A Definição de uma Estratégia Nacional de Cibersegurança

Paulo Fernando Viegas Nunes

Tenente-Coronel de Transmissões. Licenciado em Ciências Militares pela Academia Militar. Mestre e Licenciado em Engenharia Eletrotécnica e de Computadores pelo IST. Doutorado em Ciências da Informação pela Universidade Complutense de Madrid. No âmbito da Presidência Portuguesa da União Europeia (UE), foi Secretário do Helsinki Task Force (HTF). Adjunto para a UE na Representação Militar Permanente de Portugal junto da NATO e da UE (2007-2010). É coordenador científico da Pós-Graduação/Mestrado em Guerra de Informação/Competitive Intelligence da Academia Militar (AM) desde 2002. Membro do Centro de Investigação da AM (CINAMIL) e da Competitive Intelligence Information Warfare Association (CIIWA). Professor convidado na AM, Universidade do Minho, ISCTE e Universidade Lusófona.

Resumo

A necessidade de adaptação permanente das modernas sociedades ao contexto estratégico e às envolventes sociais, económicas e militares em que estas se inserem, tem vindo a colocar novos desafios aos Estados, obrigando, nomeadamente, ao levantamento de novas capacidades, à revisão dos seus modelos de governação e à geração de competências, cada vez mais associadas à exploração das Tecnologias de Informação e Comunicação (TIC), ao acesso à internet e à utilização do ciberespaço.

Portugal tem vindo, essencialmente ao longo do último ano, a desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura deste espaço de interação global. Atendendo à necessidade de desenvolver uma estratégia concertada, integradora e mobilizadora de sinergias nacionais, capaz de reduzir o risco social e potenciar a utilização do ciberespaço, este artigo desenvolve um quadro de análise a partir do qual se procura edificar e propor o levantamento de uma Estratégia Nacional de Cibersegurança.

Abstract

The Definition of a National Cybersecurity Strategy

Modern societies need permanent adaptation to their strategic context, mainly due to a technical, social, economical and military environmental drift, a process that raises new challenges, forcing Nation States to develop new capabilities, revising models of governance and generating competencies more and more associated to the exploitation of Information and Communications Technologies, the internet and cyberspace.

During last year, Portugal started the process of developing a set of initiatives destined to assure a more open, reliable and secure cyberspace. Attending to the need of developing a concerted, integrated and mobilizing strategy, capable of generating national synergies, reducing social risk and potentiating the use of this space of global interaction, this article draws a framework of analysis from which we attempt to build and propose the establishment of a National Cyber Security Strategy.

Introdução

Com a utilização generalizada da internet, surgiram novas formas de comunicação que acabaram por alterar os tradicionais processos de interação social, económica, política e cultural. O ciberespaço, incluindo todas as infraestruturas de informação acessíveis através da internet, construiu um espaço de comunicação à escala global, transcendendo as fronteiras territoriais dos Estados.

A internet tornou-se um importante catalisador do crescimento económico e um recurso fundamental para a nossa sociedade, constituindo hoje uma ferramenta essencial de informação, educação e exercício de cidadania. Abre novas oportunidades de negócio às empresas, através do acesso direto a um número importante de novos clientes e permite estruturar novos caminhos e formas de governação, através da melhoria da eficiência na administração pública e da redução do custo das transações. O ciberespaço favorece assim o crescimento do país, ajudando a desenvolver os serviços públicos e privados de uma forma mais rápida e económica, promovendo o progresso e a prosperidade nacional.

Este espaço virtual, estruturado com base numa rede de redes, serve também de suporte tecnológico a muitos dos serviços críticos e infraestruturas de que milhões de pessoas dependem diariamente. No entanto, a dependência crescente relativamente ao ciberespaço expõe a sociedade a novas vulnerabilidades, aumentando exponencialmente o risco social. Ataques lançados por atores interessados em prejudicar o normal funcionamento das redes e sistemas de informação têm vindo a aumentar em número e em impacto, tornando as ameaças mais sérias e persistentes. Estes ciberataques, devido ao seu poder disruptivo e destrutivo crescente, têm vindo a afirmar-se como uma preocupação estratégica prioritária não só para os Estados mas também para a comunidade internacional.

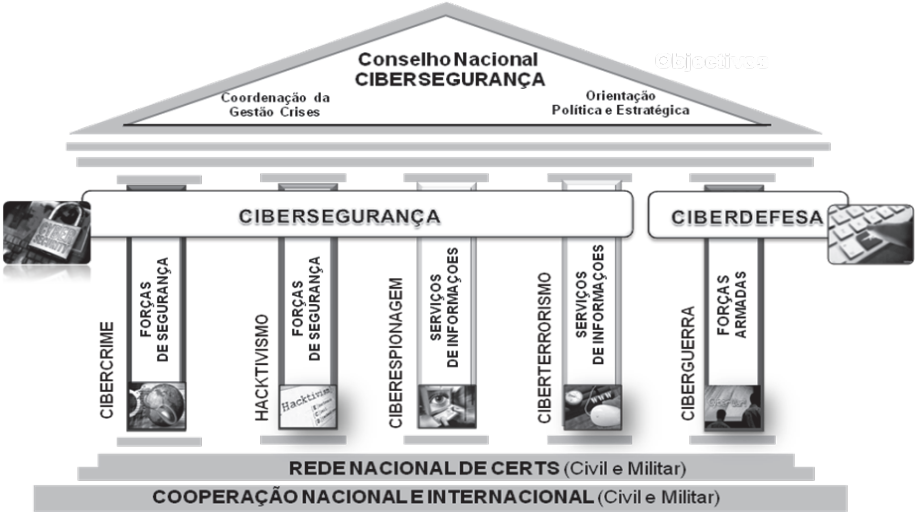
Reconhecendo-se a existência de um nível nacional e supranacional da cibersegurança (figura 1), constata-se que cada Estado terá que garantir não só a utilização segura do ciberespaço aos seus cidadãos mas também a salvaguarda da própria soberania.

Figura 1 – Enquadramento da Cibersegurança Nacional

Neste contexto, importa analisar o risco social e o impacto dos diversos tipos de ciberataques, separando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado. Enquanto o primeiro tipo se enquadra no âmbito da cibersegurança, este último tipo de ataques, enquadra-se no domínio da ciberdefesa.

Enquanto espaço de interação social, o ciberespaço materializa assim uma área de responsabilidade coletiva onde a atribuição de responsabilidades e competências na sua segurança deverá obedecer à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado. Desta forma, considera-se fazer sentido que as Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às atividades relacionadas com o cibercrime e o "hacktivismo", que os Serviços de Informações da República atuem em casos de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham que intervir para fazer face a ações de ciberguerra. Neste contexto, conforme se demonstra na figura 2, considera-se necessário prever a existência de um órgão coordenador das áreas ligadas à cibersegurança e ciberdefesa do Estado (Conselho Nacional de Cibersegurança), facilitando a definição não só de uma orientação política e estratégica mais coordenada e sinérgica como também uma gestão de crises mais eficaz.

Figura 2 – Cibersegurança Nacional (um edifício, vários pilares)



Apesar de se reconhecer atualmente a dificuldade do legislador acompanhar a dinâmica registada em muitos dos domínios de exploração do ciberespaço, este tipo de abordagem permitirá colmatar a existência de hiatos legais decorrentes, em muitos casos, da inexistência de legislação específica. Com esta aproximação, onde se mantém a mesma lógica de atuação e o suporte legal para a intervenção dos diversos atores responsáveis pela Segurança e Defesa do Estado, tanto no "mundo real" como no ciberespaço, considera-se ser possível evitar muitos dos problemas que estão na base de uma aparente paralisia nacional e internacional, por vezes justificada pela "falta de mandato institucional".

Garantir a segurança do ciberespaço (cibersegurança) constitui hoje um imperativo nacional, essencial para garantir a soberania e a sobrevivência do país. Se Portugal pretender ocupar um lugar no grupo das "Sociedades de Informação"[1], torna-se necessário garantir a segurança e a defesa da Infraestrutura de Informa-

1 De acordo com os objetivos traçados na Estratégia de Lisboa, vertidos no Programa Operacional para a Sociedade de Informação e posteriormente reforçados no âmbito do Plano Tecnológico. Neste âmbito, importa também assinalar a importância do "Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Pública" (Horizonte 2012-2016), recentemente aprovado pela Resolução do Conselho de Ministros Nº12/2012. Este Plano, estabelece princípios de governação na área das TIC orientados por uma visão de serviço público de qualidade mais racional e eficiente, identificando a necessidade de rever e desenvolver uma Estrutura Nacional de Segurança da Informação (ENSI) e prevendo o levantamento de um Centro Nacional de Cibersegurança.

ção Nacional (IIN), encarando esta necessidade como um processo contínuo e sistémico de análise e gestão do risco social. Nesse sentido, importa refletir sobre as vulnerabilidades estratégicas e o espectro da ameaça no ciberespaço, uma vez que estes aspetos devem ser tidos em conta na definição de uma Estratégia Nacional de Cibersegurança.

Vulnerabilidade Estratégica e Ameaças no Ciberespaço

Face à existência de redes de comunicações transnacionais, os Estados são confrontados com um ambiente de informação global, onde não é possível definir de forma clara o que representa a IIN. O ciberespaço, devido à sua natureza virtual, não é gerido nem é propriedade dos governos, mas de todos os utilizadores de uma sociedade de informação global. Devido ao rápido desenvolvimento das TIC, o ciberespaço encontra-se em permanente evolução e modificação. Por essa razão, os instrumentos clássicos de regulação e soberania, postos em prática pelos Estados para reduzir os riscos emergentes do ciberespaço, são difíceis de implementar.

Quando se analisam as ameaças decorrentes da possibilidade de atores hostis explorarem as vulnerabilidades das infraestruturas de informação de um país, temos que avaliar as suas intenções e capacidades para infligir danos a essas infraestruturas, de forma a definir o nível da ameaça a enfrentar. As ameaças podem materializar-se através de ações conduzidas por indivíduos isolados (amadores, *hackers* ou *crakers*), por grupos organizados (criminosos, grupos de pressão social ou terroristas) ou mesmo por Estados (ciberguerra).

Os ataques que têm por base as TIC são extremamente fáceis de realizar. Os meios são relativamente baratos, fáceis de contrabandear, praticamente indetetáveis e difíceis de correlacionar. A consciência de que um ator individual, dotado de um computador e das necessárias competências técnicas, pode tornar inoperacionais as infraestruturas críticas dos países mais desenvolvidos do mundo, tem vindo a suscitar uma profunda reflexão tanto no âmbito nacional como internacional. Exemplos recentes como os ciberataques lançados contra a Estónia (abril/maio de 2007) e contra a Geórgia (agosto de 2008), vieram provar a necessidade de salvaguardar o fluxo de informação vital entre as estruturas governamentais e os diversos órgãos/setores considerados críticos para a sobrevivência do Estado.

Um número crescente de computadores é todos os dias objeto de intrusões sendo a sua integridade comprometida por *hackers*. Dados sensíveis são roubados de redes e sistemas informáticos de empresas privadas e do governo. O ciberespaço é utilizado pelo crime organizado de forma ilícita para realizar fraudes e para extorsão. Ciberataques têm também vindo a ser utilizados para espionagem e para o exercício de coação política contra Estados, como componente integrante de cam-

panhas militares ou como ferramentas para desativar infraestruturas industriais. Tais ataques podem afetar a relação entre os Estados, podendo tornar-se uma arma nas mãos de terroristas. Os diversos tipos de ataque e a indisponibilidade do ciberespaço têm assim um importante impacto estratégico ao nível social, económico, político e militar.

A necessidade urgente de levantar mecanismos de proteção e defesa, destinados a garantir a livre utilização da internet e do ciberespaço têm conduzido os Estados ao aprofundamento de uma cultura de cibersegurança e à tomada de consciência coletiva, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético. Assim, iniciativas recentes de âmbito nacional e internacional (ONU, NATO, UE, OSCE e G8) têm vindo a propor acordos de cooperação e dispositivos legais que definem normas e princípios destinados a garantir uma internet sustentável e um comportamento aceitável no ciberespaço.

Estratégia Nacional de Cibersegurança

Enquadramento e Definição

Dentro da lógica da defesa dos seus interesses, é de esperar que atores mal-intencionados procurem manipular e controlar os fluxos de informação que circulam nas redes de comunicações dos diversos países, afetando a disponibilidade e a utilização segura do ciberespaço. Quando estão em risco a segurança e o bem-estar social, o Estado terá que desenvolver uma "Política para o Domínio da Informação" que permita garantir, não só a convergência estrutural para os parâmetros tecnológicos da Sociedade de Informação e do Conhecimento, como também a Segurança e a Defesa da sua Infraestrutura de Informação.

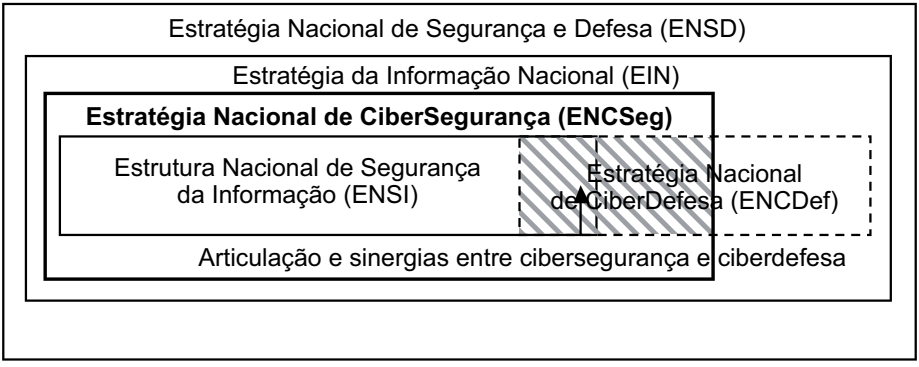
Atendendo ao princípio de que a cada forma de coação corresponde uma estratégia distinta (Couto, 1988: 227), a utilização da informação e do ciberespaço como forma de coação faz surgir uma nova estratégia, a Estratégia da Informação Nacional (EIN). Assim, como uma das componentes desta Estratégia e subordinada à Estratégia de Segurança e Defesa do Estado (ENSD), surge a Estratégia Nacional de Cibersegurança (ENCSeg).

Constituindo o ciberespaço uma das componentes do ambiente da informação, a Estrutura Nacional de Segurança da Informação[2] (ENSI), deve ser perspetivada

2 Atualmente em revisão, no âmbito da medida 4 da Resolução do Conselho de Ministros N.º 12/2012.

no âmbito da ENCSeg (ver figura 3). Por outro lado, importa também referir que, assim como existe uma estreita ligação entre a Segurança e a Defesa Nacional, também a cibersegurança se revela indissociável da ciberdefesa do Estado. Na prática, isto significa que não será possível garantir a cibersegurança sem o levantamento de uma capacidade de ciberdefesa.

Figura 3 – Enquadramento da Estratégia Nacional de Cibersegurança



Neste contexto, a Estratégia Nacional de Cibersegurança (ENCSeg), pode ser definida como o conjunto integrado de iniciativas (de natureza orgânica, operacional e genética), destinadas a potenciar a livre utilização do ciberespaço e garantir a sua segurança, promovendo a proteção da Infraestrutura de Informação Crítica Nacional contra eventuais ciberataques, de âmbito nacional ou internacional que, pelo seu caracter disruptivo, afetem a sociedade portuguesa e a defesa dos Interesses Nacionais.

Devido ao enquadramento apresentado, constata-se que a ENCSeg deverá contribuir tanto para a implementação dos processos de Segurança da Informação associados ao ciberespaço como, de forma articulada e sinérgica, para o levantamento dos mecanismos de ciberdefesa (zona sombreada da figura 3) que são necessários mobilizar para garantir a própria cibersegurança do país e a salvaguarda dos interesses nacionais. A ENCSeg encontra-se assim alinhada não só com a EIN mas também com a própria ENSD.

Neste contexto, parece claro que os benefícios decorrentes da livre utilização do ciberespaço só serão atingidos se formos capazes de proteger e defender as infraestruturas de informação nacionais, garantindo um nível aceitável e sustentável de segurança, fiabilidade e disponibilidade na sua exploração.

Finalidade

O enquadramento e a definição da ENCSeg constituem os fundamentos da visão estratégica que se pretende estruturar neste domínio. No entanto, a clarificação da sua finalidade revela-se também um elemento fundamental para podermos deduzir os objetivos a atingir e, a partir daí, perspetivar as linhas de ação estratégica que vão orientar a sua implementação.

A finalidade a atingir pela ENCSeg, conforme foi possível constatar (figura 3), decorre do nível de ambição e da finalidade que for definida para a EIN e para a ENSI. Com base neste pressuposto, procuraremos estabelecer o âmbito e os princípios que caracterizam a EIN, de forma a permitir e posteriormente determinar a finalidade a atingir pela ENCSeg.

A Estratégia da Informação tem como âmbito a infoconflitualidade resultante das relações de competição e conflito geradas entre a infoesfera do país, definida com base nos interesses nacionais, e a infoesfera de outros atores (Estado ou não-Estado). Atendendo ao âmbito da EIN (Nunes, 2011), considera-se que esta pode apresentar três finalidades principais: garantia da Informação (*Information Assurance*)[3], superioridade da informação (*Information Superiority*)[4] e domínio da informação (*Information Dominance*)[5].

Tendo por base as capacidades nacionais (Nunes, 2011), consideramos que Portugal deve orientar a sua Estratégia da Informação de acordo com a prioridade de satisfação da primeira finalidade apresentada (curto prazo) e perspetivar a segunda (médio/longo prazo). Não se considera como objetivo realista o levantamento das capacidades necessárias à consecução da terceira finalidade (Domínio da Informação).

A Estratégia da Informação torna-se assim indispensável em todos os domínios da conflitualidade refletindo-se, ao nível da globalização da economia e das transações digitais (Estratégia Económica), nas redes de influência social e diplomática, criadas com base na internet (Estratégia Política), na influência dos média e do

3 Neste âmbito, o principal desafio que os Estados e a generalidade das organizações têm que enfrentar é a proteção da sua infraestrutura de informação. Este desiderato requer tanto a implementação de mecanismos de Segurança como de Defesa da IIN.

4 Uma vez garantida a disponibilidade e a integridade dos sistemas de informação de um Estado, uma opção futura que se coloca é a expansão da sua infoesfera de influência em direção a outros ambientes mais alargados, dentro dos quais a organização ou o Estado pretende intervir.

5 Após estabelecido um certo grau de superioridade no ambiente de informação, um ator estará em posição para lançar uma campanha orientada para a obtenção de uma vantagem operacional, se assim o desejar. A condução com sucesso desta campanha requer o domínio do ambiente de informação adversário por aqueles que necessitem dessa informação.

ciberespaço na gestão das perceções (Estratégia Psicológica) e na utilização dos sistemas de armas (Estratégia Militar).

Assumindo-se a garantia da informação como a finalidade primária da EIN, considera-se que a Estratégia Nacional de Cibersegurança, face à necessidade de articulação e integração permanente que tem de existir entre a cibersegurança e a ciberdefesa, deverá apresentar a mesma finalidade. Neste contexto, importa também referir que a NATO, na definição da sua Política de Ciberdefesa (CM, 2011), também elegeu a garantia da informação como objetivo final a atingir[6].

Tendo sido definida a finalidade da ENCSeg, importa agora clarificar os objetivos a atingir e as linhas de orientação geral e específica que a estes se encontram associadas, de forma a traduzir a visão numa ação estratégia coerente e eficaz.

Objetivos a Atingir e Linhas de Orientação

O ciberespaço, enquanto espaço de defesa de interesses, impõe novas formas de interação e de relacionamento onde as estratégias prosseguidas se centram no valor dos recursos de informação e em atividades destinadas a afetar esse valor. Neste domínio, onde se geram novas oportunidades mas também surgem novos riscos, Portugal deverá procurar atingir os seguintes três objetivos principais:

- Garantir a segurança do ciberespaço (proteger valor), assegurando a disponibilidade, integridade, autenticidade e confidencialidade da informação que serve de base ao governo e aos órgãos de soberania (responsáveis políticos e militares) para tomarem decisões e desenvolverem a sua ação;
- Melhorar a eficiência com que o país utiliza a informação (gerar valor), explorando para esse efeito as redes e os sistemas de informação que tem disponíveis;
- Explorar com eficácia o ciberespaço (afirmar e defender valor), de forma a salvaguardar a defesa dos interesses nacionais e afirmar a soberania nacional neste domínio.

Relativamente ao primeiro objetivo, considera-se que a Segurança da Informação Nacional constitui um pré-requisito para a livre utilização do ambiente da informação e que esta só pode ser garantida através de um conceito alargado de proteção das infraestruturas de informação nacionais, onde a articulação e a exploração de sinergias entre a cibersegurança e a ciberdefesa é decisiva para garantir essa proteção. Torna-se assim evidente a necessidade do país dispor de mecanis-

6 De acordo com a Política de Ciberdefesa da NATO (CM, 2011), a cibersegurança só poderá ser conseguida com base na implementação de mecanismos de Segurança da Informação (INFOSEC) e da sua integração e articulação sinérgica com uma capacidade de ciberdefesa.

mos de segurança e defesa do ciberespaço, implementando para esse efeito um Sistema de Proteção da Infraestrutura de Informação Crítica Nacional (SPIICN).

Considera-se que a filosofia a seguir, na implementação do SPIICN, se deverá articular de acordo com uma perspetiva de gestão do risco: proteção, deteção e reação. Reconhecendo-se que se trata de garantir o funcionamento ininterrupto (*Business Continuity*) e a recuperação (*Disaster Recovery*) das Infraestruturas Críticas Nacionais face à ocorrência de ciberataques, importa também perceber que o Estado só será capaz de atingir este objetivo se tiver capacidade para deter e se defender contra este tipo de ataques, nomeadamente, face àqueles que coloquem em risco a Soberania Nacional. A proteção, deteção e reação têm a ver essencialmente com a área da cibersegurança ao passo que o deter e o defender se encontram mais ligadas à ciberdefesa.

O segundo objetivo pretende essencialmente melhorar a estrutura de enquadramento e as infraestruturas tecnológicas nacionais com o objetivo de, a partir delas, gerar e incorporar mais valor e aumentar a competitividade do país. Consubstancia-se através do desenvolvimento de iniciativas destinadas a melhorar a qualidade dos equipamentos, das infraestruturas e dos processos associados à utilização da informação.

A exploração eficaz do ciberespaço, enunciada no terceiro objetivo, pressupõe uma clara definição dos objetivos operacionais a atingir e a capacidade nacional para moldar o ambiente de informação, de acordo com os interesses nacionais a defender. Tal desiderato só se consegue através do desenvolvimento de Operações de Informação (incluindo Operações em Redes de Computadores), potenciando os "pontos fortes" na exploração de oportunidades e reduzindo ao máximo o impacto de eventuais ataques que pretendam explorar os "pontos fracos" e as vulnerabilidades nacionais neste domínio.

A visão clara das implicações/necessidades associadas a cada um dos objetivos enunciados, conforme se ilustra na tabela em anexo, permitirá traçar o caminho a seguir, perspetivando uma orientação geral e específica para os atingir.

Linhas de Ação Estratégica

No âmbito da ENCSeg, para além de objetivos concretos a atingir e das orientações (gerais e específicas) a seguir para a sua implementação, importa também definir linhas de ação concretas, destinadas a reforçar o potencial estratégico nacional neste setor. Cada uma destas linhas de ação interliga-se necessariamente com as restantes, reforçando a capacidade do país para garantir uma utilização mais livre, segura e eficiente do ciberespaço.

Neste contexto, identificam-se as seguintes linhas de ação estratégica destina-

das a garantir a liberdade de ação no ambiente da informação e a vencer os desafios colocados pela utilização segura do ciberespaço:

- Garantir a proteção das Infraestruturas de Informação Críticas, nomeadamente, através da criação do SPIICN, levantando desta forma uma organização/estrutura que implemente os mecanismos de proteção e segurança dessas infraestruturas e permita garantir a sua defesa;
- Melhorar a Segurança das TIC nacionais, desenvolvendo parcerias público-privadas destinadas a reforçar a "soberania" e a "diversidade tecnológica", ações de sensibilização e de formação especializada, promovendo a adoção generalizada de normas de segurança da informação que tenham em conta os aspetos sociais e económicos;
- Reforçar a Segurança das TIC nas redes do governo e da administração pública, definindo uma infraestrutura crítica mínima a proteger prioritariamente, estabelecendo mecanismos de resposta a incidentes coordenados por um Centro Nacional de Cibersegurança (CNC), criando planos de recuperação e continuidade da atividade específicos, desenvolvendo ferramentas de segurança básica certificadas (ex: assinatura digital e criptografia), definindo códigos de boas práticas, políticas e normas de segurança da informação mais exigentes que permitam auditar as TIC a incorporar nas redes do governo e da administração pública do Estado;
- Controlar de forma eficaz a cibercriminalidade revendo o quadro legal e a moldura penal ligada a este tipo de crimes e reforçando as capacidades dos órgãos de investigação criminal, das forças de segurança e dos serviços de informações da república, no combate a todas as formas de cibercrime, tendo em especial atenção as ações associadas a atividades de espionagem e sabotagem cibernética;
- Rever e desenvolver o quadro legal, adaptando o ordenamento jurídico nacional de forma a facilitar o combate à cibercriminalidade, dando suporte legal à atuação das várias entidades que participam na cibersegurança e ciberdefesa do Estado. Neste âmbito, importa promover uma harmonização global da lei criminal baseada na Convenção Europeia do Cibercrime e de outras convenções internacionais que venham a ser ratificadas neste domínio;
- Levantar o Conselho Nacional de Cibersegurança e Ciberdefesa, como estrutura responsável pela orientação político-estratégica e pela gestão de crises no ciberespaço, garantindo a coordenação de topo do combate a todas as formas de cibercrime, ciberterrorismo, ciberespionagem e ciberguerra, respeitando a especificidade (civil/judicial/policial/militar) das atividades a desenvolver e promovendo ao mesmo tempo a sua integração, de forma a fomentar sinergias e potenciar a sua utilização operacional em proveito do SPIICN e do Estado;

- Levantar a estrutura responsável pela cibersegurança do Estado, nomeadamente, através da criação de um Conselho Nacional e de um Centro Nacional de Cibersegurança que, através do SPIICN, garantam a segurança do ciberespaço nacional.
- Levantar a capacidade de Ciberdefesa Nacional, que, em articulação com o SPIICN e a estrutura de cibersegurança permita assegurar a defesa do Estado contra ciberataques que, pela sua natureza e potencial disruptivo e destrutivo, coloquem em risco a soberania nacional ou sejam lançados por outros Estados;
- Desenvolver e reforçar iniciativas nacionais estruturantes da "Sociedade de Informação", como o Plano Tecnológico, POSI, POSC, EGOV, INFOCID, SIMPLEX, difusão da banda larga, "Empresa na Hora" e "e-Escolas";
- Desenvolver ações de sensibilização e formação especializada, para edificar uma cultura de cibersegurança e garantir a existência de especialistas nacionais neste domínio;
- Potenciar a inovação e as atividades de I&D de âmbito nacional e internacional, nomeadamente, das associadas ao desenvolvimento de TIC mais fiáveis, confiáveis e seguras;
- Reforçar e potenciar a cooperação internacional, aprofundando o relacionamento e estabelecendo parcerias e acordos de cooperação bilateral e multilateral (NATO, UE, OSCE e ONU) no âmbito da cibersegurança e ciberdefesa do Estado;
- De forma transversal, as atividades desenvolvidas no âmbito da implementação da Estratégia Nacional de Cibersegurança, contribuirão para a consolidação do vetor estratégico "Informação e Segurança do Ciberespaço", influenciando também todos os outros vetores que contribuem para a Estratégia Nacional de Segurança e Defesa.

Conclusões

O ciberespaço impõe novas formas de interação e de relacionamento, colocando o país na vanguarda da revolução digital. A definição de uma agenda digital permite disponibilizar benefícios económicos e sociais sustentáveis, estimular a criação de empregos, a sustentabilidade e inclusão social, extrair o máximo benefício das novas tecnologias digitais e melhorar a estrutura de enquadramento nacional.

Existe um consenso generalizado, tanto no plano nacional como internacional, que a sobrevivência das modernas sociedades depende cada vez mais de uma utilização mais segura e fiável do ciberespaço. A dependência crescente relativamente

ao ciberespaço, de todos os domínios da vida e interação social, conduz ao surgimento de vulnerabilidades que têm de ser cuidadosamente analisadas e, se possível, solucionadas ou reduzidas.

O ciberespaço não é limitado pela esfera pública ou privada, interna ou externa. As ameaças podem surgir de qualquer local e ter efeitos assimétricos e fortemente disruptivos. Métodos de ataque semelhantes podem ser utilizados para atingir indivíduos, empresas ou Estados. O inegável valor associado à livre utilização da internet pode assim ser seriamente comprometido por uma vaga crescente de ciberataques, minando a confiança na segurança global do ciberespaço.

A perceção de que os processos e mecanismos de cibersegurança existentes dificilmente acompanham a dinâmica das vulnerabilidades, levanta a necessidade urgente de uma forte sensibilização nacional para a importância de prevenir e responder à ocorrência de disrupções e ataques, garantindo assim a proteção e defesa das infraestruturas críticas e recursos de informação nacionais.

Para Portugal, um ciberespaço fiável e confiável constitui um domínio estratégico prioritário, de defesa de valores e interesses nacionais. Os desafios que o ciberespaço apresenta aos Estados, no seu conjunto e no âmbito social próprio, não podem ser ignorados ou negligenciados. A defesa dos interesses nacionais neste espaço de interação global, não se poderá focalizar apenas numa visão securitária da informação, sob pena de se promover uma visão exclusivamente reativa. Antes se deverá potenciar uma atitude proactiva que, garantindo uma utilização mais segura do ciberespaço desenvolva também a capacidade para explorar e moldar o ambiente de informação de forma a favorecer a salvaguarda dos interesses nacionais.

A construção de um futuro digital para Portugal, seguro e sustentável, passa assim por um desafio coletivo e por uma partilha de responsabilidades que envolva, numa visão conjunta, o governo, a administração pública, forças armadas e de segurança, empresas e cidadãos. O desenvolvimento de uma Estratégia Nacional para o Ciberespaço permitirá potenciar o impacto das iniciativas governamentais já em curso, fornecendo-lhes uma visão e um enquadramento integrador, que facilita a implementação e reforça o seu impacto, num contexto onde o desenvolvimento de sinergias nacionais e de parcerias internacionais desempenha um papel central.

Neste contexto, não será possível ignorar a necessidade de uma Estratégia Nacional de Cibersegurança enquadrada e integrada numa Estratégia da Informação Nacional, sob pena de, no quadro das relações internacionais, Portugal correr o risco de ser remetido para um papel de mero executante das estratégias ditadas pelas nações líderes neste domínio ou, no quadro de um empenhamento bilateral ou nacional, das organizações que desenvolvem ciberataques e atividades mal-intencionadas no domínio da informação.

Bibliografia

Couto, Cabral (1988). *Elementos de Estratégia*, Volume I. Lisboa: IAEM.

CM (2011). CM0042-*NATO Policy On Cyber Defence And Cyber Defence Action Plan*, 7 de Junho.

Francart, Loup (2000). *La Maitrise de l'Information*. Disponível em www.Infoguerre.com, acedido em 23-09-2003.

GPTIC (2011). *Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Pública*. Grupo de Projeto para as TIC (GPTIC), 15 de dezembro.

JP 3-13 (1998). *Joint Doctrine for Information Operations Publication*. Joint Chiefs of Staff, Joint Electronic Library. Disponível em http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf**,** acedido 25-09-2009.

Nunes, Paulo (2011). "Mundos Virtuais, Riscos Reais: Fundamentos para a Definição da Estratégia da Informação Nacional". *Atas I Congresso Nacional Segurança e Defesa*, dezembro 2010.

RCM 12/12 (2012). *Resolução Conselho de Ministros N.º 12 de 2012*, DR, 1.ª Série – N. 27, 7 de fevereiro.

Anexo A – Estratégia Nacional de Cibersegurança: da Visão à Ação

Estratégia Nacional de Cibersegurança (definição)	Finalidade Primária	Objetivos	Orientação Geral	Orientação Específica	Linhas de Ação Estratégica
Conjunto de iniciativas (de natureza orgânica, operacional e genética), destinadas a potenciar a livre utilização do ciberespaço e garantir a sua segurança, promovendo a proteção da Infraestrutura de Informação Crítica Nacional contra eventuais ciberataques, de âmbito nacional ou internacional que, pelo seu caracter disruptivo, afetem a sociedade portuguesa e a defesa dos interesses nacionais.	**Garantia da Informação** O principal desafio que o Estado tem que enfrentar e o de estimular uma utilização segura e eficiente do ciberespaço por parte de todos os cidadãos, ao mesmo tempo que garante a proteção e defesa da sua infraestrutura de informação crítica. Este desiderato requer tanto a implementação de processos de Segurança da Informação como de mecanismos de Ciberdefesa.	Garantir a Segurança do Ciberespaço ***(proteger valor)***	Desenvolver mecanismos de proteção, deteção, reação e defesa contra ciberataques; Criar um Sistema de Proteção da Infraestrutura de Informação Crítica Nacional (SPIICN); Assegurar a coordenação operacional com a Estrutura Nacional de Segurança da Informação; Definir uma Estratégia Nacional de Ciberdefesa;	Avaliar o risco social no ciberespaço, identificando as vulnerabilidades das Infraestruturas de Informação Críticas, os recursos da IIN que podem ser atacados e os condicionamentos impostos pelo espectro da ameaça; Implementar, com base na rede de CSIRTs nacional, um sistema de alerta e registo de incidentes que permita proteger, detetar e reagir face a ataques conduzidos contra a IIN; Criar mecanismos necessários para combater o cibercrime e assegurar a proteção e defesa da IINcontra os diversos tipos de ameaças; Desenvolver uma estrutura responsável pela cibersegurança do Estado, com base num Conselho Nacional e num Centro de Cibersegurança (CERT Nacional); Rever e desenvolver o quadro legal de forma a clarificar o papel dos diferentes atores que intervêm na segurança e na ciberdefesa do país; Melhorar a segurança das TIC nas redes nacionais, nomeadamente, através da implementação de um Sistema de Certificação Eletrónica do Estado e de um Sistema de Criptografia Nacional certificado; Sensibilizar os cidadãos para a utilização mais segura das TIC e garantir a formação de especialistas vocacionados para a segurança da informação e ciberdefesa do Estado; Estabelecer parcerias e aprofundar a cooperação internacional (UE, NATO, OSCE e ONU) no âmbito da cibersegurança e ciberdefesa do Estado.	Garantir a proteção das Infraestruturas de Informação Críticas; Melhorar a segurança das TIC Nacionais; Reforçar a segurança das TIC nas redes do governo e da administração pública; Rever e desenvolver o quadro legal; Controlar de forma eficaz a cibercriminalidade; Criar a estrutura responsável pela cibersegurança do Estado; Desenvolver ações de sensibilização e formação especializada; Reforçar e potenciar a cooperação internacional.
		Melhorar a eficiência de utilização do ciberespaço ***(gerar valor)***	Assegurar a integração do país na "Sociedade de Informação e do Conhecimento"; Potenciar a capacidade competitiva do país no contexto de uma economia digital.	Garantir a convergência nacional para a "Estratégia de Lisboa"; Desenvolver iniciativas de I&D, estruturantes da "Sociedade de Informação"; Vencer dificuldades estruturais e melhorar a estrutura de enquadramento nacional com base na utilização das TIC.	Reforçar iniciativas nacionais estruturantes da "Sociedade de Informação e do Conhecimento"; Potenciar a inovação e as atividades de I&D de âmbito nacional e internacional; Reforçar formação especializada e potenciar utilização das TIC.
		Garantir a liberdade de ação no ciberespaço ***(afirmar e defender a***	Assegurar o combate a todas as formas de cibercrime, ciberterrorismo, ciberespionagem e ciberguerra.	Definir os condicionamentos impostos pelo espectro da ameaça e as possíveis respostas a adotar, criando regras de empenhamento tanto ao nível nacional como internacional; Definir mecanismos de coordenação nacional de topo (civil/judicial/policial/militar) para a exploração de sinergias no âmbito do combate ao cibercrime, ciberterrorismo,	Criar o Conselho Nacional de Cibersegurança e Ciberdefesa; Criar um Centro Nacional de Cibersegurança; Criar um Centro Nacional de Ciberdefesa;