"A Ciber-resiliência no setor financeiro"

Em defesa do ciberespaço

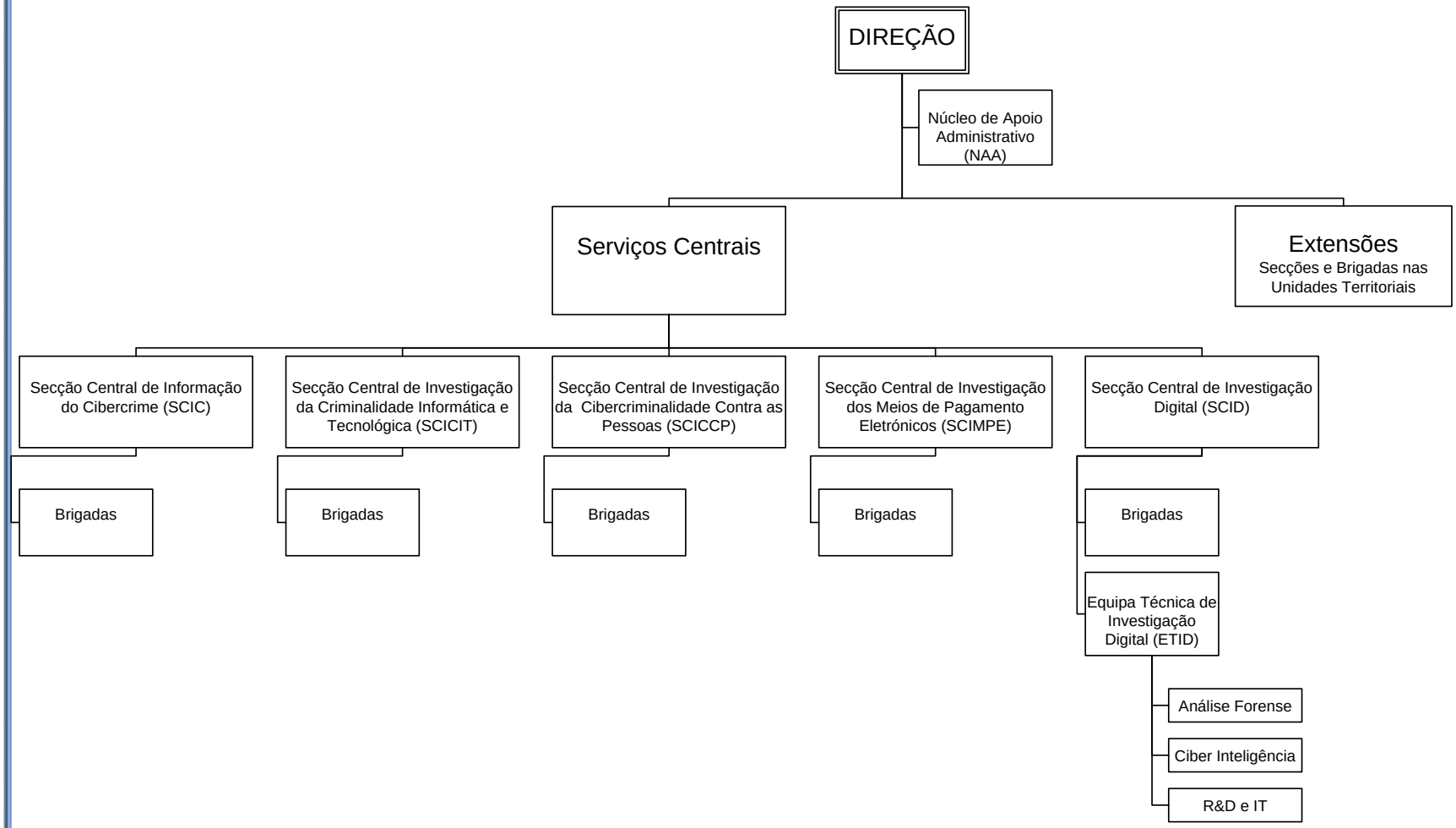
Carlos Cabreiro, jun. 2019

Agenda

- Unidade do Cibercrime –UNC3T
- Áreas de cooperação estratégica
- Tendências do cibercrime/setor financeiro
- Sinergias e desafios

UNC3T - organização

Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica



UNC3T - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

- Áreas de intervenção
  - **Hacking, ciberatacks**
    - Intrusão em sistemas
    - Botnets, Malware, Ransomware
    - Banca online (phishing)
    - Furto de identidade (Identity thief)
    - Extorsão
    - Exfiltração de dados (privada, concorrência desleal, segredo comercial)
    - “CEO fraud”

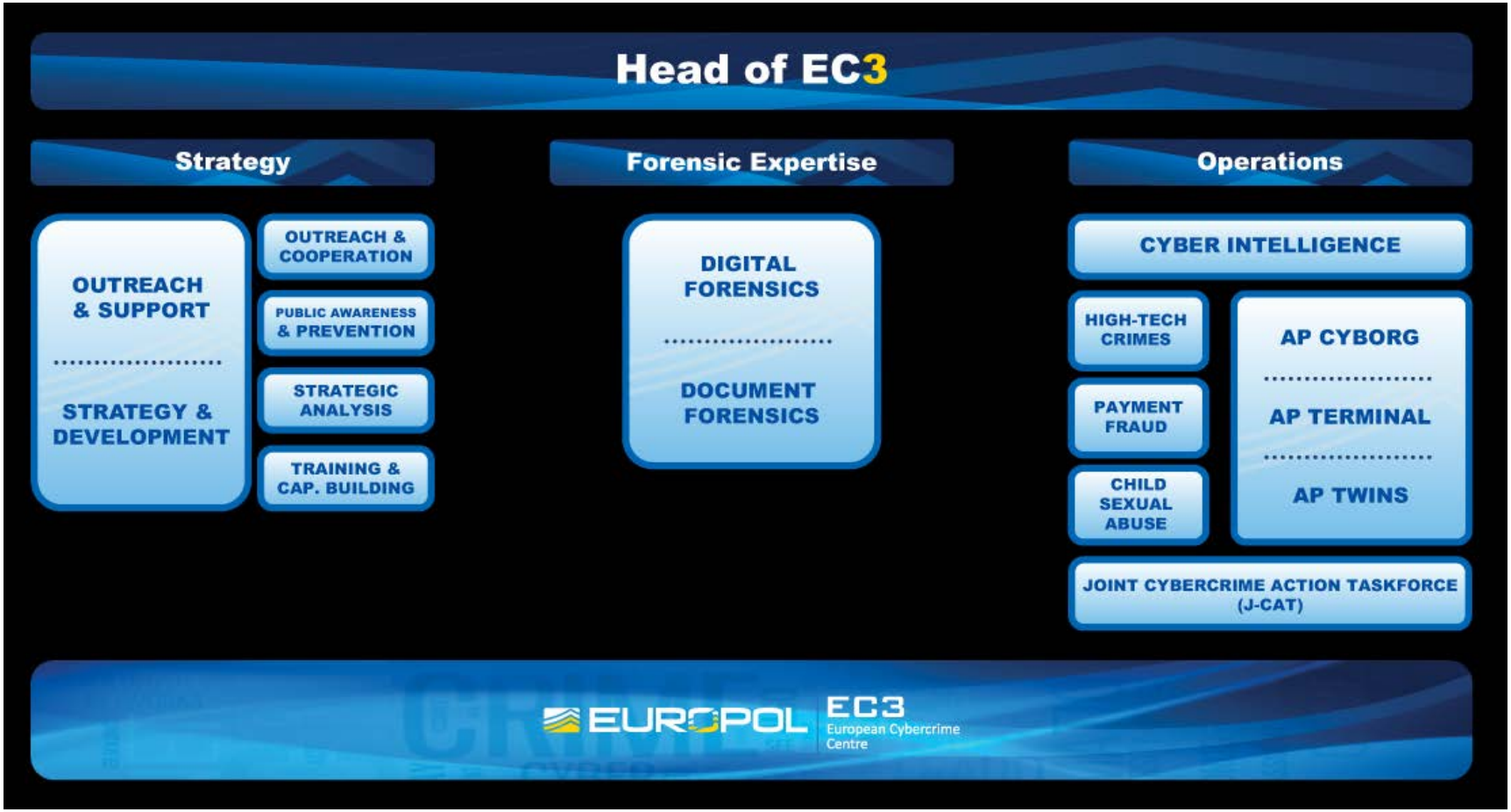
UNC3T - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

- Áreas de intervenção
  - **Meios de pagamento eletrónicos**
    - Contrafação e clonagem de cartões
    - Cartão não presente – e-comerce
    - Cartões pré-pagos
    - Mercados virtuais
    - Cripto moedas (bitcoin)

UNC3T - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

- Áreas de intervenção
  - **Abuso sexual de crianças online**
    - Pedofilia/pornografia de menores
    - “Sextortion”
    - Sofisticação
    - Repositórios de imagens (ICSE)
    - Deslocalização do crime (anonimização, Tor, P2P)
    - Cooperação internacional

Cooperação Estratégica/ Europol



Cooperação Estratégica/ Europol

- *EMAS – EUROPOL MALWARE ANALYSIS SYSTEM*" edoc-799327-v2-europol_malware_analysis_system_2 (2).pdf
  - Deteção e análise automática de malware enviado pelos EM
  - Submissão a exame forense em ambiente e sistema protegido
  - Eliminação de efeitos adversos noutros sistemas
  - Facilidade de cruzamento
- "*No More Ransom*" https://www.nomoreransom.org/pt/index.html
- *Plataforma do EC3*
- ECTEG- European Cybercrime Training and Education Group http://www.ecteg.eu/courses.html
- *ICSE* - International Child Sexual Exploitation – Interpol
- contacto24.7@

Cooperação Nacional

- Ligação com o CNCS;
- Grupo de trabalho com cibersegurança, ciberdefesa, e serviços de informações;
- Partilha de modelos sobre taxonomia e níveis de alerta comum;
- Modelo de análise forense (recolha, tratamento e análise de prova digital);
- Intervenção sobre o poder legislativo;
  - Novos meios de obtenção de prova
  - Legislação sobre conservação e obtenção de dados de tráfego
  - Transmissão e preservação de prova por parte dos ISPs
- Cooperação com BP; APB

Tendências do cibercrime

- ✓ Aumento de APT (Advanced Persistent Threat)
- ✓ Anonimização e cifragem
- ✓ Branqueamento de capitais com recurso a moedas, contas bancárias e cartões virtuais
- ✓ Ataques dirigidos com exfiltração de Informação sensível/dados pessoais
- ✓ Exposição a campanhas de extorsão com base em programas maliciosos - rasomware", sextortion"
- ✓ Hacktvismo

A ameaça v. setor financeiro

- ✓ Ressurgimento de ataques de “phishing” com base em obtenção ilícita de 2ªvias de cartões SIM;
- ✓ Aperfeiçoamento e variantes de atuação das “Money Mules”
- ✓ Ataques lógicos sobre ATMs
- ✓ Criminalidade associada aos cartões “pré-pagos” e “moedas virtuais”
- ✓ Criminalidade “Insider“ e Engenharia Social


Sinergias e Desafios

Ciberespaço

- Características:
  - Desafio de limites:
    - Velocidade
    - Territorialidade
    - Do próprio conceito de nação
  - Não tem restrições geográficas ou de tempo
  - Possibilidade de dano alargado sobre número elevado de pessoas e num curto espaço de tempo
  - Grande capacidade do crime organizado

Questões associadas à prova

- Atribuição V Retribuição
- Rastreabilidade dificultada (No traceabillity)
  - cifragem,dissimulação, fácil destruição
- Anonimização
  - Falsa identidade
  - *"Avatares"*
  - Utilização de recursos alheios (botnets)
- Prova essencialmente técnica

Questões associadas à prova

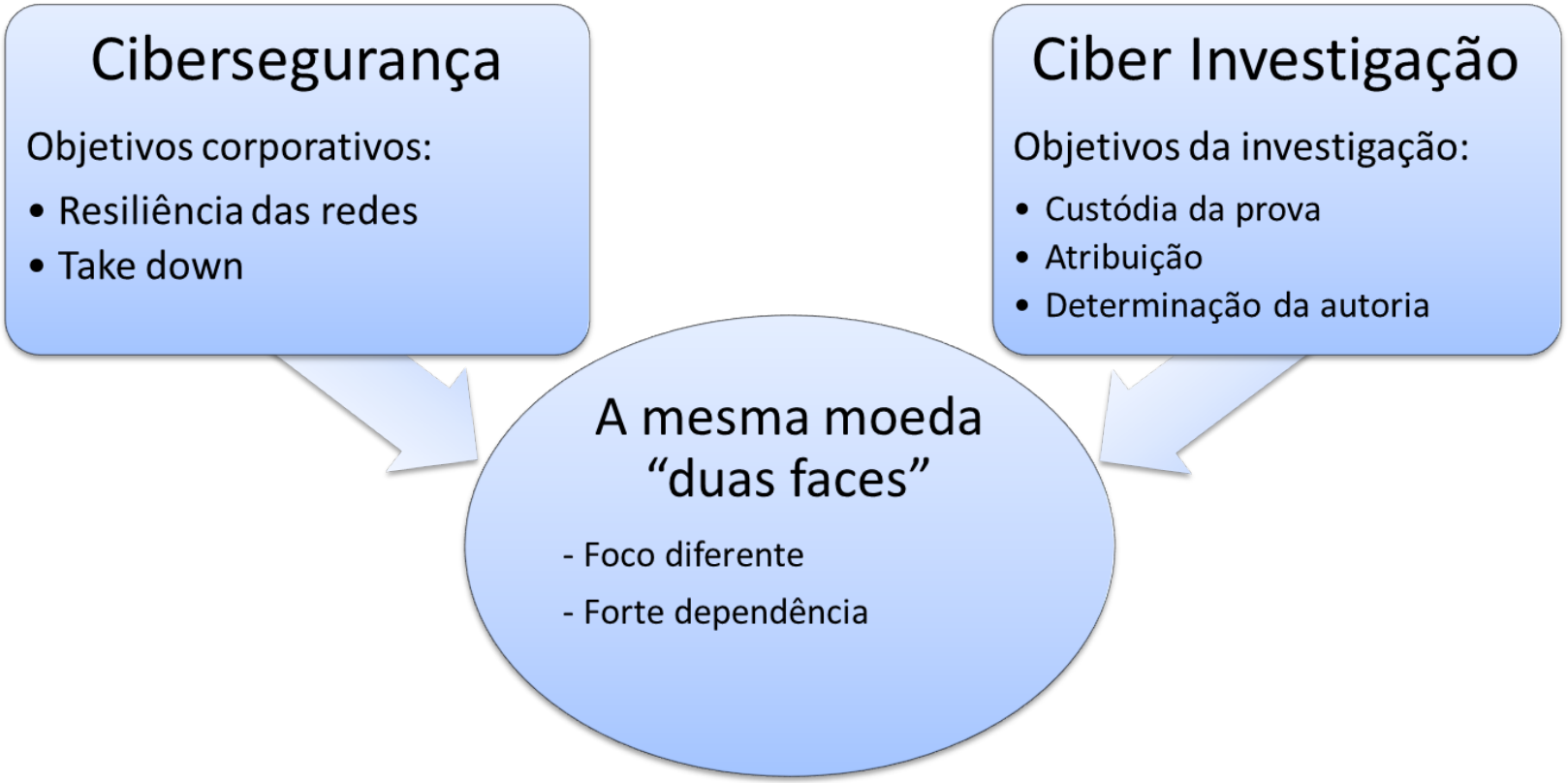
- Grande dependência de opinião especializada
- Não existe prova testemunhal
- Exigências do julgamento
- Nível de ameaça crescente
- Preocupações de governabilidade

  - Dimensão virtual e física
    - Intervenção humana
    - Conjunto de componentes físicos
    - Comunicação em rede

Os dados de tráfego

- ✓ Metadados
- ✓ CGNat Carrier-grade NAT
- ✓ Regime de acesso
- ✓ Acesso transfronteiriço
- ✓ Diretiva E-Evidence

Cooperação Nacional



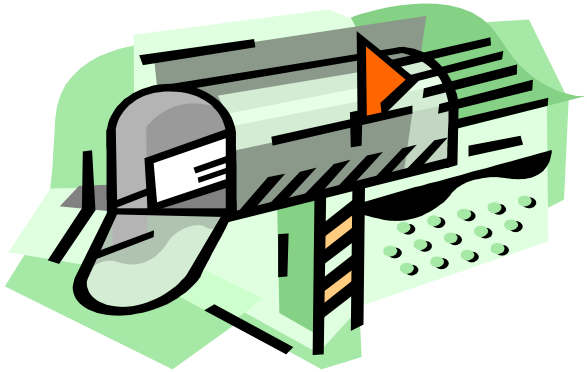
O significado de "atribuição" em processo penal

Caso MO “Phishing+SIM”

- A queixa crime
- Intelligence (NUIPCs, Tlm, mails associados,)
- Caráter transnacional
- Branqueamento (mecanismos de bloqueio e congelamento, identificação de contas de destino)
- O takedown dos sites de distribuição de phishing (CNCS)
- A intervenção expedita sobre ISPs
- Interferir na ação criminosa (Money mules)
- Coligir indicadores de compromisso e divulgar
- Afetar a capacidade, vontade e oportunidade do COrg

Obrigado

Polícia Judiciária



Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

UNC3T

Rua Gomes Freire, Edifício sede - Lisboa

Tel. 21 864 10 00

Fax: 21 864 19 96

E-Mail : UNC3T@pj.pt

Url: http://www.pj.pt