



DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

Política e Plano de Ação para a Ciberdefesa NATO: Perspetivas de Evolução

CFR Sérgio da Silva Pinto
29 abril 2016

10º Simpósio Internacional “Estratégia da Informação Nacional”



DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

1. Evolução da Ciberdefesa na NATO
2. Contributo de Portugal para a Ciberdefesa NATO
3. Perspetivas Futuras



DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

1. Evolução da Ciberdefesa na NATO



2008:

1ª Política de Ciberdefesa

- ❖ Responsabilidade NATO vs Aliados
- ❖ *NATO Computer Incident Response Capability (NCIRC)*



2010:

“Ciberataques ameaçam
segurança Euro-Atlântica”

2011:

2ª Política de Ciberdefesa

- ❖ Objetivos capacitários
NATO Defence Planning Process



2014:

Política Reforçada de Ciberdefesa

- ❖ Defesa Coletiva (art. 5º)
- ❖ Direito Internacional



DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

2. Contributo de Portugal para a Ciberdefesa NATO



Assistência a Aliados

- ❖ Equipas Reação Rápida NATO
- ❖ MoU NATO - Portugal



Liderança Formação e Treino

- ❖ NCI & Cyber Academy (Oeiras)
- ❖ Smart Defence MN CD E&T



Cooperação NATO-UE

- ❖ Plataforma coordenação E&T
- ❖ NCI & Cyber Academy para UE



DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

3. Perspetivas de Evolução - NATO



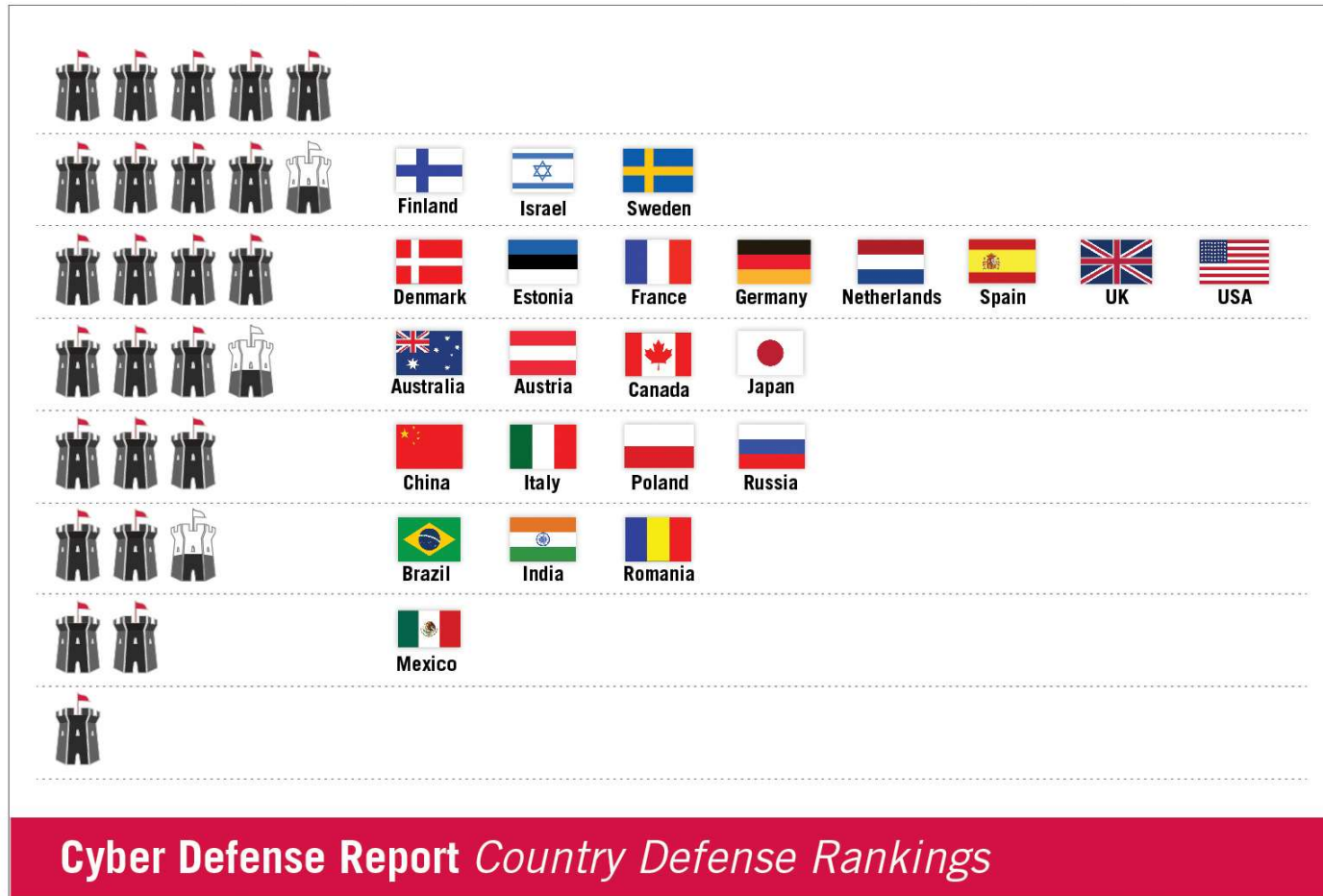


DELEGAÇÃO
DE PORTUGAL
NA NATO



PORTUGUESE DELEGATION TO NATO

3. Perspetivas de Evolução - Nacional



Cyber Defense Report *Country Defense Rankings*

Source: SDA Cyber Defense Report Sponsored by McAfee. Full report can be downloaded at www.mcafee.com.





DELEGAÇÃO DE PORTUGAL NA NATO

PORTUGUESE DELEGATION TO NATO



CFR Sérgio da Silva Pinto

smpinto@bx.emgfa.pt

+32 (0)27 076 412



Revista da ARMADA

Ciber-Trilogia

- Abril
- Maio
- Julho



Revista da ARMADA

CONDIÇÃO MILITAR

NIP BARTOLOMEU DIAS NA MADEIRA TORPEDO BLACK-SHARK CTM EM TIMOR-LESTE



Strategia 22

Cibersegurança e ciberdefesa – Portugal e NATO

INTRODUÇÃO

Quando os investigadores da Adversus Research Project Agency, do Departamento de Defesa norte-americano, citaram em 1990 o perigo da Internet, não podiam imaginar o impacto que a sua invenção veio a ter em todo o Mundo. Só a título ilustrativo, refira-se que hoje atualmente mais de 3 mil milhões de páginas web. Contudo, quando a Internet foi originalmente concebida não houve grandes preocupações de segurança, pelo o objetivo era apenas criar um sistema aberto que permitisse a cientistas e investigadores enviar informação de forma espónea. Dessa forma, o ciberecossistema veio, desde início, bastante vulnerável aos mais variados tipos de ataques cibernéticos, sendo que a dependência da sociedade atual relativamente a este novo domínio (incluindo na área militar), apenas veio potenciar os riscos decorrentes desses ataques. De tal forma que o Director of National Intelligence norte-americano classificou recentemente a ameaça cibernética como sendo a principal ameaça estratégica ao país.

Centos de riscos neste domínio, no EUA lançaram em Junho de 2008 (i.e. pouco tempo após o celebre ciberataque à Estónia) a primeira Diretiva Presidencial dedicada à cibersegurança, sob o título Cybersecurity Policy. Pouco depois, em 2009, editaram o Cybersecurity Policy Review e criaram, no seio das suas Forças Armadas, o US Cyber Command, com a missão de coordenar o comando das operações no ciberecossistema e coordenar a proteção das redes militares norte-americanas.

No entanto, os desenvolvimentos na cibersegurança e na ciberdefesa ocorreram com algum atraso, embora a Estónia (por motivos óbvios) também tenha lançado a sua Estratégia de Cibersegurança em 2008. Muitos outros países europeus só seguiram em 2011 (entre os quais, se pontuam Alemanha, França e Reino Unido), espelhando uma tendência que se foi propagando aos outros Estados da UE nos anos seguintes.

nes ou chés, coletivos ou individuais), cooperação (com Aliados e parceiros, nacionais e internacionais), proporcionalidade (dos meios e medidas empregues na cibersegurança) e sensibilidade (nomeadamente, dos utilizadores finais, para a importância da prevenção de riscos). Neste quadro, permitimo-nos destacar a importância verdadeiramente fundamental da cooperação, não só entre Estados, mas também com os setores industrial, comercial e tecnológico, que dispõem de competências e de conhecimentos essenciais para a proteção do ciberecossistema. Além disso, a Estratégia Nacional de Segurança do Ciberecossistema atribui um papel nuclear ao Centro Nacional de Cibersegurança na coordenação operacional, em matéria de cibersegurança, das entidades públicas e das infraestruturas críticas. Cabe aqui referir que o Centro Nacional de Cibersegurança foi criado em maio de 2014, funcionando no âmbito do Gabinete Nacional de Segurança, assim, na dependência do Primeiro-Ministro, com a missão de "contribuir para que o país use o ciberecossistema de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança".