ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

9º Fórum das Comunicações da CPLP

22 de março, 2018

Da Cibersegurança à Ciberoportunidade

Painel II - Ameaças e desafios colocados aos Estados. Que estratégias de futuro para garantir a cibersegurança na CPLP?

José Sousa Barros

22 III 2018

ÍNDICE

- **Agenda Global para a Cibersegurança**
- ***TC Cyber***
- ***Digital Single Market strategy*** *'the cybersecurity act'*
- **Grupo de trabalho sobre a segurança e privacidade na economia digital**

Agenda Global para a Cibersegurança

- Matriz para a cooperação internacional de promoção da cibersegurança e valorização da confiança e segurança na sociedade de informação
- Lançada em maio de 2007, na *World Summit on the Information Society* (***WSIS*** – Conferência Mundial da Sociedade de Informação) como alinhamento aos Objetivos de Desenvolvimento Sustentável, pelo então Sec.-Geral Hamadoun I. Touré, promove a Cibersegurança através de cinco pilares ou Áreas de Trabalho:
  - **Medidas legais**: compatibilidade internacional
  - **Medidas técnicas e procedimentais**: vulnerabilidades em *software* (produtos, acreditações, protocolos e normas)
  - **Estruturas organizacionais**: matrizes genéricas e respostas estratégicas de prevenção, deteção, resposta e gestão de crises a ciberataques – incluindo infraestruturas críticas de sistemas de informação nacionais
  - **Capacitação**
  - **Cooperação internacional**: diálogo e coordenação face a ciberameaças

Global cybersecurity index https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Agenda Global para a Cibersegurança

- Para a Agenda Global para a Cibersegurança - ou WSIS Action Line C5 - em discussão no próximo Conselho (abril), o Secretário-Geral apresentará os seguintes desenvolvimentos:
  - **Medidas legais**: entre outros, trabalho desenvolvido em proximidade com a United Nations Office on Drugs and Crime, desde 2011, é possível apoiar estratégias nacionais de Cibersegurança, harmonizadas regional e internacionalmente, conforme ITU Cybercrime Legislation Resources
  - **Medidas técnicas e procedimentais**: destaque para o *Study Group* (SG17) exclusivamente dedicado ao tema

O *Study Group* 17 (**SG17**) do Sector de Normalização da UIT (UIT-T) foi criado em 2001 e tem por missão desenvolver trabalho para criar confiança e segurança no uso das TIC e em resultado disso existem mais de 170 normas (Recomendações e suplementos do Sector T) publicados cujo enfoque é a segurança das infraestruturas das redes de comunicações, serviços e aplicações. O SG17 coordena transversalmente todos os grupos de estudo do Sector T no que diz respeito à segurança e coopera ainda nesse âmbito com outras organizações de desenvolvimento de normas e consórcios industriais

- **Medidas técnicas e procedimentais**:

Especificamente, o **SG17** desenvolve trabalho orientado para (20 temas):

Cibersegurança / gestão da segurança / arquiteturas e referenciais de segurança para redes / combate ao *spam*, à contrafação de equipamentos e ao roubo de dispositivos móveis / IMT-2020 (*International Mobile Telecommunications* e 5G para o alcance de uma sociedade interligada em 2020) / sistemas RFID (*Radio Frequency IDentification*) / *e*-saúde / gestão de identidade / proteção da informação pessoal e proteção *online* de menores / segurança de aplicações e serviços para a *Internet of Things* (*IoT*) / *smart grids* (redes de eletricidade, gás, água) / *smartphones* / *software-defined networking* (SDN) / serviços *web* / *big data* / redes sociais / computação na *cloud* / sistemas financeiros móveis / televisão por IP (IPTV) / telebiometria

Standardizing Security https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx

- **Medidas técnicas e procedimentais**:

Algumas referências importantes do trabalho desenvolvido pelo **SG17** :

- Recomendação ITU-T X.509 para autenticação eletrónica em redes de comunicações públicas
- *Cybersecurity Information Exchange* (CYBEX – ITU-T X.1500) – conjunto de técnicas e ferramentas para assegurar respostas rápidas e coordenadas a nível internacional contra ameaças cibernéticas. Contém um mecanismo normalizado para troca de informação de cibersegurança que é necessária para os *Computer Incident Response Teams* (CIRTS) atuarem com eficácia, e é uma ferramenta essencial para prevenir o contágio entre nações dos ataques cibernéticos
- Recomendação ITU-T X.805 que dá aos operadores de redes de comunicações e às empresas a capacidade de descreverem uma arquitetura integrada dos sistemas a partir de uma perspetiva de segurança

- **Medidas técnicas e procedimentais**:

  Algumas referências importantes do trabalho desenvolvido pelo **SG17** :

- Recomendação ITU-T X.1254, que apresenta um quadro de referência para assegurar a autenticação de entidades nas comunicações eletrónicas. Define quatro níveis de segurança de autenticação e os critérios e as ameaças a endereçar para cada um dos níveis. Esta recomendação permite a troca segura de dados entre entidades e reduz a fraude, a usurpação de identidade e a capacidade dos *hackers* comprometerem o funcionamento das organizações
- Recomendação X.1040: gestão de *e-commerce*
- Recomendação X.1053: código de segurança de informação para PME de telecomunicações
- Recomendação X.1146: proteção para serviços de valor acrescentado de operadores de telecomunicações
- Recomendação X.1213: requisitos de prevenção de *botnets* em *smartphones*
- Recomendação X.1248: requisitos de prevenção de SPIM (*spam* em SMS)

- **Medidas técnicas e procedimentais**:

Para além de três novas Recomendações para aprovação na próxima reunião do **SG17** (março), presentemente trabalha-se para aprovação a curto prazo de:

- Matriz técnica de prevenção de publicidade *spam* em aplicações móveis
- Matriz de segurança para a Internet das Coisas (*IoT*)
- Matriz de segurança para redes de *voice-over-long-term-evolution* (*VoLTE*)
- Protocolo de autenticação em metadados

Em estudo está o desenvolvimento de normalizações de facetas de segurança de *Blockchain*, a discussão de requisitos de segurança de todos os intervenientes na cadeia de valor de sistemas de transmissão de dados, a realização de *workshop* sobre Segurança em 5G, a segurança em *IoT* (em comunidades), e, a permanente normalização nas radiocomunicações modernas: segurança em IMT – *International Mobile Telecommunications*, sistemas digitais em satélites e melhoria de desempenho de protocolos de transmissão em redes de satélites.

- **Estruturas organizacionais**:

National CIRT Programme (https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) – 103 países já oficializaram o seu CIRT - *National Computer Incident* / 68 países dispõe de equipas de resposta a incidentes computacionais, em avaliação / *Cyber*exercícios em mais de 100 países

National Estrategies https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx Guia de referência / em fase final ddesenvolvimento de estojo de ferramentas para uma Estratégia Nacional de Cibersegurança

Securing Radiocommunications
https://www.itu.int/en/action/cybersecurity/Pages/radiocommunications.aspx

Agenda Global para a Cibersegurança

- **Capacitação**:

Organização de fora regionais / período de estudos 2018-2021, realização de ações e eventos de formação, seminários

- **Cooperação internacional**:

Parceria com várias organizações e iniciativas

Destaque para o Council Working Group on Child Online Protection (CWG-COP): Grupo de Trabalho para a Proteção de Crianças em Linha

Agenda Global para a Cibersegurança

Em conclusão:

- A área da Cibersegurança é dos assuntos mais sensíveis que atualmente se discutem na UIT, sendo um tema fraturante entre Membros da UIT, em diversas reuniões / fora da UIT
- Países como a Rússia, China e países em desenvolvimento procuram reforçar a importância da UIT na arquitetura de um edifício global para a Cibersegurança. Do outro lado, alguns países da União Europeia, os Estados Unidos, Japão e outros países desenvolvidos opõem-se, de um modo geral, a esta crescente importância, defendendo que há outros instrumentos e Organizações mais capazes para endereçar o problema, com destaque para a Convenção de Budapeste
- Mantém-se como tema cada vez mais recorrente nas diversas atividades da UIT em que é de realçar a Visão da China (em documento para o Grupo de Peritos UIT em **International Telecommunication Regulations** (**EG-ITRs**), que alerta para um "dividendo digital" crescente entre regiões e países num contexto crítico de infraestruturas ainda muito vulneráveis

Agenda Global para a Cibersegurança

Visão da China:

O Desenvolvimento e Segurança surgem lado a lado, sendo essencial uma liderança previsional para abordar:

. crescentes questões de segurança em redes internacionais de telecomunicações/TIC

. proteção de informação privada dos consumidores

. global e constante alargamento do distanciamento digital

Recomendação da China:

Regulação internacional que transforme o tradicional Serviço Universal incorporando o investimento (financeiro e em redes) dos operadores, em objetivos universais, permitindo um entendimento comum que acompanhe os desenvolvimentos, privilegiando o diálogo ao confronto

TC Cyber

European Telecommunications Standards Institute (formado pela Comissão Europeia em 1988, inclui fabricantes e operadores): encara a cibersegurança na vertente técnica e de normalização, tendo sido especialmente criado, em 2014, um Comité Técnico *TC Cyber*

(https://portal.etsi.org/TBSiteMap/CYBER/CyberToR.aspx.)

Termos de Referência (atividade):

- Cibersegurança
- Segurança de infraestruturas, equipamentos, serviços e protocolos
- Aconselhamento em segurança, orientação e requisitos de segurança operacional para utilizadores, fabricantes e operadores de infraestruturas e redes
- Técnicas e ferramentas de segurança
- Preparação de mecanismos de segurança de proteção de privacidade
- Criação de especificações de segurança e alinhamento com outros Comités Técnicos

Digital Single Market strategy
'the cybersecurity act'

A ENISA – *European Network and Information Security* (*https://www.enisa.europa.eu/*) agência fundada em 2004, presta apoio à União Europeia (UE) e aos países da UE na prevenção, deteção e resposta a incidentes de segurança da informação

http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)

Em setembro de 2017, a Comissão Europeia publicou pacote legislativo sobre cibersegurança, reconhecendo que as ameaças à cibersegurança são cada vez mais e constituem uma ameaça não só para as economias e a unidade do mercado único digital, mas também para as democracias, liberdades e valores

Pacote Cibersegurança: mandato para a ENISA até 2020 e previsto como permanente, e, criação de matriz de certificação de segurança para produtos TIC (*"the cybersecurity act"*)

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505737096808&uri=CELEX:52017PC0477

Diretiva NIS (*Network and Information System*) criou CSIRT (*Member State Incident Response Teams*), secretariado pela ENISA, que deve ser transposta até maio de 2018

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505328053124&uri=COM:2017:476:FIN

Salienta-se *o European Cyber Security Challenge* (ECSC), uma iniciativa da ENISA que pretende contribuir para melhores níveis de segurança cibernética em toda a Europa, através da simulação de casos e da partilha de experiências (https://www.europeancybersecuritychallenge.eu/index.html)

Comissão Europeia procedeu já em 2018, ao mapeamento dos centros de especialização existentes no campo da cibersegurança na UE. Os resultados deste mapeamento serão traduzidos para o "Atlas da Cibersegurança", um índice dos Centros de Segurança Cibernética existentes da UE que será disponibilizado publicamente

Grupo de trabalho sobre a segurança e privacidade na economia digital

Organização para a Cooperação e Desenvolvimento Económico

Instituição para o desenvolvimento de políticas nacionais coordenadas, equilibrada e pragmática no respeito de diferenças culturais, legais e sociais, focada numa comunidade internacional alargada por mecanismos de cooperação com não-membros e outras organizações internacionais e regionais (como o Conselho da Europa e a APEC - *Asia-Pacific Economic Cooperation*)

Grupo de trabalho sobre a segurança e privacidade na economia digital

- Trabalha a segurança de informação e a privacidade como questões complementares e essenciais à sustentabilidade da economia da Internet como plataforma para a prosperidade social e económica
- Plataforma onde decisores políticos monitorizam tendências, experiências partilhadas e a análise do impacto tecnológico em segurança de informação e elaboração de políticas de privacidade
- Desenvolve e monitoriza a implementação de instrumentos legais não vinculativos (*soft law*) adotados por consenso no Conselho da OCDE
- Mantém uma rede ativa de especialistas governamentais, económicos, da sociedade civil e da comunidade técnica da Internet

Grupo de trabalho sobre a segurança e privacidade na economia digital

Grupo de trabalho sobre a segurança e privacidade na economia digital

- Integrado no do Comité para as Políticas da Economia Digital (CPED) da OCDE, Plataforma em que a segurança e a privacidade são consideradas essenciais para a economia digital continuar enquanto plataforma para a inovação, as novas fontes de crescimento económico e o desenvolvimento social, desenvolve políticas para garantir que a segurança e a privacidade promovem a prosperidade económica e social num mundo digital aberto e interligado

Atividades / lista dos trabalhos referentes à cibersegurança (instrumentos, relatórios e eventos):

https://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm

Going Digital, projeto horizontal, liderado pelo CPED que também incide sobre a segurança:

https://www.oecd.org/going-digital/topics/digital-security-and-privacy/

Grupo de trabalho sobre a segurança e privacidade na economia digital

Conjunto de documentos da OCDE que abordam o tema da cibersegurança:

- *OECD Digital Economy Outlook 2017*: https://www.keepeek.com//Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#page1
- *Managing Digital Security and Privacy Risk 2016 Ministerial Meeting on the Digital Economy*: https://www.keepeek.com//Digital-Asset-Management/oecd/science-and-technology/managing-digital-security-and-privacy-risk_5jlwt49ccklt-en#page1
- *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*: http://dx.doi.org/10.1787/5k8zq92vdgtl-en
- *Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document*: https://www.keepeek.com//Digital-Asset-Management/oecd/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1

(primeiro e ultimo destes títulos também acessíveis em **francês**)

9º Fórum das Comunicações da CPLP

22 de março, 2018

Da Cibersegurança à Ciberoportunidade

arctel CPLP
Associação de Reguladores de Comunicações e Telecomunicações da CPLP

LusNIC

Obrigadu

José Sousa Barros

jose.barros@anacom.pt