

Direção Geral
Departamento de Polícia Federal
Ministério da Justiça



Crime e Ciberespaço

Outubro/2013

Números da Internet no Brasil

- 28,1 milhões de domicílios com computador¹
- 24,3 milhões de domicílios com acesso à Internet¹
- 80,9 milhões de usuários de Internet¹
- 37 milhões de contas Internet Banking²
- Em 2012, as transações feitas em Internet Banking representaram 39% do total de transações do mercado, sendo hoje o canal preferencial de uso



¹ Fonte: Pesquisa CGI.br sobre o Uso das Tecnologias de Informação e Comunicação no Brasil – junho/2013

² Fonte: Pesquisa FEBRABAN de Tecnologia Bancária - junho/2013

Prestação de Serviços Governamentais pela Internet

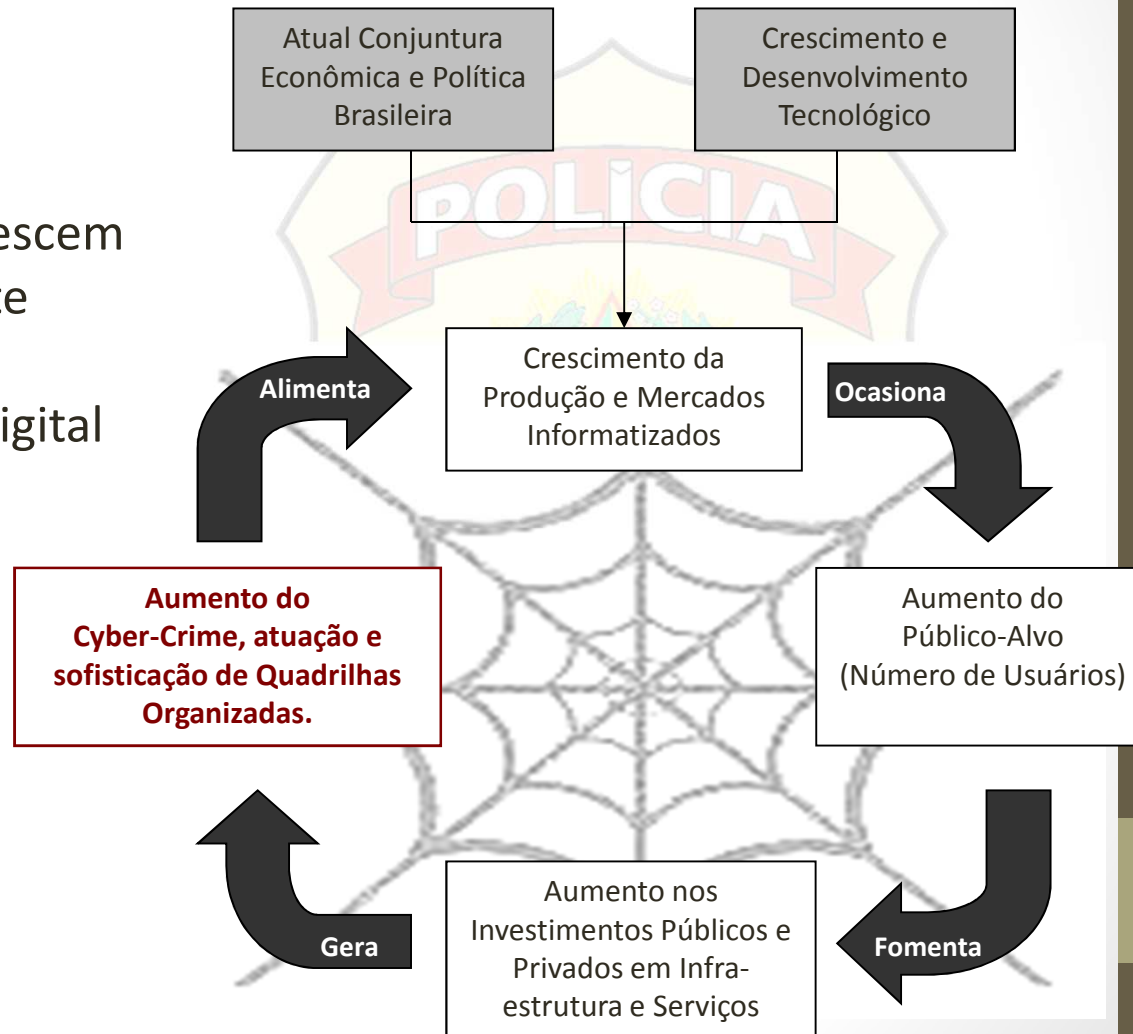
- Processos judiciais eletrônicos;
- Sistema eletrônico de votação;
- Declarações de imposto de renda;
- Sistema Nacional de Passaportes;
- Delegacias policiais virtuais;
- Outros.



e-gov

Potencial lesivo da criminalidade cibernética

Os crimes cibernéticos crescem em proporção diretamente relacionada à evolução tecnológica e a inclusão digital



Crime na Internet

- Furto em contas bancárias com Internet Banking;
- Pornografia infantil;
- Crimes de ódio;
- Crimes contra a honra;
- Ameaça;
- Venda de produtos ilegais;
- Outros.



A Polícia Federal e o combate à criminalidade eletrônica

Projeto Tentáculos



Serviço de Repressão a Crimes Cibernéticos
Coordenação Geral de Polícia Fazendária
Diretoria de Combate ao Crime Organizado

Antes do Projeto Tentáculos

Modelo de Atuação Tradicional

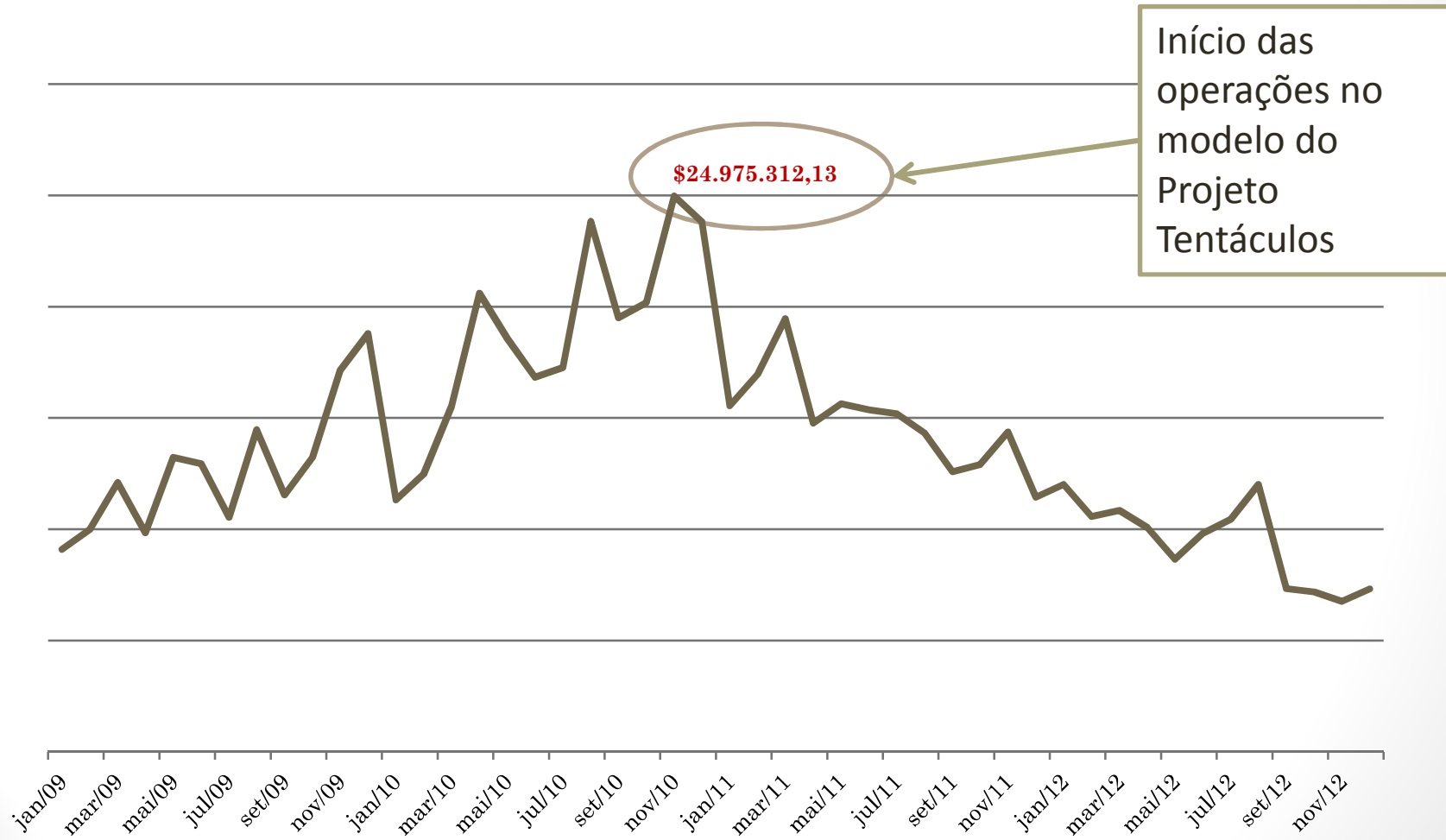
- **CADA** notícia crime = **UM NOVO** inquérito policial
- Comunicações dispersas pelo País
- Informações limitadas
- Impossibilidade de cruzamento de dados
- Instauração do IPL no local da conta vítima

Projeto Tentáculos

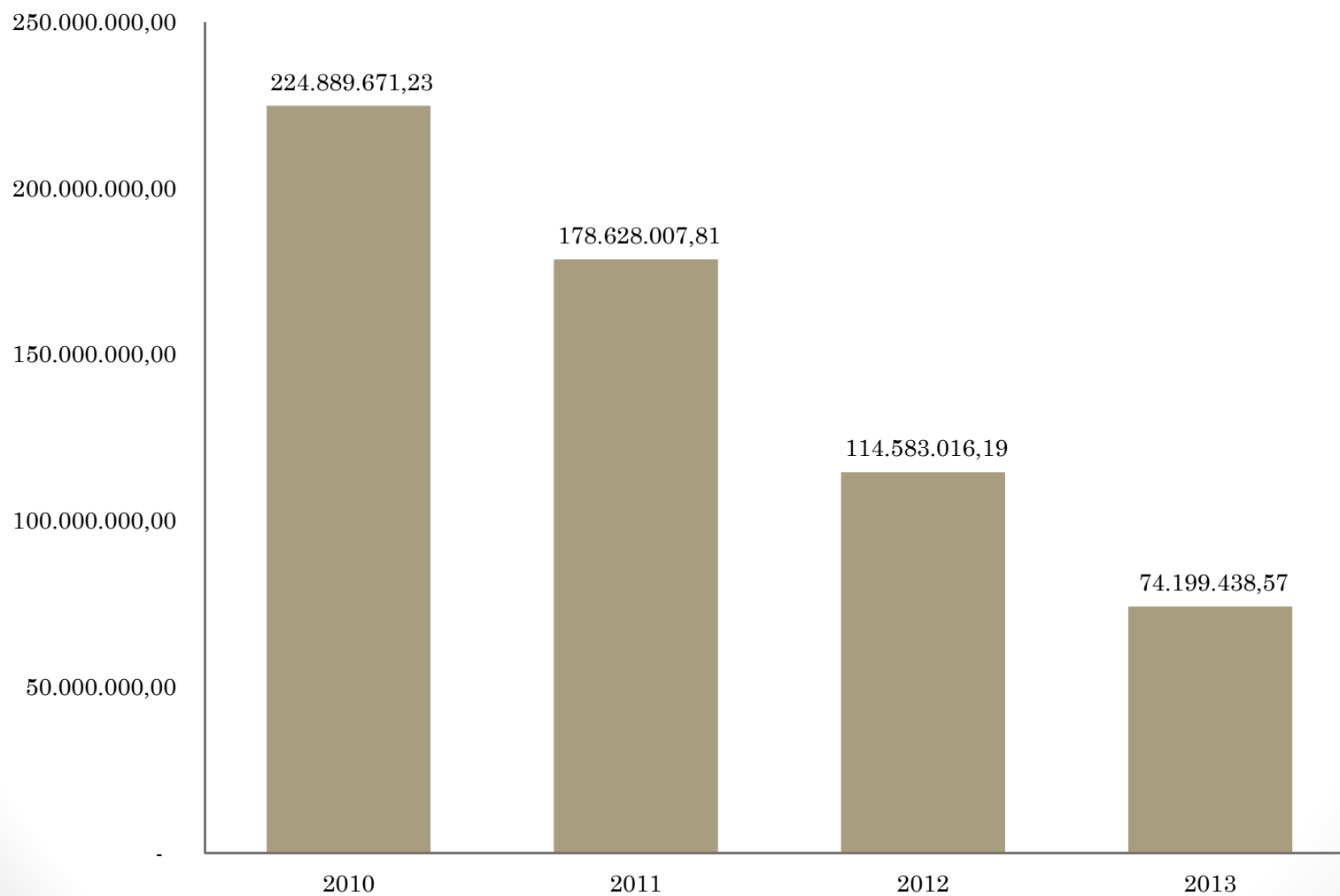
Novo Modelo de Atuação

- Celebração de um termo de cooperação técnica entre Polícia Federal e Caixa Econômica Federal
- Comunicação eletrônica centralizada de notícias crime
- Criação de uma base de dados nacional (BNFBe – Base Nacional de Fraudes Bancárias Eletrônicas)
- Cruzamento prévio de informações
- Combate prioritário à criminalidade organizada
- Seleção do melhor local para a investigação
- Estudos prospectivos para planejar atuação preventiva

Evolução Mensal do Prejuízo Financeiro

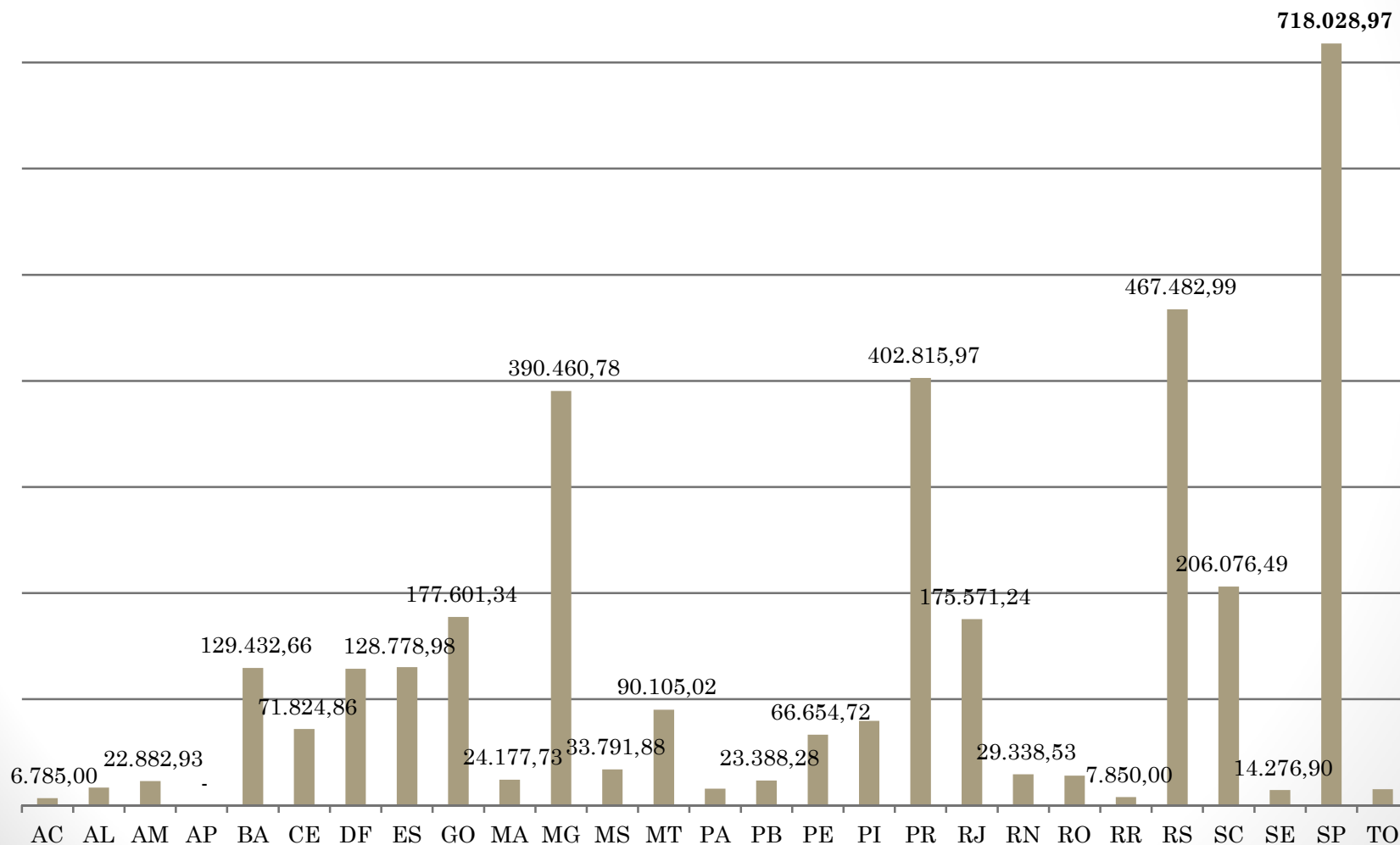


Decréscimo do prejuízo registrado



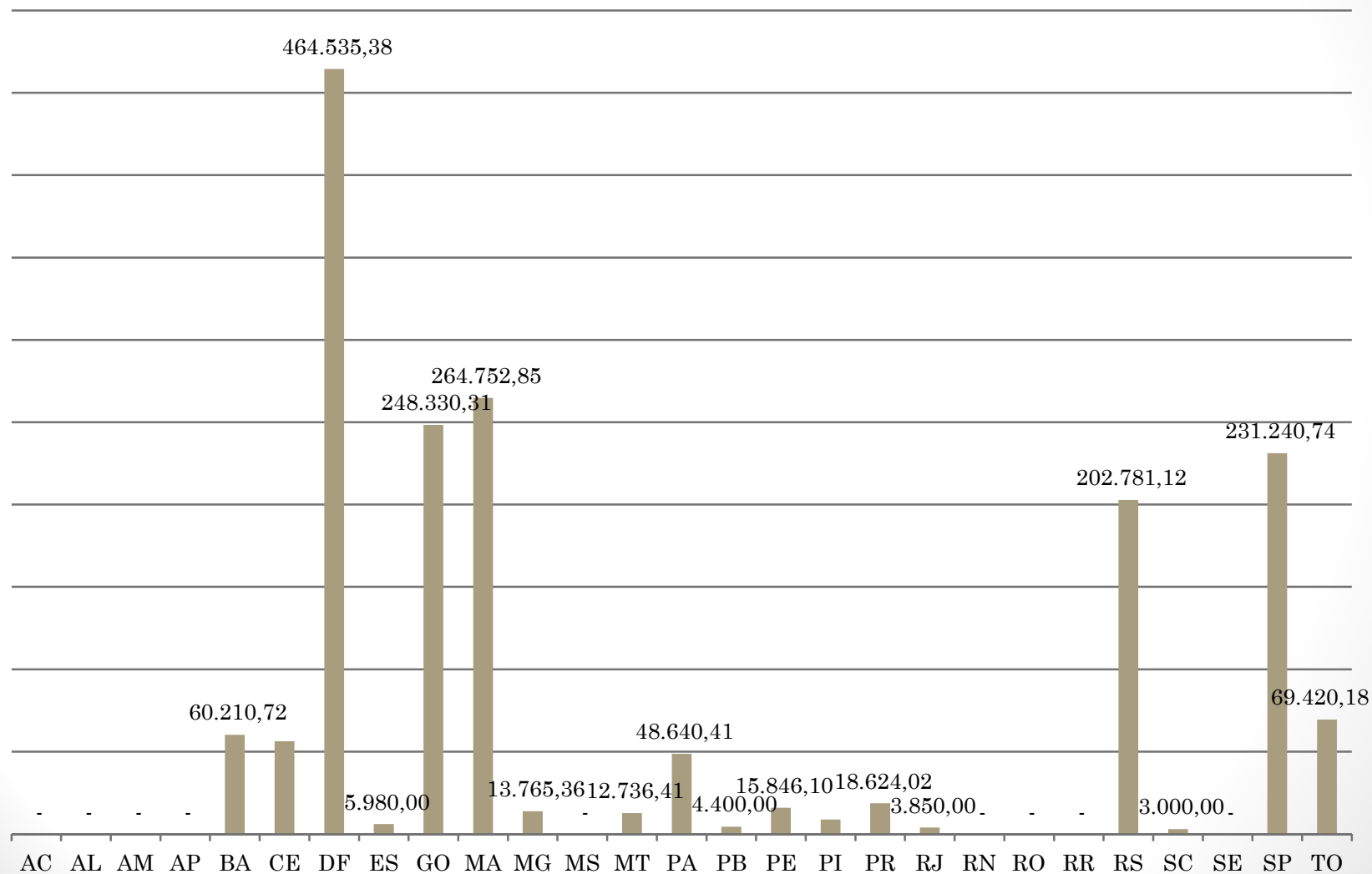
Estudos Prospectivos

Transferências Internet ORIGEM 2013



Estudos Prospectivos

Transferências Internet DESTINO 2013



Nova Criminalidade Eletrônica

- Pichação eletrônica (*defacement*);
- Ataques de negação de serviço (*DDOS – distributed denial of service*);
- Invasão de computadores;
- Roubo de dados eletrônicos;
- Extorsão online.



Os ataques já começaram!

- Em 2010, Hackers brasileiros aproveitaram uma onda de ataques internacionais para atacar “sites” e base de dados no Brasil, principalmente, de órgãos públicos federais, com o objetivo de:
 - Acessar e copiar dados pessoais e institucionais;
 - Alterar o teor do site (*defacement* ou “pichação eletrônica”);
 - Impedir o funcionamento do site (ataques de negação de serviço ou DDOS – *distributed denial of service*).
- Estas novas práticas se mantêm até hoje.



Lacuna Legal

- Antes da Lei de Delitos Informáticos (Lei 12.735/13), era necessário estabelecer analogias
- Problemas enfrentados:
 - Impossibilidade de aplicar analogia no Código Penal para algumas condutas altamente especializadas
 - Investigações iniciadas eram sobrestadas ou encerradas por dificuldades legais
 - Provedores de conexão e de conteúdo na Internet não estavam preparados para atender as demandas das investigações
 - Utilização de técnicas especiais de investigação restava prejudicada

Lei 12.735/2013

- Dispõe sobre a tipificação criminal de delitos informáticos
- Alterou o Código Penal, modificando e inserindo condutas típicas adequadas ao combate à criminalidade cibernética
- Destaques:
 - **Invasão de dispositivo informático (CP art.154-A)**
 - **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (CP art.266, §1º)**

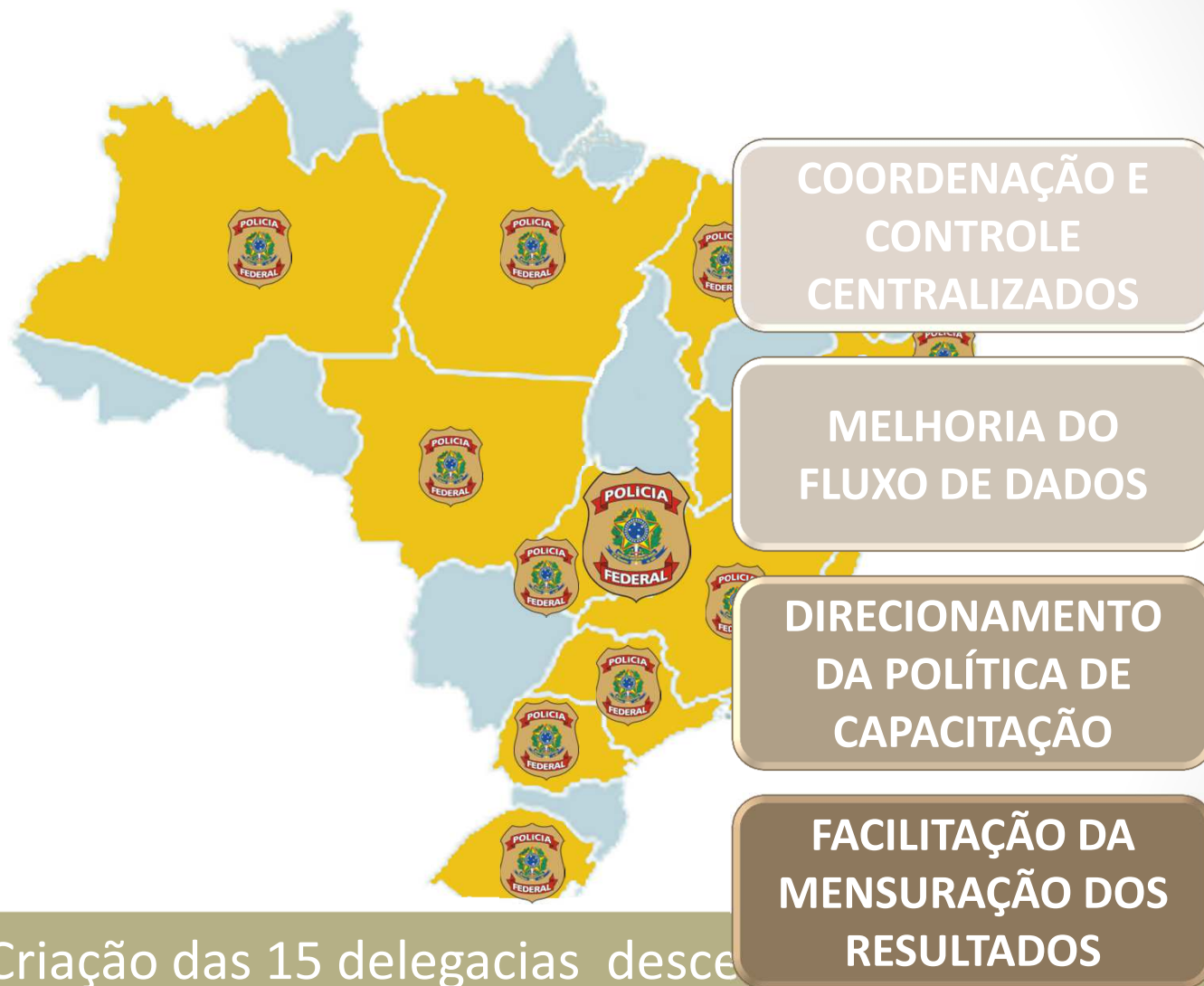
Riscos emergentes

Durante a realização de grandes eventos, ataques desta natureza tomam proporções ainda maiores:



**BRASIL EM EVIDÊNCIA NO CENÁRIO MUNDIAL
REPRESENTANDO RISCOS E OPORTUNIDADES**

Como agiremos?



2

Criação das 15 delegacias descentralizadas para a repressão a crimes cibernéticos (14 estados e DF)



Obrigado!

João Vianey Xavier Filho

Delegado de Polícia Federal