PROTECÇÃO DO CIBERESPAÇO: VISÃO ANALÍTICA

Lino Santos[1] *,Rogério Bravo*[2] *e Paulo Viegas Nunes*[3]

[1] CERT.PT, Fundação para a Computação Científica Nacional,
Lisboa, Portugal
lino@fccn.pt

[2] Polícia Judiciária
Lisboa, Portugal
r.bravo@pj.pt

[3] CINAMIL, Centro de Investigação da Academia Militar,
CIIWA, Competitive Intelligence and Information Warfare Association,
Lisboa, Portugal
nunes.pfv@mail.exercito.pt

Resumo

Vários factores têm contribuído para destacar na agenda política dos Estados a protecção do ciberespaço. Por um lado assistimos a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em praticamente todas as funções vitais do funcionamento de infra-estruturas críticas nacionais. Por outro, este "mundo em rede" desenvolveu um novo plano de condução de conflitos com características únicas, que obriga a uma redefinição das políticas de segurança e de defesa nacionais.

Para a redefinição destas políticas devem contribuir, de forma inclusiva, o conjunto de domínios de actuação que contribuem para a Segurança e Defesa Nacional, designadamente o da protecção simples, o da prossecução criminal e o da defesa do Estado e condução da guerra. Não sendo totalmente disjuntos, estes domínios apresentam diferenças relevantes nos respectivos objectivos, nos seus principais actores, nos meios técnicos disponíveis e no enquadramento jurídico aplicável.

O presente artigo tem como objectivo analisar os diferentes domínios de actuação associados à Segurança e Defesa, a sua adequação ao contexto do ciberespaço e dos novos tipos de ciberconflitualidade, bem como a necessidade de garantir uma estreita articulação entre eles.

1 Introdução

Durante a última década, o ciberespaço e os seus componentes tornaram-se numa infra-estrutura essencial de suporte à comunicação, à realização de transacções financeiras e comerciais e até à prestação de serviços públicos ao cidadão. Neste contexto que vulgarmente designamos de sociedade da informação, as interacções entre indivíduos, empresas e Estado são, cada vez mais, realizadas com recurso às Tecnologias da Informação e da Comunicação (TIC) designadamente o computador, o telemóvel e a Internet.

Os ataques informáticos de que a Estónia e a Geórgia foram alvo, em 2007 e 2008 respectivamente, vieram alertar as autoridades nacionais e internacionais para uma nova realidade. Se há muito se escrevia, quer sobre a utilização das tecnologias no contexto de ciberconflitos de cariz assimétrico – tais como o cibercrime organizado, o hacktivismo ou a ciberguerra –, quer sobre os possíveis efeitos destes nas sociedades mais dependentes das TIC, estes dois eventos mostraram ser urgente a definição de uma nova agenda global nesta área.

Tendo por base a sistematização realizada por Pedahzur (2009) relativamente ao contra-terrorismo, sugerimos, salvaguardadando as diferenças entre este fenómeno e os ciberataques (não obstante estes poderem constituir um instrumento daquele), a existência de três domínios de actuação[1] face a estes últimos, designadamente o domínio da protecção simples, o domínio da prossecução criminal e o domínio da defesa do Estado.

A cada um destes domínios corresponde uma perspectiva relativamente aos ciberataques, a qual determina diferenças relevantes no que respeita aos objectivos a atingir, aos principais actores envolvidos, aos meios técnicos disponíveis e ao enquadramento jurídico aplicável (ver Tabela 1). Vistos a partir da perspectiva da defesa do Estado os ciberataques são entendidos como actos de guerra, pelo que a resposta se centra na acção militar, com todos os recursos disponíveis, apenas sujeita na acção, no plano nacional à Constituição da República, à Lei do estado de Sítio e do estado de Guerra e, no plano internacional, ao Direito Internacional dos Conflitos Armados[2] e ao

[1] O conceito "domínio de actuação" aqui usado refere-se ao conjunto dos meios técnicos e humanos (actores), bem como do enquadramento legal, envolvidos na prossecução de um conjunto de objectivos, os quais são em parte determinados por uma perspectiva relativamente ao fenómeno da ciberconflitualidade.

[2] O Direito Internacional dos Conflitos Armados é composto pelas Convenções de Genebra de 1948 e Protocolos adicionais. Estas sujeitam a acção militar a um conjunto de princípios que visam evitar o uso indiscriminado da força,

Direito Internacional dos Direitos Humanos. No domínio da prossecução criminal, os ciberataques são vistos e definidos como actos criminalmente relevantes, passíveis de sancionamento dentro do edifício jurídico do respectivo país. Já para a protecção simples contribui um vasto espectro de actores com o objectivo último de proteger os activos das organizações e dos indivíduos. Esta protecção compreende todos os meios tecnológicos permitidos na lei, bem como as normas técnicas e os instrumentos legais, e é realizada, em primeira instância, pelos donos desses activos, bem como por empresas privadas em regime de *outsourcing* e fabricantes de hardware e de software especializados, mas também pelo Estado, através das suas Forças e Serviços de Segurança e autoridades reguladoras.

	Protecção Simples	**Prossecução criminal**	**Defesa do Estado**
Caracterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros activos.	Os ciberataques são vistos como actos criminalmente relevantes.	Os ciberataques são vistos como um acto de Guerra, pondo em risco a existência do Estado.
Objectivos	Proteger potenciais alvos contra ciberataques.	Prevenir crimes e identificar e condenar os responsáveis.	Eliminar uma ameaça que coloque em causa a Soberania Nacional ou ganhar uma vantagem competitiva sobre outro Estado.
Aspectos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Actuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial.	Actuação sujeita à Constituição da Republica, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Actores	Técnicos de sistemas e de redes, Indústria TIC, autoridades reguladoras sectoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais.	Forças Armadas e Serviços de Informações.

Tabela 1 – Domínios de actuação na protecção do ciberespaço

Na definição de uma política de protecção do ciberespaço, o seu centro de gravidade depende de vários factores, nomeadamente daquilo que Dunn

---

nomeadamente os princípios da proporcionalidade dos meios e o da distinção entre o plano civil e o militar.

(2005) descreve como "*threat politics*", ou seja, "o processo pelo qual uma nova ameaça é introduzida na agenda política." De facto, percebe-se que os Estados com programas de contra-terrorismo, entre os quais se destacam os Estados Unidos, incluam a cibersegurança num contexto de segurança e defesa nacional, focando as atenções no desenvolvimento de meios técnicos para a monitorização do uso da Internet e para a construção de capacidades militares destinadas a fazer face a ataques de larga escala.

Por sua vez, os Estados preocupados com a importância da Internet para a economia e com o facto de esta ser gerida e operada maioritariamente por entidade privadas colocaram o enfoque da cibersegurança no plano do combate à cibercriminalidade e da regulação e do robustecimento da resiliência das infra-estruturas de comunicação, independentemente do tipo de ameaça. Neste ponto de vista, a cibersegurança é vista como factor de geração de confiança no comércio electrónico e como parte integrante das políticas de desenvolvimento da designada sociedade da informação ou, mais recentemente, sociedade do conhecimento. Neste contexto, a cibersegurança é igualmente vista como um instrumento necessário à garantia da protecção da privacidade dos cidadãos. Esta perspectiva torna-se particularmente relevante quando muitos governos encaram como prioritária a desmaterialização da informação e a mediação informática entre o Estado e o cidadão, tudo factores potenciadores de um acesso desmaterializado e situado em patamares de controlo distintos da tradicional posse material de documentos em suporte de papel.

Por outro lado, nos países com tradição no desenvolvimento de planos de protecção de infra-estruturas críticas, a interdependência da Internet e das TIC em geral com outros sectores particularmente críticos como a energia ou os transportes elevou a cibersegurança para um patamar de relevo na estratégia de protecção dessas infra-estruturas face ao poder disrruptivo dos ciberataques. Por este mesmo motivo o próprio ciberespaço passou a ser classificado como infra-estrutura crítica, designando-se, normalmente, como infra-estrutura de informação críticas.

Posto isto, e independentemente do ponto onde deve estar situado o centro de gravidade da acção política nacional nesta matéria, passamos a descrever os três domínios de actuação identificados por Pedahzur.

2 Domínio da protecção simples

O domínio de actuação da protecção simples engloba os meios técnicos, processuais e humanos que realizam diariamente as componentes preventiva, reactiva e de gestão da qualidade da segurança. É, pois, a primeira linha de protecção das infra-estruturas, dos serviços e da informação presentes no

ciberespaço. Neste contexto, um ciberataque é entendido como uma sequência de acções destinadas a produzir um resultado não autorizado ou uma perturbação indesejada na confidencialidade, na integridade ou na disponibilidade de um serviço ou produto, ou seja, a protecção do ciberespaço é perspectivada numa lógica de mercado e de continuidade de negócio.

Tendo em conta que grande parte das componentes do ciberespaço são propriedade ou são geridas por privados, a sua protecção não é um assunto da exclusiva responsabilidade dos Estados. Em diferentes estágios, são muitos os participantes nesta protecção simples, desde os fabricantes de produtos de software, de hardware ou de processos, os técnicos que administram os sistemas e as redes, as entidades reguladoras sectoriais, a academia, os CSIRT – *Computer Security Incident Response Team* –, até, em última instância, o utilizador de tecnologia.

Neste contexto, a indústria das TIC representa um papel muito importante. Por um lado é responsável por uma boa parte das vulnerabilidades nos seus produtos que são alvo de exploração em ciberataques. Por outro é fornecedora e motor, conjuntamente com a academia, da investigação e desenvolvimento para soluções de segurança. A jusante, a eficiente utilização destas soluções depende da capacidade técnica dos administradores de sistemas e de redes das organizações, donde se releva a importância do investimento público e privado quer em tecnologia, quer em pessoas, para a realização das tarefas de monitorização, detecção, reacção e de gestão da segurança.

Para o domínio da protecção simples contribuem, igualmente, o desenvolvimento e a adopção de normas e de boas práticas que permitam a utilização de uma taxonomia comum e de um referencial de medida com vista à avaliação e à fiscalização dos controlos de segurança. Exceptuando alguns casos pontuais de autoregulação como os dos sectores da banca ou da defesa nacional, as normas são geralmente de adopção voluntária e, portanto, a sua adopção é dependente quer da percepção dos respectivos operadores relativamente ao grau de ameaça quer da análise custo-benefício da mesma. Esta dificuldade levou Glaessner (2004) a considerar que "a cibersegurança deve ser assumida como um bem público com intervenção directa do Estado" e Baird a advertir para a falência do actual sistema de governança do ciberespaço – descentralizada, pouco transparente e não centrada nas necessidades dos utilizadores –, e para a necessidade de participação dos Governos num processo de regulação e na "procura do exacto equilíbrio entre um sistema aberto e em rede e a segurança de um ambiente mais controlado" (Baird 2002).

Neste sentido e com uma perspectiva de bom funcionamento do mercado, a Comissão Europeia, através da sua Agência para a Segurança das Redes e da Informação, tem apostado no reforço das medidas de regulação do sector das comunicações electrónicas e na criação da função de CERT nacional em cada Estado-membro.[3]

De facto, no contexto da gestão da segurança, associa-se a cibersegurança essencialmente a medidas preventivas ou de protecção de perímetro. As CERT – *Computer Emergency Response Team* –, por seu lado, foram criadas para realizar as funções de alerta e de resposta a incidentes de segurança informática num contexto aterritorial e distribuído como é a Internet. Um factor bastante importante para o desempenho de uma CERT é o nível de cooperação nacional e internacional. Por um lado a resposta a um incidente de segurança é normalmente centrada no dano visível, quando o incidente pode ser mais vasto, por outro, grande parte dos incidentes de segurança informática têm carácter transnacional, pelo que requerem a participação de várias entidades e a existência de uma rede de contactos. Sobre este particular, e com o objectivo de reforçar o grau de confiança entre equipas e melhorar a sua eficácia têm sido desenvolvidos vários esforços com vista à homogeneização de políticas de tratamento de informação sensível, à definição de uma taxonomia comum para efeito de troca de informação, seja de novas vulnerabilidades, seja de incidentes e ainda para acordar níveis e qualidade de serviço prestado entre elas.

3 Domínio da prossecução criminal

O sistema judicial tem como objectivo principal a dissuasão da prática de crimes, pela prevenção geral (actos de prevenção criminal e o "exemplo" dado pela retribuição social através da sanção penal) e pela especial (a condenação concreta do autor de um crime). A maior parte dos ciberataques configuram ilícitos à luz da legislação nacional e internacional, pelo que importa identificar e julgar os perpretores.

Considerando a importância da protecção das infra-estruturas críticas nacionais, o legislador entendeu, através da nova Lei do Cibercrime, alavancar esse princípio dissuasor, agravando consideravelmente as penas aplicáveis a quem realizar ciberataques contra estas (prevenção geral positiva).

[3] A Agência Europeia para a Segurança das Redes e da Informação (ENISA) tem conduzido um programa plurianual subordinado a este tema e cujo objectivo é a avaliação e o desenvolvimento da segurança e resiliência das redes na Europa. Para mais informação ver http://www.enisa.europa.eu/activities/Resilience-and-CIIP, consultado em Março de 2012.

A título de exemplo, isto significa que numa visão juridicamente menos precisa, mas pragmática, os crimes informáticos são especiais em relação aos praticados por meio de tecnologias de informação, processamento e comunicação, dirigindo-se, tendencialmente, contra as pessoas (como exemplo, a pornografia de menores e os crimes contra a honra) ou contra interesses patrimoniais (ex.: direitos de autor, burla informática) ou, finalmente, contra dados e informação (falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, acesso indevido). Só estes últimos constituem crime informático e só estes tipos do crime são totalmente compatíveis com os princípios da segurança informática (confidencialidade, integridade e disponibilidade). Até ao momento, o enfoque nacional quanto à efectivação do princípio da disponibilidade tem encontrado correspondência prática na tentativa de identificação e no planeamento da manutenção das chamadas infra-estruturas críticas nacionais perante desastres.

Como consequência deste tipo de análise em termos de estratégia nacional, deveriam corresponder-lhe como preocupação de âmbito alargado, tanto a manutenção e salvaguarda das referidas infra-estruturas críticas, como uma relativa à manutenção e salvaguarda dos "dados críticos de interesse nacional"[4].

A competência legal para prevenção[5] criminal e a investigação criminal[6] dos crimes informáticos está atribuída por lei à Polícia Judiciária[7] sendo previsível a constituição de uma Unidade Central[8] (Nacional) para lidar com estes crimes e com os praticados com recurso a meios informáticos.

Em matéria de informações tendentes a contrariar ou a "garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de actos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido"[9] a competência é do Serviço de Informações e Segurança.

---

[4] Dados do Registos e Notariado, Banca e mercado mobiliário, informação criminal e civil, são mero exemplo.

[5] art. 3.º, al. f) da Lei 38/09. 20JUL; e art. 4.º da Lei 37/08 6AGO;

[6] "averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo"; cf. art. 1.º Lei 49/08, 27AGO;

[7] cf. art. 7.º, n.º 3, al. l) e n) da Lei 49/08, 27AGO;

[8] http://www.inverbis.pt/2012/orgaos-policia-criminal/judiciaria-unidade-cibercrime;

[9] art. 3.º da Lei 9/07, 19FEV;

Dentro destas competências legais para prevenção e garantia da Segurança Interna quanto a actos que, pela sua natureza, possam alterar ou destruir o Estado de Direito, existem áreas, como as de diferentes formas de radicalismo, que podem concorrer entre a Polícia Judiciária e os referidos Serviços de Informações.

A título exemplificativo, significa isto, que no actual quadro legal português, perante notícias de um eventual crime de sabotagem informática dirigido a sistemas informáticos críticos[10], em vias de se poder realizar no futuro ou eminente, estaremos no domínio típico da prevenção, sendo de esperar que as entidades visadas pelo ataque cooperem com a Polícia Judiciária e com o SIS no sentido de proceder a acções de desmotivação para a concretização dos actos ilícitos. Se o crime estiver em curso, qualquer entidade (Forças Armadas, SIS, Polícia Judiciária) tem o poder-dever de o comunicar ao Ministério Público, iniciando-se uma investigação criminal legalmente reforçada, uma vez que existe um dever geral de cooperação entre instituições do Estado e um dever especial de cooperação expresso nos diferentes estatutos das entidades referidas, sempre sujeitos ao princípio da proporcionalidade perante o caso concreto.

Chegando a investigação a alguma fase de condução de meios de obtenção de prova, com ou sem necessidade de cooperação internacional (policial ou judicial) segue-se o processo penal "clássico" A final deste processo, os resultados obtidos da investigação podem e devem reverter em nova informação, com destino à prevenção criminal e /ou "*intelligence*".

4 Domínio da defesa do Estado

O campo de aplicação dos ciberataques e das atividades de Guerra de Informação é vasto e ainda pouco definido, não se restringindo a sua utilização apenas à esfera militar. A Guerra no domínio da Informação pode desenvolver-se com base em diversas atividades específicas e permitir, ao Estado que melhor a conduzir, o domínio do ambiente de informação. Só a correta percepção das dinâmicas que afetam este domínio e o acompanhamento da evolução do conceito de Guerra de Informação, nos diferentes Países e Forças Armadas do mundo, pode permitir o desenvolvimento de defesas mais eficazes.

Face ao impacto disruptivo das ciberameaças e à necessidade de garantir o comando integrado das operações a desenvolver no ciberespaço, o Secretário da Defesa dos Estados Unidos da América (EUA) anunciou em Junho de

[10] Seja em termos de conteúdo, seja em termos de trabalho de utilidade para um Serviço do Estado que pela sua importância deve manter-se em trabalho;

2009 a criação do *U.S Cyber Command*. Com a criação deste comando, os EUA passaram a encarar e a assumir de forma clara o ciberespaço como um novo domínio operacional, onde podem vir a ser conduzidas operações militares. Seguindo a iniciativa norte-americana, a Alemanha anunciou pouco tempo depois o levantamento da sua estrutura nacional de cibersegurança e ciberdefesa, no âmbito da qual se previa o levantamento e activação de um comando militar para o ciberespaço em Abril de 2011. Mais recentemente, cerca de 30 países assumiram igualmente iniciativas neste domínio.

Reconhecendo a existência de esforços similares atualmente em curso noutros países, na NATO[11] e na UE,[12] constata-se que todas as Forças Armadas, incluindo as Portuguesas, devem hoje possuir uma capacidade para intervir no domínio cibernético de forma a garantir o correto funcionamento e a proteção das suas comunicações e sistemas de informação, elementos fundamentais para o exercício do comando e controlo no moderno campo de batalha.

Tendo por base o desenvolvimento e exploração de uma capacidade residente de Guerra de Informação, consubstanciada através da condução de operações de informação (OI), de operações em redes de computadores (*Computer Network Operations* – CNO) e da implementação de mecanismos de garantia da informação (*Information Assurance*),[13] as Forças Armadas em geral e o Exercito em particular têm vindo a envidar esforços no sentido do levantamento de uma capacidade de Ciberdefesa.

As Forças Armadas, à luz da Constituição da República Portuguesa, constituem o corpo social responsável pela defesa do Estado contra ameaças externas e devem assegurar, em situações de excepção (ex: estado de sítio), o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado. Face à natureza assimétrica e transversal da ameaça, onde se torna difícil clarificar a origem (interna ou externa) e o impacto dos ciberataques, as Forças Armadas deverão também assegurar o

---

[11] O novo Conceito Estratégico da NATO, aprovado na Cimeira de Lisboa em Novembro de 2010, define como prioritário o levantamento de uma capacidade de ciberdefesa da Aliança.

[12] Constituindo uma das principais lacunas identificadas no âmbito das capacidades militares da UE, foi recentemente desenvolvido um conceito de *Computer Network Operations* que, entre outros aspectos, procura dar resposta aos desafios levantados pela ciberdefesa da UE.

[13] Esta capacidade é vista pela NATO como resultando do desenvolvimento integrado da segurança da informação (*Information Security* – INFOSEC) e de operações de ciberdefesa.

desenvolvimento de capacidades e assumir competências no domínio da ciberdefesa, nomeadamente, as que permitem contribuir para proteger as infra-estruturas de informação críticas e o governo electrónico do Estado.

Também ao nível da segurança da informação é possível constatar que as políticas de segurança foram no passado sempre baseadas no princípio de "evitar o risco". Esta aproximação, encontra-se no entanto desajustada da realidade devendo o nível do risco ser mantido razoavelmente baixo, nomeadamente, através do levantamento de capacidades associadas à *Information Assurance*. Na prática, trata-se de implementar mecanismos associados à protecção e defesa das infra-estruturas de informação críticas. Neste contexto, segundo uma perspetiva de duplo-uso, as Forças Armadas deverão trabalhar em conjunto com outros actores relevantes neste domínio, contribuindo desta forma para, colaborativamente, melhorar a proteção e coordenar a defesa dessas infra-estruturas.

Perspectivando-se de forma consistente a tendência para um aumento crescente das ciberameaças, tanto no âmbito internacional como nacional, importa assim equacionar o desenvolvimento urgente de uma capacidade nacional de Ciberdefesa, explorando de forma articulada as capacidades existentes nas Forças Armadas. Só assim será possível fazer face a eventuais ciberataques (de âmbito nacional ou internacional) que afetem a Sociedade Portuguesa e ponham em causa a Soberania Nacional.

5 Articulação entre domínios

No plano táctico e operacional, a resposta a ciberataques contra infra-estruturas da informação críticas pressupõe sempre uma intervenção no domínio da protecção simples, podendo ainda, considerando a sua motivação e a extensão do seu impacto, implicar a acção nos domínios da prossecução criminal e da defesa do Estado.

Ora, é nestas situações de pretensa escalagem da ameaça ou da gravidade da situação que é primeiramente percebida a necessidade de articulação entre os principais actores de cada um dos domínios descritos. Por outro lado, não sendo propriamente necessária, é por demais evidente que a proximidade cultural, a partilha de informação, a criação de referenciais comum, bem como a cooperação na investigação e desenvolvimento, são factores que potenciam a eficácia global e indivídual dos vários domínios.

Ilustração 1 - Articulação entre domínios de actuação

Esta necessidade de articulação tem levado, no plano internacional e mais recentemente no nacional, à criação de estruturas nacionais para lidar especificamente, com as ciberameaças e os ciberconflitos, em planos diferentes, mas concorrentes, dirigidos à paz social e à segurança nacional.

Num Estado de Direito Democrático, como é o caso do nosso, tal deveria ser atingido, primeiro, pelo estabelecimento de uma Estratégia Nacional de Segurança da Informação, de médio e longo prazo, à qual deveria depois corresponder um conjunto de acções no plano legislativo e operacional, bem como a definição de uma estrutura de governação da cibersegurança para Portugal, identificando para o efeito pontos focais quer na estrutura do Governo quer na estrutura funcional do Estado, com a responsabilidade, respectivamente, no plano político e estratégico, da protecção do ciberespaço, ou seja, da articulação entre os domínios da protecção simples, da prossecuação criminal e da defesa do Estado.

Dito isto, e face à sistematização feita, parece existir a necessidade de equacionar um conjunto de tópicos de fronteira entre os vários domínios essenciais à articulação entre os seus actores (ver Ilustração 1). De entre estes tópicos podemos destacar a partilha de informações de segurança, a sistematização de medidas de mitigação ou boas práticas de resposta a

incidentes, a recolha e preservação de prova digital, bem como a partilha do resultado da análise da ameaça (*situational awareness*). De facto, a experiência e o acompanhamento de casos reais, bem como as dificuldades legislativas (tanto em termos de trabalhos nas suas fontes como na sua aplicabilidade prática após a transposição) e a aparente evolução tecnológica da situação nacional e internacional, apontam no sentido de ser necessário considerar que as informações externas, internas e criminais (*intelligence*) necessitam de alguma forma de submissão a tratamento e a análise comuns, com base em modelos previamente definidos de classificação uniforme de ilícitos e de actos de interesse para a prevenção criminal e para a prevenção de ameaças à Segurança Nacional, obrigando assim, a um plano de recolha e a uma taxonomia comum entre Forças e Serviços de Segurança, passível de adopção pelas entidades intervenientes nos modelos de resposta.

Com base nessa possibilidade técnica e legal, seria então possível adoptar modelos de sinalização antecipada de ameaças (*early warning systems*) que se pudessem, depois, traduzir na possibilidade de disseminação nacional da informação relativa, quer à qualificação do nível de ameaça, quer à declaração do nível de segurança em cada momento.

Em consequência, no espaço relativo ao tema da cibersegurança, as fases do planeamento operacional e da acção táctica terão de revelar acções de conjunto dos seus actores, por forma a preencher os campos de acção internos e externos, na recolha de informação pertinente, previsão de incidentes e reacção aos mesmos, tanto no plano individual (pessoas singulares e colectivas) como no plano nacional.

O alinhamento dos diferentes actores citados anteriormente, não pode, portanto, ser estanque, nem exclusivo e teriam de participar, conforme o caso concreto, umas vezes em primeira linha, outras em segunda, garantindo um trabalho contínuo de produção e de partilha de informações atinentes ao estabelecimento de fraquezas e de forças organizacionais, perfis pessoais, organizacionais e tecnológicos. Neste cenário, faz todo o sentido pensar que um modelo de Centro Nacional de Cibersegurança, à imagem do que Brechbuhl (2010) designa de *network-centric*, composto por entidades que directa e legalmente já tenham nas suas competências legais que ver com as diversas facetas do conceito de cibersegurança, possa ter competência para aglutinar outras entidades úteis ao planeamento e coordenação de acções ininterruptas de âmbito nacional, específicas, nos campos da sensibilização, da formação e da prevenção,[14] dirigidos a grupos alvo concretos, como a

[14] Desenho, apoio e motivação para a formação técnica e académica na área dos ciberataques, das matérias de prevenção criminal em disciplinas do Ensino Secundário e Superior, abrangendo os temas da fraude económico-financeira, criminalidade informática e a praticada com recurso a meios informáticos, visando

população académica e científica, o tecido empresarial composto pelas pequenas e pelas médias empresas, e a população activa, que tipicamente recorra às tecnologias de informação, processamento e comunicação, visando aumentar o nível médio de conhecimento (e consequentemente de sensibilização para a segurança da informação e segurança informática) e a gerar efeitos no espaço cibernético estrangeiro e nacional, que potenciem sinergias de âmbito e do interesse nacional, enquanto que desmotivando a ocorrência de acções externas e hostis.

Mais do que grandes investimentos financeiros, importa organização, método e vontade de articulação efectiva no âmbito do interesse nacional.

6 Conclusões

A evolução das ciberameaças, no âmbito nacional e internacional, afeta transversalmente toda a Sociedade, impondo o levantamento de capacidades de protecção e defesa e a clarificação dos diferentes aspectos ligados à cibersegurança e à ciberdefesa do Estado.

Uma vez que o ciberespaço, enquanto espaço de interação social, materializa uma área de responsabilidade coletiva, torna-se necessário identificar o papel a desempenhar pelos diversos órgãos, públicos e privados, na garantia da sua protecção e utilização segura. Neste contexto, importa analisar o risco social e o impacto dos diversos tipos de ataque cibernético, 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, exigindo uma participação activa das Forças Armadas.

Neste contexto, a atribuição de responsabilidades e competências no âmbito do ciberespaço, entendido como uma extensão virtual do mundo (físico e real) em que habitamos, deverá obedecer à mesma lógica e fundamentos que caracterizam a segurança e a defesa do Estado. Obedecendo aos mesmos princípios legais enformadores, os operadores de infra-estruturas da informação críticas e os CERT são responsáveis pela primeira linha de defesa dentro do respectivo quadro regulatório, os órgãos de polícia e de investigação criminal serão responsáveis por perseguir e punir os

---

despoletar e participar em trabalhos de interligação entre diferentes entidades sujeitas a formas de sigilo, de segredo profissional, de segredo de justiça e de Estado que possam assim contribuir para a Cibersegurança e para o combate ao Cibercrime, simultaneamente nos planos da autotutela, da repressão criminal e da defesa do Estado.

cibercriminosos, assim como as Forças Armadas devem ser vistas como o corpo social responsável pela ciberdefesa do país. 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 da inexistência de legislação específica.

O levantamento de um Centro de Ciberdefesa deverá assim ser enquadrado nas iniciativas actualmente em curso no País, nomeadamente, as associadas ao levantamento de um Centro Nacional Cibersegurança e de uma Rede Nacional de CSIRT. Neste âmbito, deverão também ser tidos em atenção os esforços cooperativos já lançados pelas Organizações Internacionais de que Portugal faz parte integrante (NATO e UE) e por outros Países que, de forma individual ou cooperativa, procuram também estruturar uma capacidade neste domínio.

Neste contexto, face às capacidades residentes e ao conjunto de iniciativas já desenvolvidas, faz todo o sentido perspetivar-se as Forças Armadas, na ótica de serviço público, como elemento gerador de futuras capacidades de duplo uso Civil-Militar, no quadro do desenvolvimento da Estratégia da Informação Nacional e do levantamento de uma capacidade de Ciberdefesa do País.

Referências:

Baird, Z. (2002), "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs* 81 (6), pp. 15 – 20.

Brechbühl, H., R. Bruce, S. Dynes, and M. E. Johnson (2010), "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy", *Information Technology for Development* 16 (1), pp. 83 – 91.

Dunn, M. (2005), *A Comparative Analysis of Cybersecurity Initiatives Worldwide*. Technical report, ITU - WSIS Thematic Meeting on Cybersecurity. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, consultado em Janeiro de 2009.

Glaessner, T. C., T. Kellermann, and V. McNevin (2004). *Electronic Safety and Soundness: Securing Finance in a New Age*. Technical report, The World Bank. http://www.ftc.gov/bcp/workshops/proofpositive/e-safety-and-soundness.pdf, consultado em Janeiro de 2009.

Pedahzur, A. (2009). *The Israeli Secret Services & the struggle against Terrorism*. Nova Iorque: Columbia University Press.