REFLEXÕES EM TORNO DO TEMA "DIREITO E CIBERSEGURANÇA EM PORTUGAL": NOTAS DISPERSAS

Reflections on "Law and Cibersecurity in Portugal": some notes

Eduardo Alves Vera-Cruz Pinto[1]

RESUMO

A cibersegurança só pode ser organizada pelo Estado, nas sociedades livres e democráticas, a partir de um compromisso político de respeito pelas regras e princípios do direito, efetivados em uma legislação comprometida com os valores jurídicos, que atua como limite aos poderes do Estado. Para a garantia da segurança no ciberespaço deve-se partir de três premissas: não há respostas apenas nacionais, é necessária a cooperação organizacional internacional/transnacional; somente em nível nacional é possível criar sensibilidade, cultura e mentalidade para prevenir e detectar ataques e reduzir riscos; e, por fim, a segurança das redes leva à eficiência de custos na administração pública. A segurança não é uma questão de ordem, mas de cumprimento de expectativas legítimas, de respeito às funções do Estado e de Justiça na intervenção dos poderes públicos. Por isso, o direito à cibersegurança pressupõe identificar os valores que partilhamos como comunidade e os conceitos, instituições e regras que constituem, em cada Estado, o corpo normativo-institucional da cibersegurança.

Palavras-chave: Cibersegurança; Direito; Organização do Estado; Portugal.

ABSTRACT

The cybersecurity can only be organized by the State, in free and democratic societies, through a political compromise with the rules and principles of law, realized in a legislation which is committed to legal values and which acts as a limit to the power of State. The guarantee of the cibersecurity should be based on three assumptions: there are no answers which are only national, it is necessary international cooperation and organization; only at the national level it is possible to create sensitivity, culture and

---

[1] Diretor da Faculdade de Direito da Universidade de Lisboa. Lisboa – Portugal. Texto recebido em 13.12.2010.

mentality to prevent and detect attacks and mitigate risks and, the third one, networks secutiry leads to cost efficiency in public administration. Security is not a point of order, but it is a question of realization of legitimate expectations, of respect for State functions and of justice in government intervention. Therefore, the right to cybersecurity means to identify shared values and the concepts, institutions and rules, in each State, that constitute the normative-institutional body of the cibersecurity.

Keywords: Cibersecurity; Law; Portugal; State Organization.

1 INTRODUÇÃO

A cibersegurança[2] só pode ser organizada pelo Estado, nas nossas sociedades livres, democráticas e de pendor social (não individual), se existir um compromisso político de respeito pelas regras e princípios de Direito, efectivado numa legislação comprometida e fiel a estes valores próprios do Jurídico, que actua como limite aos poderes do estado, sem tolher a eficácia da sua actuação no dever de garantir a segurança da comunidade e de cada um dos seus cidadãos.

Por isso, os juristas não podem deixar de participar na criação, consolidação e difusão de doutrinas úteis à cibersegurança nacional articulando as regras, princípios e conceitos do direito com os conceitos e doutrinas essências do domínio *ciber*[3]. A compreensão do Jurídico pelos decisores políticos e pelos cientistas informáticos, bem como a entendimento pelos juristas das angústias e perplexidades dos primeiros, na hora de decidir, e as possibilidades dos segundos, na hora de construir os meios de acção – é fundamental para a eficácia da prevenção e da resposta a incidentes e ataques no espaço ciber que colocam em causa a segurança nacional.[4]

Cabe também aos juristas tentar impedir: quer a securitização do ciberespaço pelo estado com prejuízo dos direitos das pessoas, através das tentativas de certos meios de criar pânico nas populações agitando um ciberataque, tipo "11 de Setembro", com um ataque massivo às

[2] Estão afastadas aqui as problemáticas próprias da ciberguerra/ciberdefesa e as suas implicações jurídicas, bem como as do cibercrime e do sua configuração jurídico legal.

[3] Ver: JOUBERT, Vincent. Getting the essence of cyberspace: a theoretical framework to face cyber issues. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 111-125.

[4] Ver: WOLFERS, Arnold. "National security" as an ambiguous symbol. *Political Science Quarterly*, v. 67, n. 4, p. 481-502, dec. 1952.

infraestruturas vitais dos estados democráticos e livres; quer a ausência de intervenção estadual para garantir a cibersegurança porque qualquer acção do Estado é vista como uma ameaça de violação dos direitos mais sensíveis das pessoas e uma intromissão na sua intimidade.

Muitos sãos os aspectos e as problemáticas que ligam os juristas que se dedicam a estudar as implicações jurídicas da cibersegurança e os especialistas em cibersegurança que procuram saber o direito aplicável aos domínios em que actuam. Não podemos aqui abordar aspectos jurídicos concretos com implicações na cibersegurança como: a regulação das comunicações; a legislação sobre a construção e manutenção de infraestruturas; o planeamento energético; a responsabilidade do Estado por intromissão informática na intimidade da vida de uma pessoa e de uma pessoa por dificultar a acção legítima/legal de defesa ciber do Estado, etc.

Aqui trataremos apenas, de forma genérica, do lugar do Direito na elaboração de uma estratégia nacional para a cibersegurança centrada num dos elementos integrado no conceito genérico de ciberforça que é um Centro Nacional de Cibersegurança.

Vencer o preconceito em matéria de segredo para a segurança

Em Portugal existe uma desconfiança que persiste no que respeita ao segredo garantido pela classificação de documentos como secretos e pela necessidade de vedar o acesso generalizado a certos procedimentos e decisões dos titulares de poderes do Estado. Mais de três décadas após o derrube da ditadura, nada justifica que se continua a alimentar tal desconfiança considerando-a uma ameaça aos direitos dos cidadãos, quando o segredo existe num Estado de Direito exactamente para proteger os cidadãos enquanto comunidade politicamente organizada no Estado.

Fomentado o preconceito no plano político e jurídico, ele é depois ampliado pelos meios de comunicação social, impedindo qualquer debate no espaço público que expresse os resultados das análises mais profundas e prolongadas feitas em ambientes académicos e de investigação sobre esta temática.

O actual sistema legal sobre os vários segredos precisa de ser revisto porque está desactualizado, é ineficaz e descredibiliza a possibilidade de segurança, ridicularizando o país no exterior[5], além de

[5] Basta pensar no *Official Secrets Act* do Reino Unido, que tipifica cerca de 2.000 ilicítos em que os funcionários do Estado ou servidores públicos e os cidadãos podem violar o seu dever de sigilo.

criar vulnerabilidades e ameaças que cabe ao poder político, pela via legislativa, prever e evitar.

Deixar à discricionaridade do executivo o que classifica e não classifica sem seguir critérios rígidos para a classificação nos vários graus; não haver quem no governo saiba ainda que muito pouco sobre isso; não estando o pessoal político e de confiança política preparado, ou mesmo sensibilizado, para os problemas envolvidos na classificação de documentos e na acreditação de sistemas informáticos; não existir qualquer orientação policial ou judiciária na prevenção e repressão de atentados contra os segredos públicos, todos conhecendo uma realidade onde eles são constante e impunemente violados – são apenas sintomas de um Estado que, apesar dos seus compromissos internacionais, é desleixado com as questões de segurança e procura, muitas vezes, argumentos no Direito para justificar/legitimar este laxismo político, cívico e legislativo.[6]

Esta situação precisa de ser profundamente alterada em dois planos muito concretos: a longo prazo investindo, desde já, nas temáticas de segurança nas disciplinas curriculares desde os primeiros graus de ensino até à formação universitária e à investigação científica; depois a curto prazo, aprovando leis mais concretas na tipificação dos comportamentos lesivos, graduação das censuras normativas pela hierarquia dos valores a proteger, responsabilizando as hierarquias pela diligência nos ambientes a proteger e pela denúncia das violações detectadas, e finalmente, com sanções mais claras e exequíveis.

Sem se iniciar este percurso não adianta muito, a não ser para responder à pressão dos nossos parceiros estratégicos e às inspecções das organizações internacionais, cuidar dos aspectos relativos à cibersegurança.

---

[6] O texto de jurisprudência mais importante entre nós continua a ser o Acordão n. 458/93, publicado a 17 de Setembro, sobre o segredo de Estado (Lei n. 6/94, que aprova o regime jurídico do segredo de Estado). A revisão constitucional de 1989 introduz o segredo de Estado na Constituição (art. 159º; 168º, n. 1, al. r) e trata dos direitos dos cidadãos na recolha de informação em ficheiros informáticos (art. 35º da Lei n. 65/93, que adapta a regulamentação dos SEGNACs ao acesso dos cidadãos aos documentos da Administração Pública). Um passo importante em matéria de segurança foi a aprovação em 1988, dos SEGNACs 1 (Instruções para a segurança nacional, salvaguarda e defesa de matérias classificadas) e 2 (segurança industrial, tecnológica e de investigação) 3, em 1990, (segurança informática) e 4, em 1991 (segurança das comunicações), sob a forma de Resolução do Conselho de Ministros. Infelizmente a falta de natureza normativa das regras limitou o alcance de procedimentos e soluções e não teve continuidade no processo legislativo.

2 UMA ESTRATÉGIA PORTUGUESA PARA A CIBERSEGURANÇA NACIONAL

Qualquer ciberestratégia nacional para garantir a segurança no ciberespaço[7] deve partir de três premissas que são pressupostos:

- em cibersegurança[8] não há respostas apenas nacionais, porque nenhuma das respostas territorialmente delimitadas é suficiente, eficaz e célere. Só existe uma resposta internacional/transnacional, através da

[7] A invenção da palavra *cyberspace (ciber* etimologicamente significa "homem do leme" ou "piloto", associado a um espaço global, sem fronteiras físicas onde circula informação) é atribuída ao escritor norte-americano *William Gibson*, *Neuromancer*, 1982. *Gibson* aplicou a palavra para se referir a uma rede de computadores ligada directamente à mente humana, numa ficção verniana, visando um futuro de pendor utópico, a funcionar dentro da internet, e não com o intuito de a conceptualizar. Já *Michael Benedikt* no livro *Cyberspace*: first steps, 1991 (no seguimento da I Conferência sobre Ciberespaço, 4 e 5 de Maio de 1990, em Austin, Universidade do Texas), define os elementos essenciais do conceito de ciberespaço: ilimitado (o acesso ao ciberespaço faz-se através de qualquer computador em rede, a qualquer hora e em qualquer lugar); virtual, (porque é um não lugar: existe em todos os lugares – todos os computadores do mundo – e não se localiza em nenhum lugar – ambiente virtual); mental (corresponde a uma "geografia mental"); eléctrico (porque depende da electricidade para funcionar); intemporal (as suas bases de dados e registos materializam passado, presente e futuro num sistema de presença horizontal); "informacional" (porque nele a informação não é filtrada, nem parcializada – é informação pura). Logo, o ciberespaço é o mundo digital que opera através do computador e das redes informáticas incluindo todos os aspectos da actividade *on.line*. O ciberespaço engloba todas as formas de actividades digitais desenvolvidas em rede – o que inclui o conteúdo e as acções realizadas através de redes digitais. O ciberespaço é hoje um domínio da comunicação computacional essencial para o desenvolvimento de uma comunidade, organizada como Estado. O ciberespaço tem uma parte física, com um pendor técnico, constituída pelos computadores e pelos sistemas de comunicações. Estes componentes técnicos suportam as nossas actividades quotidianas, pessoais e profissionais, e constituem-se em infraestrutura nacional, em vários sectores, nomeadamente para as informações e a segurança.

[8] A cibersegurança engloba todos os elementos das infraestruturas digitais e todos os aspectos cobertos pelo interesse nacional no ciberespaço, de forma articulada com a política de segurança de Portugal, através do envolvimento de todas oportunidades e benefícios que o ciberespaço oferece. A cibersegurança requer inovação, investimento e competitividade no sector informático e das telecomunicações. A cibersegurança visa maximizar a segurança das infraestruturas físicas e das redes em que circulam as informações e as comunicações electrónicas/digitais e assegurar a disponibilidade, integridade, autenticação, confidencialidade, não repúdio e resiliência da informação. A cibersegurança tem como limite a protecção dos direitos de personalidade e os direitos fundamentais sensíveis, nos termos definidos na lei.

cooperação organizacional, em que as estratégias nacionais coincidem e se compatibilizam;[9]

- só a nível nacional é possível criar as sensibilidades, as culturas e mentalidades que permitem prevenir e detectar ataques, reduzir os riscos[10] e mitigar os efeitos de um atentado à cibersegurança nacional[11]. Como só a nível nacional, no uso de prerrogativas e poderes de soberania, se pode criar e manter actualizada e operacional a rede de infraestruturas e de meios humanos especializados necessários para as exigências crescentes e especializadas da cibersegurança.[12]

- a cibersegurança é vital para a imagem e a credibilidade externa de Portugal. Se as nossas redes forem consideradas seguras e fiáveis; se

---

[9] Num mundo cada vez mais globalizado a efectivação do que é definido como o interesse nacional de Portugal está dependente do ciberespaço e esta *dependência* atinge as pessoas, as empresas, as escolas, todas as áreas da Administração Pública, da indústria, dos transportes e da defesa e da segurança. Hoje o funcionamento do Estado está dependente do ciberespaço.

[10] O risco é uma realidade normal no nosso quotidiano. As pessoas, de forma inconsciente, todos os dias fazem uma análise e uma avaliação dos riscos e a sua consequente gestão. Em termos de cibersegurança o risco pode ser definido como a probabilidade de uma ameaça explorar vulnerabilidades, de forma a causar perdas ou prejuízos nos sistemas de informação e de comunicação, de energia, de gestão de recursos. Os riscos são determinados pela combinação das ameaças, vulnerabilidades e valor dos bens visados. Tal valor é calculado com base no impacto (entendido como o conjunto de resultados de um incidente – casual ou propositado – inesperado) destes bens na vida das pessoas, das instituições e das infraestruturas críticas. Seja qual for a análise e identificação dos riscos que veem do ciberespaço é sempre difícil tomar as medidas preventivas adequadas para anular ou mesmo reduzir os efeitos. Sabemos que os riscos que se apresentam às infraestruturas críticas resultam normalmente de inconsistência ao nível da estrutura e de falta de investimento na formação e na sensibilização das pessoas que têm funções ligadas aos computadores nas várias entidades.

[11] Ver: KAMINSKI, Ryan T. Escaping the cyber state of nature: cyber deterrence and international institutions. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 79-94.

[12] A nível interno e no uso de poderes de *ius imperium*, exige-se: rigor na análise dos riscos e da definição de objectivos e de capacidades; competência e rapidez nas respostas aos desafios e aos ataques; abordagem multilateral, cooperação institucional e integração administrativa na organização da cibersegurança; equilíbrio e flexibilidade no recrutamento especializado por concurso; investimento no mérito e no conhecimento para os cargos dirigentes; parcerias com entidades ligadas à defesa dos direitos e à transparência das decisões; auditorias de entidades privadas especializadas; reforço da cultura de segurança em entidades públicas com a responsabilização da negligência propiciadora de riscos; e intensificação dos deveres de cidadania na envolvência da segurança comum, a começar pela pedagogia nas escolas.

for protegida de forma eficaz a propriedade intelectual das empresas, universidades e outras entidades, que sustentam o mundo do conhecimento; se os negócios efectuados pela nossas redes apresentarem vantagens competitivas no mercado global, pela garantia de segurança *on-line*; se os cidadãos tiverem confiança nas transacções de serviço público, conseguem-se ganhos de eficiência e redução de custos na administração pública.

Com os pressupostos estratégicos definidos, para que os desenvolvimentos posteriores se mantenham nos limites que apontam para o fim pretendido, a segurança do ciberespaço, é necessário fixar os princípios e valores que orientarão a selecção das regras e a criação das normas que concretizam a estratégia.

Nas nossas sociedades livres, democráticas e de direito (porque as leis obedecem ao direito e não o contrário: as leis criam o Direito), a segurança (logo também a cibersegurança) é concebida, regulada e aplicada nos termos e nos limites juridicamente definidos e plasmados em leis e regulamentos.

Essa posição de princípio impõe que sejam claramente afirmados os princípios jurídicos rectores nestas temáticas: respeito pelos direitos fundamentais e de personalidade; obediência ao princípio da legalidade; primado do direito, pela via constitucional; respeito pelas decisões do poder judicial; transparência na administração; direito de reserva nas matérias classificadas; controlo e fiscalização democráticos dos órgãos com competências em cibersegurança; responsabilização dos titulares de cargos e de funções face às decisões tomadas.

3 A ORGANIZAÇÃO DO ESTADO E A SEGURANÇA DA COMUNIDADE: DIAGNÓSTICO E TERAPIA

Isto assente, e sabendo que a protecção do mundo digital[13] e do espaço de circulação internética deve incidir prioritariamente sobre infraestruturas, importa reconhecer que se as nossas infraestruturas de comunicações electrónicas e as competências que lhe estão associadas, bem como as áreas secantes a elas, não forem reposicionadas, reestruturadas e actualizadas, ficaremos irremediavelmente fora dos centros de decisão e

[13] Ver o relatório do governo britânico: *Digital Britain*: the final report 2009 (Cm 7650). (London: The Stationery Office (TSO), 2009. Disponível em: <www.official-documents.gov.uk/document/cm76/7650/7650.pdf>. Acesso em: 10 jan. 2011).

dos fóruns onde se discutem e se partilham informações e conhecimentos, ao mais alto nível.

Mas quem, a nível do estado, pode fazer tal plano? Como fazer a preparação e a selecção daqueles que integram as especialidades convocadas para o efeito? Quais as metodologias de decisão a adoptar para cumprir o planeado? Qual a noção de interesse nacional que deve estar presente, de forma constante, na interpretação das decisões e normas internacionais relativas à cibersegurança?

A resposta a estas perguntas seria fácil se Portugal tivesse uma Administração Pública organizada de acordo com critérios de hierarquia e de eficiência; a funcionar por objectivos assentes em estratégias parcelares e a funcionar de acordo com critérios de racionalidade económica e de gestão atendendo aos fins. Apesar das reformas recentemente introduzidas, com óbvios ganhos organizativos, a estrutura decisória manteve-se; a burocracia aumentou; a autonomia institucional cedeu à governamentalização centralizada e a transparência, apesar de muito referida, ficou esmagada pela opacidade discricionária das escolhas políticas e dos interesses instalados.

Nada pior na instalação de infraestruturas de segurança, em sistemas fragilizados pelos avanços tecnológicos constantes e pela multiplicação de acessos, que a subjectivação nas opções e nas titularidades, e a perda de autonomia decisória dos que estão mais perto dos problemas a resolver.[14]

Junta-se a este cenário uma falta de capacidade política e de pedagogia cívica na difusão de uma cultura administrativa de responsabilidade que torne natural e normal considerar como preterição grave dos deveres funcionais, no caso dos servidores públicos, qualquer quebra de segurança motivada por negligência ou falta de cuidado, na guarda de infraestruturas ou de instrumentos e de mecanismos envolvidos na sua segurança.

A necessidade de publicitar as regras, positivá-las como normas legais e regulamentares, referindo os responsáveis a partir dos seus conteúdos funcionais, não deixando equívocos sobre o que devem fazer e as consequências de não o fazerem; e a enumeração das sanções a partir de comportamentos de risco, devidamente tipificados – é fundamental e está, na sua essência jurídica, por fazer.

---

[14] Ver: *The national security strategy of the United Kingdom*: update 2009: security for the next generation (Cm. 7590). (London: The Stationery Office (TSO), 2009. Disponível em: <http://www.official-documents.gov.uk/document/cm75/7590/7590.asp>. Acesso em: 10 jan. 2011).

Portugal tem um longo e penoso caminho a percorrer nesta matéria e deve começar a trilhá-lo de forma parcelar, porque quando a obra é muita, o ânimo fenece. Assim, o sector da cibersegurança pode ser trabalhado como um todo autónomo, ligado (ainda que não integrado) ao subsistema de segurança de infraestruturas de comunicação electrónica (porta de entrada para a cibersegurança básica).

Para iniciar tal trabalho, com as dificuldades técnicas e de mentalidade já referidas, é necessário consensualizar um modelo orgânico para a segurança nacional e depois investir na sua concretização. Ora, os partidos políticos portugueses não estão de acordo sobre o modo de organizar a segurança nacional e têm nos últimos tempos aprofundado divergências sobre o tema.

Quando assim é exige-se aos decisores políticos que transfiram a definição do modelo e a montagem das estruturas para o plano científico e técnico, juntando especialidades e criando as condições mínimas para que o trabalho seja continuado e útil para que as decisões, reservadas aos políticos, possam ser efectivadas e céleres.

A questão da cibersegurança é de tal modo importante para a defesa da comunidade e do estado, do nosso modo de vida e do regime político em que escolhemos viver, das nossas infraestruturas críticas[15] e

[15] Infraestrutura crítica é um sistema, físico ou electrónico, cuja destruição pode ter um impacto negativo na segurança interna, na defesa externa ou na subsistência económica de um Estado. As infraestruturas críticas são controladas por um sistema de informação que regula automaticamente o seu funcionamento. A debilidade destas infraestruturas críticas pode afectar o regular funcionamento dos serviços públicos, das entidades da sociedade civil e das instituições democráticas, criando uma situação favorável à subversão interna e à invasão externa. A metodologia para análise e gestão do risco recai sobre a potencialidade das agressões e riscos vindos através do ciberespaço. Logo, assenta nas vias de acesso lógico ou normal aos sistemas e actividades críticas com necessidades de ligação dos sistemas à internet. A gestão do risco integra três elementos: 1. a análise de risco - identificação dos recursos, infraestrutura existente, ameaças, vulnerabilidades e medidas de protecção já existentes, incidindo tanto nas matérias tecnológicas como nas organizacionais, bem como analisar essas informações, avaliar o impacto de algumas ameaças e determinar quais os riscos mais graves propondo soluções para a redução dos riscos recenseados, alterações às políticas de segurança e necessidades de formação e de treino de pessoal; 2. a mitigação de riscos - reduzir riscos implica concluir o processo de planeamento e efectivar soluções que reduzam os riscos apontados na fase de "análise de risco", fixando prazos, responsabilidades e respectivas configurações; 3. e a análise e avaliação dos riscos - monitorizar a eficiência das práticas seguidas e a eventual experimentação de novos riscos, controlar alterações na infraestrutura e no pessoal e reajustar o que se fez de novo nos processos de gestão dos riscos.

das nossas vidas, da nossa estrutura social e das nossas opções pessoais e cívicas; da nossa liberdade religiosa e da livre expressão; da nossa intimidade e do valor da participação política que só pode ser considerada uma questão de estado.

Por isso, a governamentalização do estado pela via administrativa e a partidarização do estado pela governamentalização da sociedade (sem espaço de afirmação das estruturas não estaduais ou não infiltradas pelos partidos políticos através da imposição legislativa de membros indicados pelo governo e pelo parlamento) impõe que a estrutura seja mantida em constância ao longo do tempo; e só as decisões que ela serve sejam reservadas à decisão política institucional.

Em Portugal a entidade pública que deve ter a responsabilidade de organizar os meios que iniciem a construção de rede de segurança ciberespacial deve ter a natureza jurídica de uma entidade independente do Estado[16], como deveria ser a Autoridade Nacional de Segurança.[17]

---

[16] Actualmente a ANS está em Portugal diluída no Gabinete Nacional de Segurança (GNS). No processo inelutável de revisão das missões da ANS após o 11 de Setembro, tentamos, por incumbência dada pelo Almirante José Torres Sobral, na proposta de diploma legal apresentada para apreciação do Secretário de Estado da Presidência do Conselho de Ministros, dar à ANS o estatuto jurídico-legal compatível com as funções exigidas no âmbito da OTAN e da UE. Infelizmente o DL n. 170/2007, de 3 de Maio (Lei Orgânica do GNS) confirmou a opção pela continuidade de um sistema em que a ANS só existe através do GNS, que se reduz a um serviço central da administração directa do Estado, a funcionar no âmbito da Presidência do Conselho de Ministros, junto do Gabinete Coordenador de Segurança, na dependência do Primeiro Ministro ou do membro a quem ele delegar (normalmente o Secretário de Estado da Presidência do Conselho de Ministros). A ANS é um nome que dirige um serviço que é tudo o que ela faz. Com respeito pelos que defendem tal solução, esta é a pior forma de garantir a eficácia das missões que a lei e os tratados cometem à ANS, comprometendo a eficácia dos serviços que presta e a prevenção em que participa.

[17] Como acontece na Noruega, onde a ANS é a responsável pela coordenação da cibersegurança e da *information assurance*, com o NoCert incluído na sua orgânica incluindo um dos mais avançados centros europeus de monitorização de ameaças. Nos EUA, a responsabilidade de coordenar a cibersegurança do Estado e a *information assurance* é da NSA (National Security Agency), que nos EUA tem basicamente as mesmas funções que a ANS em Portugal (criptografia; certificação de sistemas e produtos, credenciação e acreditação; e ANS dos EUA na OTAN). Na Alemanha a cibersegurança é da responsabilidade do BSI (Autoridade Nacional de Comunicações), com a função de reportar todos os incidentes, tratar da *information assurance*; produzir doutrinas e normas; fazer a *common picture* das ameaças.

Tal entidade tem de incluir as universidades e os laboratórios do Estado, bem como os centros de investigação especializados, na sua acção organizativa, como parceiros essenciais na definição de prioridades e no recenseamento dos elementos que devem ser ponderados na formação da rede pública infraestruturada para a cibersegurança.

Tal participação de académicos e investigadores pressupõe que estejam ligadas a instituições legalmente obrigadas a divulgar os seus projectos, informar sobre os seus financiamentos, partilhar os resultados das investigações e estudos efectuados, para que se possa seleccionar, em processos concursais transparentes e abertos, os melhores de entre nós para contribuir no esforço de criar um sistema eficaz de cibersegurança.[18]

Se olharmos, por exemplo, para o caso da Noruega, através de um financiamento contratualizado entre o Estado e os privados (que pagam uma taxa anual fixa para integrarem o sistema central) foi possível implantar um sistema de sensores (um sensor instalado em cada rede da infraestrutura crítica de informação integrada no sistema) com monitorização central (VDI).[19]

Concluímos, assim, que não é possível criar uma rede capaz de assegurar a cibersegurança, com eficácia técnica, prontidão de resposta e respeito pelo Direito aplicável se não for efectuada, pelo menos no que respeita a este subsector da segurança uma profunda reforma das mentalidades funcionais e dos sistemas organizativos do estado.

Infelizmente, a situação actual, que o poder político legitimou com leis e regulamentos, é de uma escolha de profissionais envolvidos em projectos nacionais a partir de critérios ligados à fidelidade política e à sua capacidade para aceitar acriticamente orientações fixadas por ministros que, não sabendo, decidem sem ouvir e só aceitam assentimentos e vénias, onde deveriam ouvir recriminações e negativas. A competência dos

---

[18] A desorganização do Estado fica exposta quando aparecem em reuniões internacionais representantes de vários departamentos do Estado e da Administração Pública, bem como de universidades, centros de investigação e de empresas, sem saberem uns dos outros, nem sequer que, no seu país, existiam organismos com competências na matéria e pessoas especializadas. As leis orgânicas e a actividade dos serviços e entidades públicas não é coordenado nem organizado. O esbanjamento de recursos públicos e a ineficácia dos serviços prestados é o resultado.

[19] A taxa ascende aos US$ 50.000, sendo actualizada todos os anos, mas protege e beneficia os privados que acedem ao VDI, pois, entre outras vantagens, são anualmente apresentados *ciber threats assessment* personalizados e prestado apoio especializado e continuado a ameaças persistentes.

escolhidos, com as excepções conhecidas, está quase só na conveniência da escolha assim feita.[20]

Portugal tem acentuado, na dependência político-partidária da estruturas de cúpula da Administração Pública, sucessivamente fragilizadas por discursos oficiais desconfiados e desmotivantes, por normas erráticas e sem futuro (porque sem projecto), por contratação de privados para fazer aquilo para que a administração pública existe e sabe fazer, com custos bem mais baixos e com eficácia bem maior.[21]

Ora, critérios políticos só aparentemente transparentes para escolher as pessoas com competência para integrar projectos nacionais na área da cibersegurança, com o arbítrio e a subjectividade própria dos decisores políticos, obriga a uma de duas atitudes:

- ou fazer uma reforma profunda e completa da administração pública que entregue a pessoas promovidas por mérito as chefias de departamentos especializados, sem intromissão dos poderes político-partidários, terminando com uma concepção de Estado, como a actual, avessa ao estado de direito;

- ou criar uma especialidade normativa que isole a cibersegurança da Administração Pública, ligando a uma entidade pública estatal com características de independência técnica e profissional, sem prisões

---

[20] As regras de transparência que o legislador aprovou são um engano. As pessoas passam a saber que a escolha foi mal feita porque os *curricula* são publicados, mas não existe um critério racional e orgânico de escolha, por selecção dos mais aptos e competentes. Para justificar os favorecimentos, diz-se que o critério de escolha é político. O conceito jurídico-material de transparência na escolha dos mais aptos para servirem o Estado, com competências técnicas, exigia de quem interpreta, com legitimidade democrática, o interesse público e o bem comum, outra atitude na criação das normas aplicáveis.

[21] Em Portugal, onde o discurso sobre a corrupção é apenas uma retórica discursiva e as medidas de combate são de um ridículo indizível, pois situado ao nível da sanção nos comportamentos menores, esquecendo a responsabilidade pedagógica, pelo exemplo das elites, nada consegue de positivo – um dos maiores factores de corrupção nos últimos tempos tem sido a contratação de "técnicos" arquitectos, engenheiros, advogados, economistas e outros, sem concursos, por escolha política, que vivem apenas desses favores políticos, constituindo-se como pontas de lança dos partidos e agentes de propaganda, pagos pelo erário público. Esta clientela de luxo paralisa e descredibiliza o Estado e a função pública, afasta a concorrência sadia e a selecção pelo mérito e mantém a comunidade de especialistas silenciosamente prisioneira da cunha e do compadrio, esperando a sua vez de beneficiar do sistema. Os que não aceitam as regras materiais fixadas, formalmente escondidas e competentemente trabalhadas na positividade legal para este resultado, ficam excluídas da participação cívico-profissional.

orgânicas ou outras a chefias intermédias e a organismos *ad hoc* ou de outra natureza, dependentes directamente do Conselho Nacional de Segurança, presidido pelo Presidente da República.

Seja qual for a via, reiteramos que deve ser a ANS a entidade que em Portugal deve coordenar a cibersegurança, o que impõe: enfrentar com coragem cívica e política a batalha na opinião pública pela necessidade de serviços de informação e segurança fiáveis, competentes e ao serviço da comunidade e de cada cidadão; uma revisão política das opções legislativas feitas na estrutura dos serviços de informação e segurança do Estado que é desarticulada, ineficaz, governamentalizada e sem crédito internacional e dos critérios de escolha das suas chefias, dos regimes de acesso do pessoal e de promoção nas carreiras; uma reestruturação normativa da ANS e a sua compaginação com as entidades homólogas da UE e da OTAN.

4 UMA SOLUÇÃO: A CRIAÇÃO DE UM CENTRO NACIONAL DE CIBERSEGURANÇA (CNC)

A criação de um Centro Nacional de Cibersegurança, no cenário descrito, passa a ser uma prioridade estratégica essencial e uma solução doméstica de segurança nacional adequada aos compromissos assumidos por Portugal na UE e na OTAN, em matéria de cibersegurança.

O CNC é uma estrutura de ciberforça[22] necessária para dar segurança ao ciberespaço e gerar a confiança dos cidadãos no seu uso pessoal – na necessidade de comunicar, fazer negócios e aceder a informações – e pelo Estado e as suas instituições nas suas relações com os cidadãos.

O CNC deve ser uma estrutura leve, pequena e aberta[23], não reconduzível a um lugar ou infraestrutura física, mas altamente sofisticada

---

[22] Ver: STARR, Stuart; KUEHL, Daniel; PUDAS, Terry. Perspectives on building a cyber force structure. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 163-181.

[23] No sentido de não permitir que a rigidez dos procedimentos, os preconceitos instalados e o cumprimento estrito de regras ou a observância de práticas instaladas na rotina decisória, afaste a análise de novas atitudes e a necessidade de rever estratégias, acessos e compromissos. Um dos temas mais discutidos actualmente é a de enquadrar os "*hackers* patriotas" nas estruturas estaduais de cibersegurança para enfrentar perigosas cibermilícias de amadores que atacam com eficácia as infraestruturas críticas do Estado. Ver: OTTIS, Rain. From pitchforcks to laptops: volunteer in cyber conflicts. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 97-109.

na conexão em rede, na harmonização de procedimentos, na disciplina conceptual, no estado permanente de prontidão, além de criativa e inovadora nos planos científico, tecnológico, cultural e educativo, com uma articulação transdisciplinar e uma coordenação uniforme ao nível da excelência dos titulares de cargos e responsáveis pelas decisões.

Como centro que protege as nossas infraestruturas, o CNC pode oferecer aconselhamento especializado, gratuito e rápido, para reduzir a vulnerabilidade das organizações, empresas e pessoas na infraestrutura nacional face às ameaças vindas do ciberespaço.

O objectivo é constituir parcerias com entidades do sector privado, organismos públicos e associações profissionais, com o fim de criar, em rede alargada, um ambiente de confiança em que as informações confidenciais podem ser partilhadas com benefícios para cada um e para todos. Assim se consegue também a partilha das melhores práticas.

A organização de um conselho de pensadores ajuda à inovação necessária, criatividade na detecção de vulnerabilidades e ameaças, capacidade crítica do que existe e de conexão de factos e informações, além da criação de normas, doutrinas e práticas com rigor conceptual e densidade teórica.

Para cumprir os seus objectivos e metas, no âmbito de uma resposta nacional/estadual, face ao quadro actual atrás descrito, o CNC não pode ser uma estrutura do governo, isto é, não pode haver uma coincidência, seja ela qual for, entre o CNC ou o CSIRT nacional e o CSIRT governamental.[24]

Em Portugal, as pressões serão muitas para que assim seja, basta olhar para o nosso passado recente e para o êxito de retóricas bem colocadas junto da opinião pública e do eleitorado[25]. Existem, no

[24] O CSIRT governamental tem a responsabilidade de proteger as redes de comunicação e informação governamentais e da sua Administração Pública.

[25] Vai ser dito pelo poder político que num país pequeno e pobre outra qualquer solução será um desperdício de recursos que podiam ser aplicados nos desempregados, nas escolas e nos hospitais, numa demagogia conhecida mas normalmente aplicada com êxito, visando o controlo partidário da coisa pública. Depois aparecerá na TV, na rádio e nos jornais a figura do especialista, coberto de neutralidade académica, com as evidências científicas e as certezas tecnológicas ao serviço destas ideias, à espera que o senhor ministro se recorde das suas intervenções e grato o nomeie para uma comissão, um grupo de trabalho ou algo mais. Um discurso anunciado como aberto mas completamente fechado e recheado de "eficiências, sinergias, operacionalidades, rentabilidades, proactividades" e tudo o que nada explica ou resume.

entanto, razões nacionais para optar por uma solução política estadual, não governamental, na estrutura de cibersegurança portuguesa, através de uma legislação simples e clara, assente em regras de direito.

O CNC congrega os CSIRTs (*Computer Security Incident Response Teams*)[26] existentes nos sectores definidos como elementos da rede nacional de infraestruturas críticas do país ou, de forma mais alargada, às redes classificadas; garante a troca de informações e a harmonização de conceitos, doutrinas e normas em que assentam as boas práticas da prevenção, detecção e resposta a incidentes e ataques no ciberespaço; permite estruturar as medidas preventivas adequadas no âmbito dos serviços de informação e de segurança; dá unidade de comando na coordenação internacional e funciona como ponto único de contacto em Portugal (PoC – *point of contact*) à OTAN e à UE.

O CNC mantém a sua eficácia (mecanismos de dissuasão; detecção e resposta a incidentes e ataques; capacidade de recuperação; avaliação de ameaças) com a conjugação de rotinas funcionais; criatividade e inovação tecnológica; actualização doutrinal e especulação teórica; e exercícios permanentes com os vários níveis de alerta; educação e sensibilização da comunidade para as questões implicadas na cibersegurança.

Só assim pode a CNC, coordenado pela ANS, responder por Portugal, no imediato, a um ataque ciber às infraestruturas críticas ou às redes classificadas do país, esperando depois a cooperação dos seus aliados e das organizações internacionais de que faz parte.[27]

---

[26] Também designados como CERTs (*Computer Emergency Response Team*). Embora se possa entender que os CERTs, surgidos primeiramente como equipas de resposta a incidentes informáticos, deram lugar aos CSIRTs, com maior incidência na prevenção e com uma maior abrangência de acção/reacção – ambas são equipas de especialistas que se reúnem com o fim de prevenir incidentes e responder recuperando os estragos feitos na segurança dos computadores e das redes. Entendemos, por isso, que pode manter-se a distinção designativa, agora com outra função: deve ser usada a sigla CERT para as equipas principais, que estão no topo de outras, e que integram o CNC; e CSIRTs, pelo seu pendor sectorial e mais reduzido, para as equipas cuja missão é a de proteger redes departamentais classificadas integradas nos CERTs que estão no CNC,. Diferente são os CIRCs (*Cyber Incident Response Capability*).

[27] Não nos é permitido esquecer a exiguidade do Estado português e a sua dependência actual em matéria de defesa e de segurança. Ver os estudos publicados em: HÖLL, Otmar (Ed.). Small states in Europe and dependence. Wien: W. Braumüller; Laxenburg, Austria: Austrian Institute for International Affairs, 1983.

5 O FINANCIAMENTO DE UM CNC É UMA QUESTÃO POLÍTICA

As estruturas de economia de mercado existentes nos estados que integram a UE e a OTAN não permitem pensar o financiamento de um CNC apenas a partir de verbas do OE ou sem as considerar. A questão dos custos da ciberprotecção[28] é mais política que económica. Os montantes implicados estão relacionados com os níveis tecnológicos envolvidos e estes com as vulnerabilidades existentes, as ameaças previstas, a organização burocrática do estado e a coesão político-social da comunidade.

A crise que em 2008 assolou as estruturas de um capitalismo centrado nos jogos financeiros obriga-nos a pensar em novos modelos de organização do financiamento da segurança comum, aproveitando o sentido pragmático dos decisores que dão prioridade ao dinheiro e a necessidade de submeter tais decisões a princípios institucionais e a critérios racionais ao serviço da comunidade, não de certos indivíduos.

A história do período de liberalização económica pautada pelas teses do egoísmo individualista oriundas dos homens da Revolução Industrial de matriz inglesa mostra a insustentabilidade do pensamento que sustenta tal ideologia predatória no confronto com a realidade quotidiana das massas famintas que sustentam o luxo e o desperdício dos seus "donos" na política e na empresa.

O *crash* de Wall Street em 1929 trouxe o falhanço do sistema de mercado "puro e duro" ao interior da nação que assentava os seus sonhos imperiais no *marketing* político deste modelo económico. A miséria da maioria era o resultado desta ausência de política e de estado na economia.

A reacção poderia ter sido brutal mas foi sendo atenuada pela corrupção dos sindicalistas, e a ajuda de Estaline e de Hitler permitiram a continuidade do sistema por outros meios, disfarçando e torcendo o que de pior existia na desumanização provocada por um governo que se funda no interesse dos empresários.

Erguendo o comunismo como inimigo externo (mackartismo), com a bandeira de uma liberdade individual erguida em direito absoluto, promovendo a violência interna contra as minorias raciais, sexuais e de género, em modelos de autodefesa armada de cada cidadão com

[28] Ver: KIRT, Toomas; KIVIMAA, Jüri. Optimizing IT security costs by evolutionary algorithms. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 145-160.

prejuízo claro para a credibilização pública das instituições estaduais e com a ajuda de um "Plano Marshall" (criteriosamente preparado nos bombardeamentos selectivos da II Guerra Mundial) que colonizaria a Europa por muitas décadas, os EUA aceitaram a infâmia do ataque nuclear sobre Hiroshima e Nagasaki, capturaram o sistema económico e político internacional (Breton Woods; ONU) e garantiram *manus militari* o seu interesse nacional nas áreas que definiam como "suas".

A socialização do capitalismo não resultou da ameaça do sovietismo de pendor marxista-leninista, mas das pressões internas e das cedências necessárias e no limite para garantir a sobrevivência possível. As doutrinas de Keynes e de Beveridge sobre o reforço do papel do Estado não podiam resultar numa comunidade como a norte-americana, onde o poder político está completamente dominado pelos donos do dinheiro.

Estava facilitada a tarefa dos defensores da liberdade absoluta para os mercados, impondo-se a lei do mais forte. O estado mínimo de Reagan e Thatcher trouxe uma nova e mais agressiva, também mais dissimulada, forma de imposição imperial abrindo as portas ao capitalismo digital, sem fronteiras e de língua inglesa.

Na Europa os maiores adversários do imperialismo anglo-saxónico, pela via digital, na versão Reagan-Thatcher, eram os sistemas de social-democracia, onde o estado social respeitava as liberdades pessoais promovendo a coesão social através de um conjunto de instrumentos financeiros assentes na progressividade dos impostos e na igualdade/universalidade no acesso aos serviços públicos, mantendo a soberania dos Estados nas organizações internacionais.

Foi, por aí, no financiamento de partidos, fazedores de opinião e meios de comunicação social com a missão de descridibilizar as ideias que permitem o estado social e os titulares do serviço público, culpando o Estado social pela despesa pública em mensagens simplistas – tipo *spot* publicitário – para eleitorados analfabetizados pelos poderosos meios de entretenimento *made in USA* e pelas reformas de ensino impostas com o mote da rentabilidade económica pensadas para promover a ignorância e indiferença – na desarticulação desses instrumentos.

Na Europa, a transição do modelo europeu para o modelo americano foi apresentada, fora do continente, sob a forma de uma solução pragmática, sem ideias ou projecto de futuro, na terceira via de Tony Blair, ele próprio um produto artificial, só possível numa Europa onde as ideias norte-americanas se impõem sem oposição digna desse nome – pela falência dos modelos que se lhe procuram opor; pela falta

de criatividade dos opositores; e pela desigualdade de armas no acesso ao público.

O modelo capitalista financeiro revela a sua flexibilidade e adaptação, num instinto único de sobrevivência, ao colocar Barack Obama na Presidência dos EUA, a culminar uma campanha política que anunciando a ruptura, garante, mais uma vez, com sacrifícios mínimos dos mais ricos, a manutenção do *status quo* vigente.[29]

Obama não desiludiu e, com uma cosmética bem propagandeada de pequenas e inócuas alterações, manteve o grande filão institucional (interno e internacional) que mantém o capitalismo financeiro como centro de decisão política, com muitas bandeiras e muita encenação patriótica na camuflagem de um imperialismo com rosto adequada à nossa época (o de Obama). A segurança continua a ser matéria de militares e de polícias; não uma função essencial de cidadania – como só pode ser quando se encara a segurança como coisa do estado-instituição – não do estado-comunidade.

a americanização do mundo pela via digital, agora na versão messiânica do obamismo (nova estrutura que garante a continuidade da supremacia americana no Mundo) não serve os interesses da Europa, ainda menos do Mundo, nem da sua defesa colectiva, por mais que os diplomados europeus com bolsas americanas e os "novos universitários" saídos dos *curricula* de Bolonha repitam a identidade de ameaças comuns e a inelutabilidade da nossa defesa depender dos EUA.

Para manter a aliança estratégica entre a Europa e os EUA, e importa mantê-la, é preciso identificar as actuais divergências e realinhar as políticas. Por exemplo: a Rússia não é hoje um inimigo da Europa, por mais que os EUA e os seus seguidores na UE tentem engendrar ameaças russas à liberdade dos europeus; existem convergências e divergências de interesses impostos pela reorganização do terrorismo dos radicais islâmicos, no interior da Europa e nos teatros de guerra do Afeganistão e do Iraque; África não pode cair numa neocolonização, após as fracassadas experiências de socialismo totalitário, como resulta da actual estratégia dos EUA definida para o continente africano (sobretudo em torno da África do Sul, Nigéria e Angola e com a criação do AfriCom).

[29] Para uma visão diversa sobre o futuro do capitalismo, ver: KALETSKY, Anatole. Capitalism 4.0: the birth of a new economy in the aftermath of crisis. New York, NY: PublicAffairs, 2010.

Assim, as respostas em cibersegurança têm mais a ver com as culturas dos povos que resistem e conseguem dialogar e cooperar em igualdade de posições e em harmonia de princípios, que com as estratégias do Pentágono para essa resistência.[30]

Ao contrário dos EUA, a UE é uma união de Estados com história e independência política assentes na ideia de nação. Assim, a cooperação tecnológica e científica entre europeus e norte-americanos é fundamental; o diálogo político e cultural é necessário; a manutenção de pluralidades de modelos de resposta e respectivo financiamento, por respeito pela soberania decisória de cada Estado é essencial para a eficácia ao combate à insegurança cibernáutica.

A Europa deve, respeitando os modelos económicos de mercado que a caracterizam e a sua história de construção de um Estado social, com investimento público em políticas de defesa e de segurança, ligada aos sistemas de informações, garantir a eficácia de uma rede de Centros Nacionais de Cibersegurança, centrada na estrutura institucional de defesa e de segurança da UE e com uma ligação secundária, mas vital, à OTAN, combinando financiamentos públicos e privados: os primeiros, para o funcionamento; os segundos para o investimento.[31]

6 O PRESSUPOSTO COLOCADO PELO DIREITO: A PARTILHA DE VALORES E A CONFIANÇA

A questão jurídica envolvida na cibersegurança é complexa e requer um conjunto de especializações e uma interdisciplinaridade que coloca o tratamento jurisprudencial do tema numa fase ainda muito embrionária.

Pelo Direito a segurança não é uma questão de ordem mas de cumprimento de expectativas legítimas, de respeito pelas funções do Estado e de justiça na intervenção dos poderes públicos. Por isso, em

[30] Basta trabalhar com norte-americanos em matéria de segurança para saber que a igualdade de tratamento e o respeito pelas posições e pela cultura dos outros não são o seu forte no relacionamento bilateral, ou mesmo multilateral.

[31] Entendemos, por isso, que o financiamento do CNC deve ter na base dinheiros público, via Orçamento de Estado no âmbito da Conselho Superior da República, destinado ao seu regular funcionamento; e financiamento privado para a prestação de serviços em áreas estratégicas para os privados e nos investimentos necessários para a sua actualização, criatividade e autonomia científica e tecnológica, sobretudo na previsão de ameaças.

Direito a segurança comum do ciberespaço pressupõe identificar os valores que partilhamos como comunidade; só depois os conceitos, os institutos, as instituições e as regras que constituem, em cada Estado, o corpo normativo-institucional da cibersegurança.

Daí que antes de passar para a positivação de regras em tratados e em convénios internacionais – e é já muito significativo e até caótico o conjunto de regras e procedimentos aprovados pelas organizações europeias e internacionais sobre a cibersegurança – importa criar um clima de confiança (*fides*) sem a qual nenhuma regulação jurídica subsiste e qualquer previsão de sanções é inútil porque se torna inaplicável.

REFERÊNCIAS

BENEDIKT, Michael. *Cyberspace*: first steps. Cambridge, Mass.: MIT Press, 1991.

GIBSON, William. Neuromancer. New York: Ace Books, 1984. (20th anniversary ed. New York : Ace Books, 2004).

GREAT BRITAIN. Department for Business, Innovation and Skills (BIS); Department for Culture, Media and Sport (DCMS). *Digital Britain*: the final report 2009 (Cm 7650). London: The Stationery Office (TSO), 2009. Disponível em: <www.official-documents.gov.uk/document/cm76/7650/7650.pdf>. Acesso em: 10 jan. 2011.

GREAT BRITAIN. Cabinet Office. *The national security strategy of the United Kingdom*: update 2009: security for the next generation (Cm. 7590). London: The Stationery Office (TSO), 2009. Disponível em: <http://www.official-documents.gov.uk/document/cm75/7590/7590.asp>. Acesso em: 10 jan. 2011.

HÖLL, Otmar (Ed.). *Small states in Europe and dependence*. Wien: W. Braumüller; Laxenburg, Austria: Austrian Institute for International Affairs, 1983.

JOUBERT, Vincent. Getting the essence of cyberspace: a theoretical framework to face cyber issues. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 111-125.

KALETSKY, Anatole. *Capitalism* 4.0: the birth of a new economy in the aftermath of crisis. New York, NY: PublicAffairs, 2010.

KAMINSKI, Ryan T. Escaping the cyber state of nature: cyber deter-

rence and international institutions. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 79-94.

KIRT, Toomas; KIVIMAA, Jüri. *Optimizing IT security costs by evolutionary algorithms*. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 145-160.

OTTIS, Rain. From pitchforcks to laptops: volunteer in cyber conflicts. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 97-109.

STARR, Stuart; KUEHL, Daniel; PUDAS, Terry. Perspectives on building a cyber force structure. In: CZOSSEK, C.; PODINS, K. (Eds.). *Conference on Cyber Conflict Proceeding, 2010*. Talinn, Estonia: CCD COE Publications, 2010. p. 163-181.

WOLFERS, Arnold. "National security" as an ambiguous symbol. *Political Science Quarterly*, v. 67, n. 4, p. 481-502, dec. 1952.