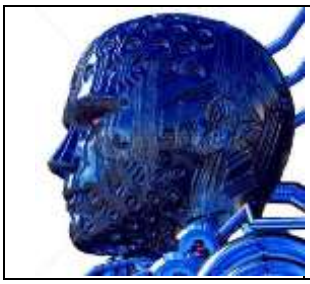

*TRS

Tecnologia, Redes e Sociedade

e-planning | networks | e-learning | **e-government**

Relatório Interno TRS 10/2017

Título
Estratégia Nacional de Segurança do Ciberespaço

Autor(es)
Luis Borges Gouveia, UFP
Raul Carvalho Morgado, UFP

Mês, Ano
Junho, 2017

Local de presença Web *http://tecnologiaredesesociedade.wordpress.com*
Repositório de trabalho científico *trs *http://bdigital.ufp.pt/handle/10284/3787*

Universidade Fernando Pessoa
Praça 9 de Abril, 349
4249-004 Porto, Portugal

Tabela de Conteúdos

Estratégia Nacional de Segurança do Ciberespaço

Luis Borges Gouveia, Raul Carvalho Morgado

Resumo

A aprovação da estratégia nacional de segurança do ciberespaço representa um momento basilar para o esforço e afirmação nacional neste domínio. A estratégia apresenta as orientações a seguir para a proteção do ciberespaço e, simultaneamente, origina um conjunto de responsabilidades, oportunidades e desafios que importa analisar no desenvolvimento deste artigo.

Estas notas foram tomadas a Julho de 2015, um mês após a Resolução do Conselho de Ministros n.º36/2015 que aprova a Estratégia Nacional de Segurança do Ciberespaço, Diário da República, 1ª série - N.º 113 - 12 de junho de 2015.

Palavras-chave: Cibersegurança, ciberespaço, infraestruturas críticas, estratégia nacional de segurança do ciberespaço, Portugal.

1. Introdução

As tecnologias de informação e comunicação (TIC) tiveram um desenvolvimento sem precedentes durante as últimas décadas. Esta evolução teve como consequência, o surgimento de uma dependência crescente do digital. Os principais sistemas, em que cada cidadão, cada empresa, cada instituição, cada Estado, baseiam as suas atividades diárias no uso intensivo de sistemas baseados em computadores e redes. Entre estes sistemas estão os associados às redes de telecomunicações e às redes de energia elétrica que carecem de especial atenção e medidas de segurança e proteção adequadas, na medida em que se constituem como infraestruturas críticas.

A crescente preocupação e a consciência das potenciais consequências de incidentes no ciberespaço nacional impulsionaram a necessidade de compromisso, afirmação e desenvolvimento de capacidades de atuação no novo domínio de interação que é designado por ciberespaço. A Estratégia Nacional de Segurança do Ciberespaço (ENSC) afigura-se como uma orientação holística do Estado que visa difundir a visão global e caminhos a seguir para

garantir a proteção e segurança das infraestruturas tecnológicas nacionais, bem como dos serviços vitais de informação.

O propósito deste artigo é o de contribuir para uma análise crítica da ENSC, identificando sempre que possível desafios e oportunidades provenientes da implementação da estratégia.

2. Síntese da Estratégia Nacional de Segurança do Ciberespaço

Na restrita observância dos princípios gerais da soberania do Estado e de outros diplomas legais, assim como nas orientações da União Europeia para a cibersegurança, o desenvolvimento da ENSC assenta em cinco pilares basilares:

1. Subsidiariedade: a proteção do ciberespaço é responsabilidade primária dos utilizadores que o utilizam e dos proprietários das infraestruturas tecnológicas que compõe este domínio de interação. Compete ao Estado apenas intervir, em última instância, a título subsidiário, auxílio e reforço para garantir a eficácia e as necessidades da segurança do ciberespaço;
2. Complementaridade: todas as partes interessadas no ciberespaço repartem entre si a responsabilidade da segurança deste ambiente. Todos devem contribuir e apoiar-se mutuamente com base nas suas capacidades em prol do bem comum;
3. Cooperação: face à ausência de fronteiras e delimitações no ciberespaço torna-se mais eficaz a sua segurança com a agregação de esforços entre todos os intervenientes nacionais e internacionais reforçadas por uma cultura de confiança global;
4. Proporcionalidade: os recursos e as ações necessárias à segurança do ciberespaço devem ser os apropriados e ajustados face aos riscos identificados para cada situação;
5. Sensibilização: a tomada de consciência por parte dos utilizadores, dos possíveis riscos existentes no ciberespaço, é fundamental para uma melhor avaliação das ações necessárias à sua prevenção e proteção.

Os principais objetivos da ENSC propõe o enquadramento do tema e quadro de operação para assegurar níveis adequados de cibersegurança, tendo em consideração as condições internas e externas do País. O objetivo principal é o desenvolvimento e incremento da segurança das

redes de computadores, da informação e das infraestruturas críticas nacionais. O mapeamento da estratégia resulta em quatro grandes temas:

1. Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;

2. Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;

3. Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;

4. Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

Dos presentes objetivos estratégicos são identificados seis eixos de intervenção que permitem indicar o rumo do caminho a seguir nesta matéria. Cada eixo de intervenção é materializado por um conjunto de medidas a desenvolver e respetivas linhas de ação.

Apresenta-se uma breve síntese das medidas e linhas de ação mais relevantes e pertinentes por cada eixo:

Eixo 1 – Estrutura de segurança do ciberespaço. As principais linhas mestras são:

1. Promover uma liderança e governação forte e transversal através de uma coordenação político-estratégica, com representantes de todas as partes interessadas, na dependência direta do Primeiro-Ministro. Esta coordenação deverá ser responsável pela integração e sincronismo das várias políticas, iniciativas e sensibilidades de todas as partes, bem como pelo controlo e revisão da aplicação da presente estratégia;

2. Impulsionar e consolidar uma coordenação operacional ágil e eficaz através do Centro Nacional de Cibersegurança (CNCS). O CNCS, enquanto coordenador operacional em matéria da cibersegurança, deverá coordenar com as várias entidades responsáveis a execução das medidas previstas na estratégia em análise, desenvolver sinergias com vista à prevenção e resolução de incidentes, disponibilizar informação relativa aos potenciais riscos, ameaças e

vulnerabilidades, bem como criar mecanismos que permitam melhorar a avaliação situacional do ciberespaço nacional;

3. Em matéria de cibersegurança consolidar o papel de autoridade nacional, relativamente às entidades públicas e às infraestruturas críticas nacionais, do CNCS;

4. Desenvolver a capacidade de ciberdefesa, conferindo "ao Centro de Ciberdefesa (CCD) e às capacidades dos ramos das Forças Armadas o planeamento e resposta imediata e efetiva a uma crise no ciberespaço". Cabe, também, às Forças Armadas a responsabilidade de garantir "a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional";

5. Fomentar e incentivar a utilização de capacidades de duplo uso entre os campos de atuação da ciberdefesa e da cibersegurança;

6. Reforçar o papel das comunidades de Computer Security Incident Response Team (CSIRT) no seio da capacidade nacional de resposta a incidentes.

7. Implementar um gabinete para gestão de crises no ciberespaço para resposta a ciberincidentes de grande impacto;

8. Realizar exercícios de gestão de crises no ciberespaço para testar a capacidade de reação e resolução de incidentes;

9. Elaborar propostas de alteração legislativa e regulamentares para a regulação do ciberespaço.

<u>Eixo 2 – Combate ao cibercrime</u>. Neste eixo de intervenção, salienta-se o seguinte:

1. Rever e atualizar todo o quadro legislativo para englobar os crimes relacionados com o ciberespaço;

2. Adequar a Polícia Judiciária com capacidades necessárias ao combate do cibercrime, bem como realizar investigações no ciberespaço

Eixo 3 – Proteção do ciberespaço e das infraestruturas. No que concerne à proteção do ciberespaço e das infraestruturas, salienta-se a adoção das seguintes medidas:

1. Avaliar o estado da arte no que concerne à segurança do ciberespaço e da capacidade de atuação dos organismos que administrem infraestruturas críticas e serviços vitais de informação, bem como prover melhorias contínuas de atuação;

2. Desenvolver a capacidade de deteção de ataques e implementar as contramedidas necessárias de modo a garantir a continuidade normal das operações;

3. Os proprietários de infraestruturas críticas devem incluir medidas de segurança do ciberespaço, baseadas na gestão do risco, nos seus planos de proteção. Devem igualmente, incluir nos seus planos de segurança medidas a adotar suster ameaças oriundas do ciberespaço;

4. Fomentar e incentivar o uso de políticas e normas de segurança para assegurar um elevado nível de proteção;

5. Os operadores de infraestruturas críticas devem constituir um conjunto mínimo de recursos humanos e técnicos adstritos à função da segurança do ciberespaço;

6. Atualizar a legislação nacional para fazer face às evoluções tecnológicas e às boas práticas para a proteção do ciberespaço.

Eixo 4 – Educação, sensibilização e prevenção. As principais medidas de atuação, neste eixo, focam-se nas seguintes linhas de orientação:

1. Iniciativas de sensibilização e promoção de campanhas de informação com vista ao estímulo e desenvolvimento de uma cultura de segurança do ciberespaço entre a população em geral, empresas e operadores públicos e privados;

2. Desenvolver e reforçar as ofertas educativas nos vários níveis de ensino, bem como formação especializada, nos vários domínios do saber da cibersegurança.

Eixo 5 – Investigação e Desenvolvimento. As medidas adotadas para estimular este eixo de intervenção são:

1. Incentivar a investigação científica e a participação nacional em projetos internacionais;
2. Desenvolver e apoiar as capacidades científicas, técnicas, industriais e humanas de modo a assegurar e conservar a independência nacional neste domínio.

Eixo 6 – Cooperação. No que se refere ao eixo da cooperação, realça-se as seguintes medidas:

1. Desenvolver iniciativas de cooperação, colaboração e participação entre os aliados e parceiros nacionais e internacionais, assim como com os CSIRT;
2. Participar nos diversos exercícios para desenvolver e avaliar as capacidades nacionais neste domínio.

3. Análise e discussão

Em primeiro lugar, importa referir que a ENSC, à semelhança das estratégias de outros países, foca as suas orientações numa visão integral e abrangente para lidar com os assuntos no âmbito do ciberespaço. A ENSC estabelece orientações gerais, sem indicar prioridades nem metas palpáveis a alcançar, destacando como áreas de atuação a desenvolver a criação de sinergias e parcerias entre sectores público e privado, a cooperação com instituições internacionais e países aliados, apelando a uma consciencialização nacional para os riscos inerentes à utilização do ciberespaço através da formação. Também refere de forma abstrata a necessidade de estimular e apoiar iniciativas de investigação e desenvolvimento nos assuntos de segurança do ciberespaço.

É fundamental mencionar que a ENSC apresenta uma divisão clara e explicita das responsabilidades em matérias de ciberdefesa, cibercrime e cibersegurança. Assim questões

no âmbito da ciberdefesa são da responsabilidade das Forças Armadas (FFAA); assuntos de cibercrime são responsabilidade da Polícia Judiciária (PJ); e assuntos de cibersegurança referentes às entidades públicas e infraestruturas críticas são da responsabilidade do Centro Nacional de Cibersegurança. Esta divisão, nomeadamente a ciberdefesa e cibercrime, está alinhada com as divisões clássicas de competências dos diversos órgãos centrais públicos do Estado, bem como com os regulamentos e normas legais. Assim e apesar de não ser definido na estratégia, pode-se inferir que as questões de ciberterrorismo são da responsabilidade do Ministério da Administração Interna (MAI) no que concerne às forças de segurança e à PJ na nos assuntos de matéria penal.

Outro aspeto a salientar são as atividades de cariz ofensivo, em que segundo a estratégia compete apenas às Forças Armadas a responsabilidade exclusiva de conduzir operações militares no ciberespaço num cenário de ciberconflito, sejam elas defensivas, ofensivas ou de exploração. É dever, também, das FFAA segundo a ENSC de executar a "resposta imediata e efetiva a uma crise no ciberespaço" e "quando necessário e determinado, a exploração proativa do ciberespaço". A alusão ao exercício de capacidades de caracter mais hostil reserva um desafio enorme às FFAA, mas de especial importância na salvaguarda da liberdade de ação neste espaço cibernético e dos interesses nacionais.

Apesar de abrangente esta estratégia não esclarece de que forma o Estado pensa operacionalizar todo este programa, não existindo orientações específicas/práticas com prazos de execução para poderem ser avaliados no prazo de um ano.

Ao analisar cuidadosamente esta estratégia, verificamos que um dos temas sensíveis que se coloca é, saber como se irá estabelecer as complexas relações entre o sector público e o privado. Os operadores privados são, na sua maioria, os proprietários das infraestruturas críticas do país e o facto de, também, terem a responsabilidade da proteção do ciberespaço, obriga-os a suportar avultados investimentos. Ora, como é que, para além das suas análises de risco e o consequente impacto nos seus negócios, se pode submeter os operadores a investir ainda mais dinheiro nesta área? Será que se consegue concretizar esse desiderato apenas através da produção de regulamentos e de normas ou terá que existir incentivos financeiros? Ainda relacionado com as relações entre os sectores público-privado é

importante interrogar como é que a autoridade nacional, CNCS, apenas com competências de coordenador operacional irá regular o sector privado?

Ao refletirmos sobre outros aspetos relevantes, levantam-se algumas questões pertinentes, de que gostaríamos no futuro ver esclarecidas, tais como:

- Como é que vai ser realizada a verificação anual dos objetivos estratégicos e das linhas de ação? Quem é a entidade responsável por esta verificação?
- Como é que vai ser acompanhado e avaliado o trabalho desenvolvido pelo sector privado, nomeadamente pelas universidades e empresas privadas de TIC? Quem é a entidade responsável?
- Quem financia o trabalho desenvolvido pelos privados? Este trabalho pode ser exportado para outros países? Quem controla essas transações comerciais?
- Relativamente às Universidades, irão ser criados fundos específicos para apoiar projetos nesta área de investigação?
- Que linhas de investigação já existem e/ou se considera serem prioritárias para I&D+i (Investigação, Desenvolvimento e Inovação)?
- Qual a oferta de formação e qualificação existente para a área da cibersegurança no sistema de ensino nacional (empoderamento dos recursos humanos)?
- Dado a ser uma área de extrema complexidade e como o ciberespaço não tem fronteiras definidas, poder-se-ia no futuro pensar-se numa estratégia europeia de cibersegurança, em detrimento de uma estratégia nacional?

Como podemos verificar existe ainda um longo caminho a percorrer com vista ao esclarecimento destas e de outras questões.

4. Comentários finais

Após esta pequena análise da Estratégia Nacional de Segurança do Ciberespaço (Portugal) que se mostra tendencialmente muito genérica, sem prioridades nem metas concretas, mas que, também, acaba por ser correta e harmoniosa, constitui-se como marco fundamental para o futuro da segurança do ciberespaço no contexto nacional. No entanto, é importante referir que ficam muitas questões em aberto que nos devem levar a refletir na tentativa de encontrarmos soluções adequadas para um tema tão atual, de complexa solução e que exige o estabelecimento e desenvolvimento de novas capacidades.

Esta estratégia apesar de ser um bom ponto de partida nesta área tão sensível terá de continuar a ser trabalhada e desenvolvida no âmbito da cibersegurança e ciberdefesa, com o contributo de todas as entidades públicas e privadas, operadores das infraestruturas críticas, empresas das novas tecnologias e estabelecimentos de ensino público e privado, num contexto em rede e de parcerias com troca de informação e conhecimento idêntico ou aproximado dos CERT (centros de respostas a incidentes).

Orientações e esclarecimentos adicionais sobre a operacionalidade de todo este ambicioso programa são essenciais para o seu sucesso. Um plano de implementação precisa-se.

5. Referências

Decreto-Lei n.º 03/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança;

Decreto-Lei n.º 162/2013, de 04 de dezembro, que procede à primeira alteração da orgânica do Gabinete Nacional de Segurança;

Decreto-Lei n.º 69/2014, de 09 de maio, que procede à segunda alteração da orgânica do Gabinete Nacional de Segurança;

Resolução do Conselho de Ministros n.º36/2015 que aprova a Estratégia Nacional de Segurança do Ciberespaço, Diário da República, 1ª série - N.º 113 - 12 de junho de 2015.