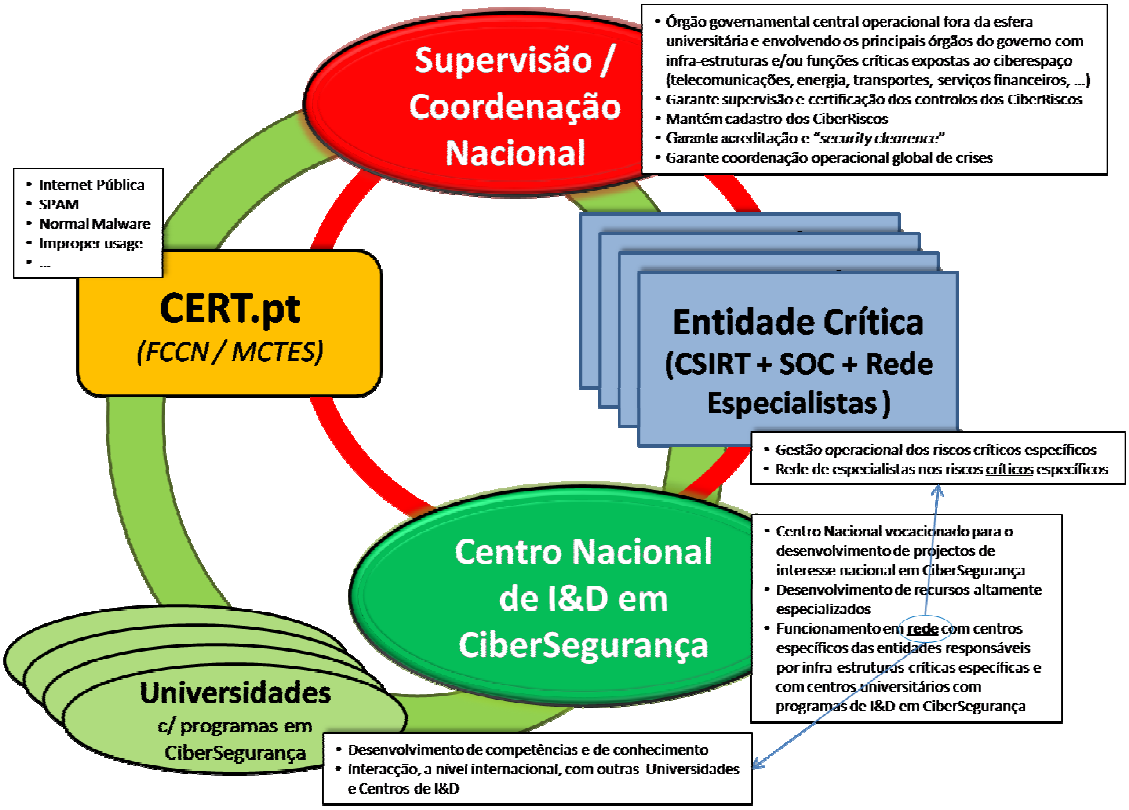
Contribuição para uma *Cibersegurança* mais Eficaz das Infra-estruturas e Serviços Críticos Nacionais

José A. S. Alegria
PT Portugal

Lisboa, 25 de Junho de 2010

Disclaimer: estas sugestões e ideias são do autor e não representam necessariamente a posição oficial da Portugal Telecom

A *cibersegurança* de qualquer nação depende, em grande parte, da capacidade, sofisticação, e interdisciplinaridade da sua rede de centros operacionais e/ou de competência em segurança da informação, redes de telecomunicações e de energia, sistemas distribuídos e de controlo, entre outros, e da eficácia da supervisão e coordenação central desta rede. Estes centros deverão ter responsabilidades operacionais claras, devendo estar associados às entidades directamente responsáveis pela gestão do risco cibernético das principais infra-estruturas e serviços críticos do país.



Centralmente, deverá ser garantido pelo governo um órgão único transversal de supervisão e de coordenação operacional, com competências específicas em CiberRiscos e CiberSegurança, preferencialmente próximo das entidades governamentais que tutelem as organizações responsáveis pelas principais infra-estruturas críticas e/ou funções críticas nacionais (telecomunicações, energia, transportes, sistema financeiro, …) face a CiberRiscos, garantindo a acreditação técnica e "*security clearance*" dos elementos da rede, a existência e manutenção

segura dos cadastros "lógicos" relevantes e CiberRiscos associados e, finalmente, a existência verificável de controlos adequados de gestão de CiberRiscos para cada uma das situações críticas identificadas. Em situações de crise declarada este órgão deverá ter os meios necessários e suficientes para coordenar transversalmente e operacionalmente uma resposta a essa crise requisitando, se necessário, os serviços dos diferentes elementos da rede.

Finalmente, e como forma de estimular o desenvolvimento de conhecimento e competências avançadas em CiberSegurança, é recomendável que um país garanta a existência de pelo menos um centro nacional de I&D na área, com fortes níveis de colaboração com centros universitários nacionais e internacionais e com centros de excelência congéneres em países aliados como o CyLab junto de CMU nos EUA.

A implementação de um órgão central responsável pela supervisão e coordenação da CiberSegurança de todas as infra-estruturas críticas do país deverá ser a 1ª prioridade. Este órgão deverá depois dinamizar a implementação, junto das diferentes entidades responsáveis, dos meios necessários e garantir a sua efectividade e a sua articulação sempre que necessários (crises). Se necessário deverá propor legislação específica.

Como 2ª prioridade, é fundamental que todas as entidades responsáveis por infra-estruturas críticas nacionais garantam, de forma verificável, a CiberSegurança das mesmas e que os meios empregues (especialistas, CSIRT[1] e SOC[2] específicos) pudessem cooperar em rede com os meios similares de outras entidades sempre que a situação o recomende ou quando assim for exigido pelo órgão de supervisão/coordenação nacional. Obviamente que não se exclui o recurso a estratégias de partilha de meios desde que adequadamente geridos e supervisionados. Infelizmente, ainda há entidades com responsabilidades sobre infra-estruturas críticas sem os meios técnicos e humanos, incluindo foco de gestão, adequados à garantia efectiva da sua CiberSegurança. Assim como também ainda não existem os mecanismos adequados de coordenação para facilitar a actuação concertada dos meios existentes nas diferentes entidades já com alguma capacidade em termos de CiberSegurança, face a eventuais incidentes globais de segurança.

Como 3ª prioridade, as universidades portuguesas deverão investir um pouco mais na sua oferta em matéria de formação e investigação em CiberSegurança (nos 3 ciclos de Bolonha). É claro que se a 2ª prioridade se materializar, a procura de especialistas vai aumentar levando a que o aumento de oferta se justifique.

Finalmente, como 4ª prioridade, propomos a implementação em Portugal de um centro do tipo do CyLab (EUA), em afiliação com uma rede de centros universitários e empresariais, e onde seja possível o desenvolvimento de projectos estratégicos de interesse nacional na área da CiberSegurança, especialmente aqueles que sejam transversais a mais do que um tipo de infra-estrutura crítica.

—·—

[1] CSIRT ≡ *Computer Security Incident Response Team*
[2] SOC ≡ Security Operations Center