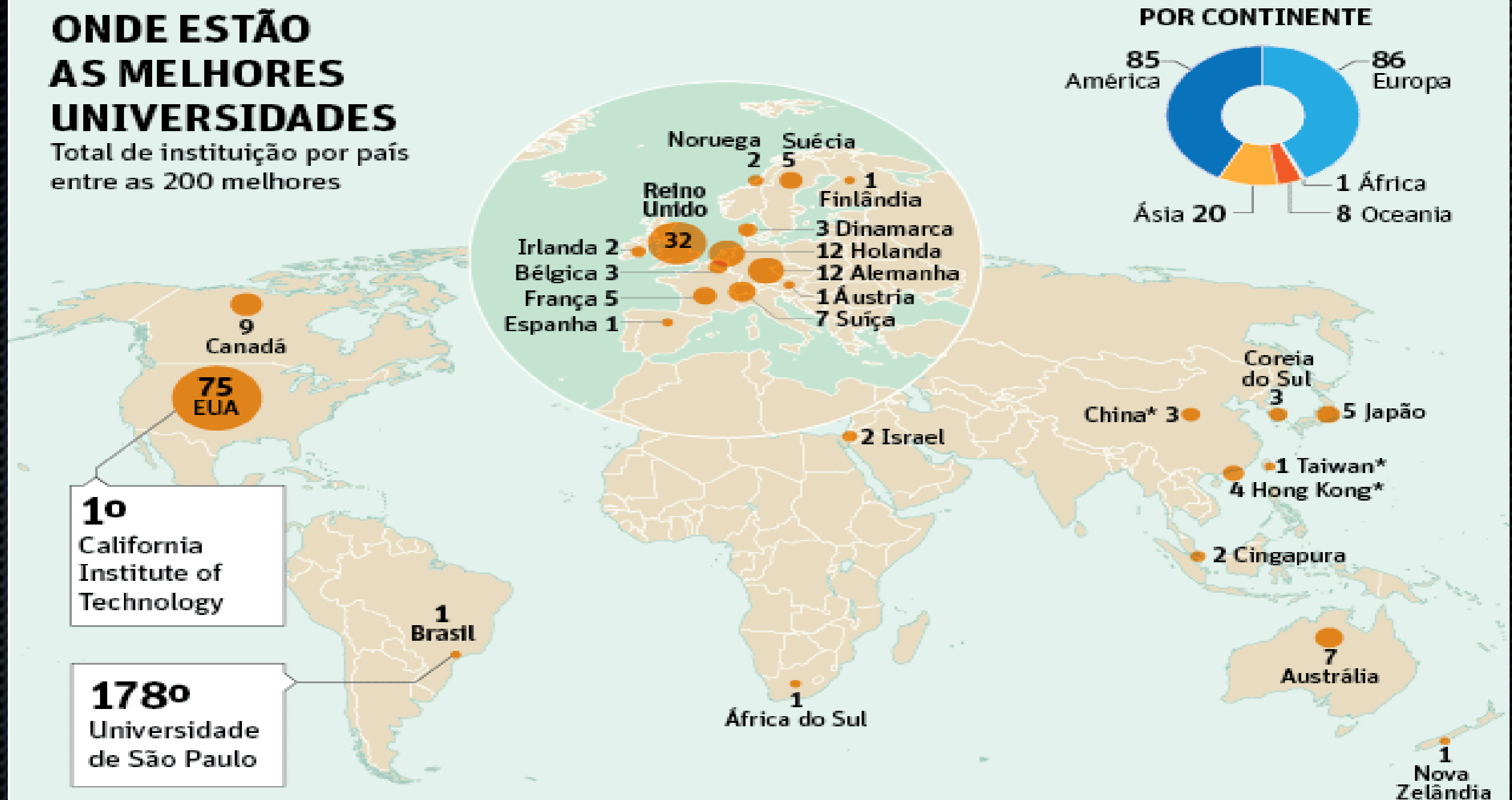




C&T no Brasil

ONDE ESTÃO AS MELHORES UNIVERSIDADES

Total de instituição por país entre as 200 melhores



Fonte: The Times Higher Education World University Rankings 2011-12

**O THE separa China de Hong Kong e Taiwan



C&T no Brasil

Posição	Instituição	País
1º	Universidade Harvard	EUA
2º	Universidade Stanford	EUA
3º	Instituto de Tecnologia de Massachussets (MIT)	EUA
4º	Universidade da Califórnia Berkeley	EUA
5º	Universidade de Cambridge	Inglaterra
6º	Instituto de Tecnologia da Califórnia	EUA
7º	Universidade Princeton	EUA
8º	Universidade Columbia	EUA
9º	Universidade de Chicago	EUA
10º	Universidade de Oxford	Inglaterra





C&T no Brasil

Posição	Instituição	País
101 - 150º	Universidade de São Paulo (USP)	Brasil
201 - 300º	Universidade de Campinas (Unicamp)	Brasil
301 - 400º	Universidade Federal de Minas Gerais (UFMG) Universidade Federal do Rio de Janeiro (UFRJ) Universidade Estadual Paulista (Unesp)	Brasil
401 - 500º	Universidade Federal do Rio Grande do Sul (UFRGS) Universidade Federal de São Paulo (Unifesp)	Brasil



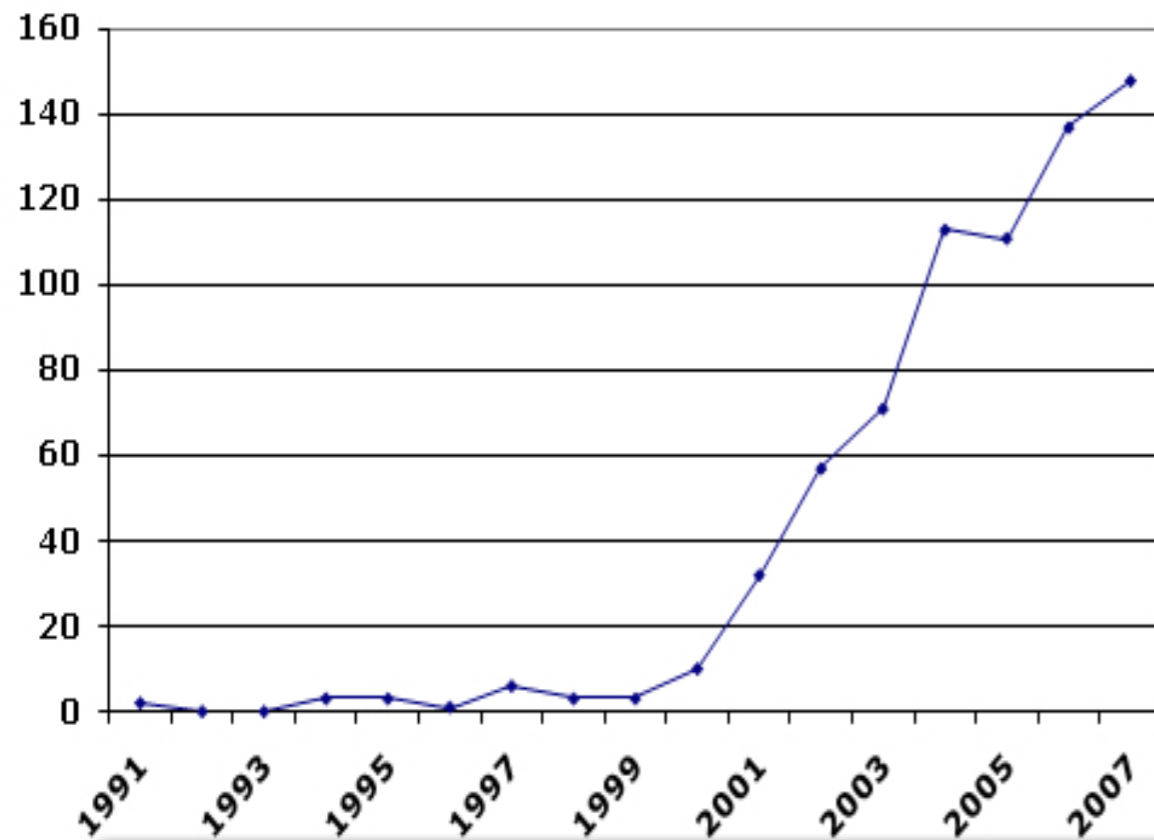
Estudo realizado pela Universidade Jiao Tong de Xangai, na China ("Ranking" 2011).



Defesa Cibernética: uma visão prospectiva

Centro de Defesa Cibernética

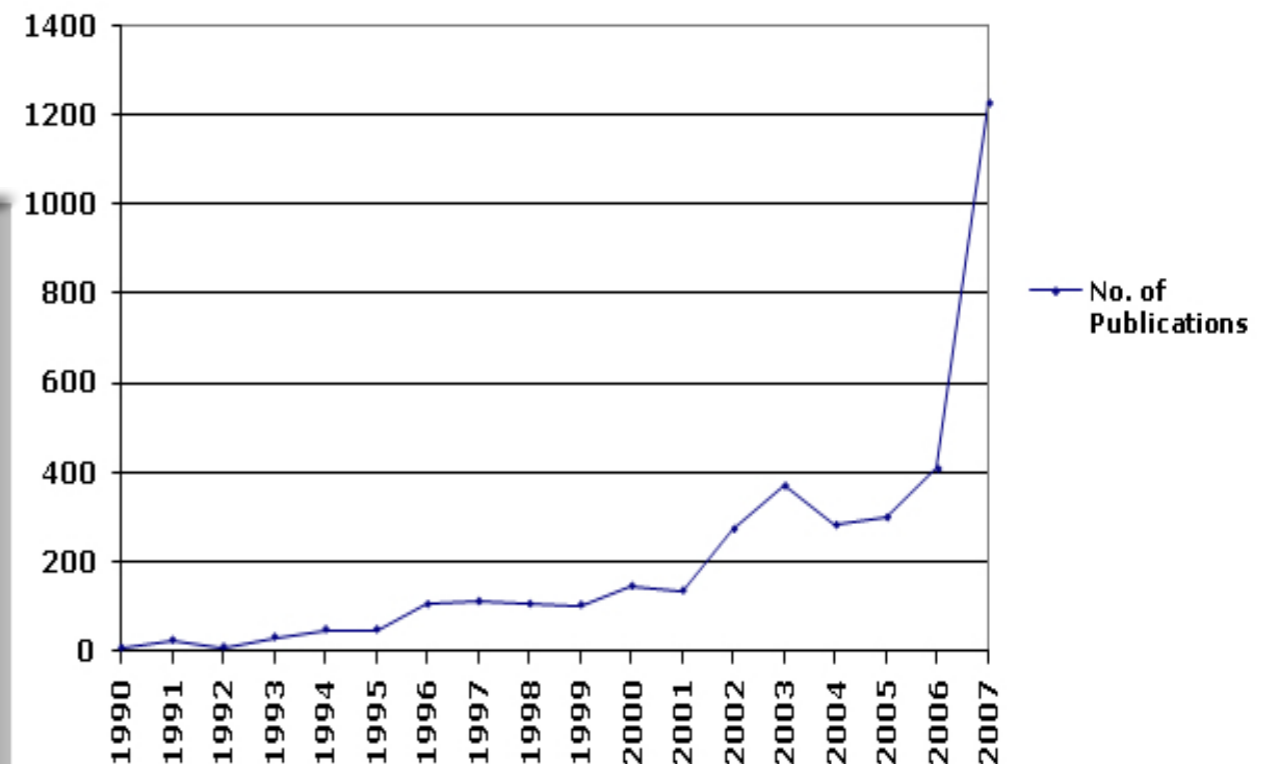
C&T no Brasil



— No. of Patents

“Information and Communication Technology (ICT) is one of the vibrant sectors of the economy, which plays a significant role in promoting economic growth, expanding economic opportunities and providing employment.”

National Institute of Science, Technology And Development Studies (NISTADS), CSIR (India)



— No. of Publications



C&T no Brasil

Para reduzir os óbices pretéritos e as ameaças atuais e futuras

Focar no desenvolvimento em TIC

Investimento é muito menor

Resultante muito mais promissora



Defesa Cibernética: uma visão prospectiva

Centro de Defesa Cibernética

Jornada de Trabalho EB - SEPIN

Julho



Setembro





Jornada de Trabalho EB - SEPIN

- Ministério da Ciência e Tecnologia (MCT)
- SEPIN/M
- Ministério do Planejamento, Orçamento e Gestão (MPOG)
- Ministério das Relações Exteriores (MRE)
- Gabinete de Segurança Institucional da Presidência da República (GSIPR)
- Secretaria de Assuntos Estratégicos da Presidência da República (SAE PR)
- Tribunal de Contas da União (TCU)
- Ministério da Defesa (MD)
- Comando da Marinha
- Comando do Exército
- Comando da Aeronáutica
- Câmara dos Deputados
- Polícia Federal (PF)
- Fundação Trompowsky
- Centro de Tecnologia da Informação Renato Archer (CTI)
- Centro de Pesquisa e Desenvolvimento (CPqD)
- Comitê Gestor da Internet no Brasil (CGI.br)
- Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)
- CERT.br
- Agência Nacional de Telecomunicações (ANATEL)
- Rede Nacional de Ensino e Pesquisa (RNP)
- Universidade Federal de Santa Maria (UFSM)
- Universidade de São Paulo (USP)
- Universidade de Brasília (UnB)
- Universidade Católica de Brasília (UCB)
- Universidade Estadual do Ceará (UECE)
- Universidade Federal de Campina Grande (UFCG)



- Universidade Federal de Minas Gerais (UFMG)
- Universidade Estadual de Campinas (UNICAMP)
- Universidade Federal de Itajubá (UNIFEI)
- CTS
- CNP
- Centro de Estudos e Sistemas Avançados do Recife (C.E.S.A.R.)
- Laboratório Nacional de Computação Científica (LNCC)
- AXUR
- Concert Technologies
- Medav
- Microsoft
- Atech Negócios em Tecnologias
- E-Sec - Segurança Digital
- Cloudshield Technologies
- Global Development Network
- Aker Security Solutions
- DECATRON
- GAS Tecnologia
- Solentech
- Módulo Solutions for GRC
- Dígitro Tecnologia Ltda
- Cyberty On Service
- ID2 Tecnologia
- Techbiz Forense Digital
- TECHGRAF/PUC RJ
- Centro de Tecnologia de Software de Brasília (TECSOFT)
- Associação Brasileira de Segurança da Informação e Comunicações (ABCIC)
- Montreal



Premissas

- Contemplar multidisciplinaridade e a dualidade das aplicações.
- Fomentar a indústria nacional de Defesa.
- Induzir a indústria nacional a produzir sistemas inovadores.
- Produzir componentes críticos nacionalmente.





Resultados



04 programas



19 projetos



R\$ 84.297.105,00



Programas



ENaDCiber



Supercomputação

Jornadas de Trabalho



Sistema Modular



Sistema de Proteção



Grandes eventos

2012



2014



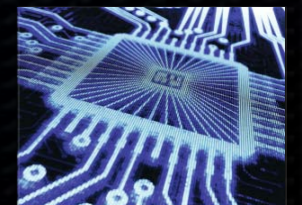
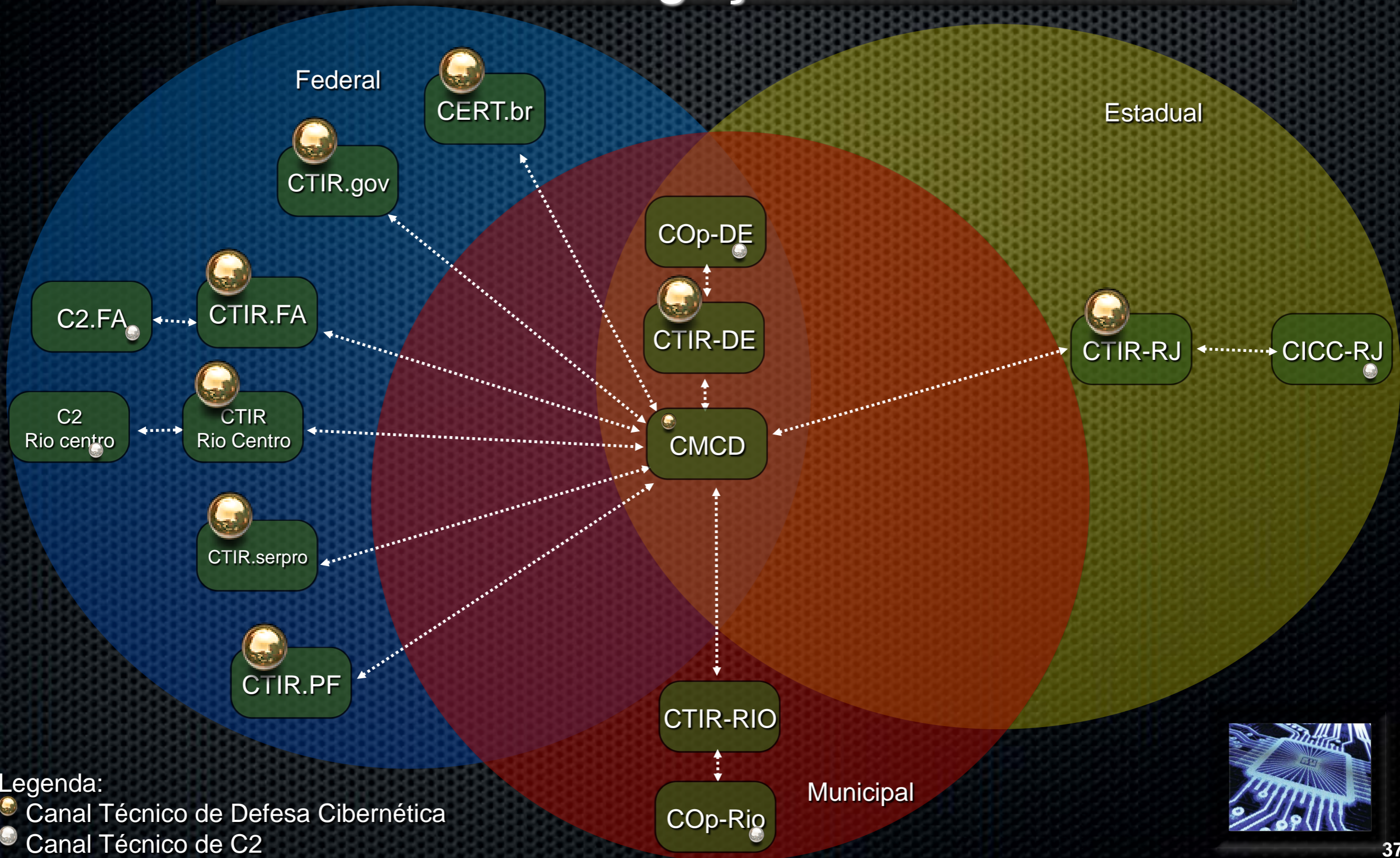
2016



Rio 2016



RIO + 20 - Ligações Necessárias





Eventos Futuros

- Estágio para Cadetes (busca de talentos)
- Curso de Guerra Cibernética
- Curso de Gestão de Redes Operacionais
- Exercício de Guerra Cibernética
- Curso de Gestão de SIC
- III seminário de Defesa Cibernética
- Coordenação da Defesa Cibernética na Rio + 20
- Participação em operações do MD
- Participação em eventos nacionais e internacionais
- Prosseguimento nos trabalhos de confecção de doutrina de Defesa Cibernética
- Ocupação da sede provisória do CDCiber





Instalações do CDCiber





Defesa Cibernética: uma visão prospectiva

Centro de Defesa Cibernética

Obrigado

