idn nação e defesa

CIBERSEGURANÇA

idn Instituto da Defesa Nacional

nº 133

NAÇÃO E DEFESA
Revista Quadrimestral

Núcleo de Edições	***Colaboração***	***Capa***
Cristina Cardoso e António Baranita	Luísa Nunes	Nuno Fonseca/nfdesign

Normas de Colaboração e Assinaturas
Consultar final da revista

Propriedade e Edição
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Composição, Impressão e Distribuição
Imprensa Nacional – Casa da Moeda, SA
Av. António José de Almeida – 1000-042 Lisboa
Tel.: 217 810 700 E-mail: editorial.apoiocliente@incm.pt www.incm.pt

ISSN 0870-757X
Depósito Legal 54 801/92
Tiragem 1 000 exemplares
Anotado na ERC

Extra Dossiê

O processo de acelerada globalização a que temos assistido nas últimas décadas trouxe vantagens conhecidas: milhões de pessoas em todo o mundo saíram da pobreza; temos hoje acesso a bens de consumo impensáveis há poucos anos; viajamos e comunicamos com mais facilidade; fazemos trocas comerciais ao minuto e podemos investir em qualquer parte do mundo. Em suma, as novas tecnologias da informação aproximaram economias, regiões e culturas.

A internet – produto da revolução científica e tecnológica que acompanha a globalização – tornou-se um instrumento absolutamente central para o desenvolvimento deste processo. Mas essa centralidade, ao mesmo tempo que traz potencialidades, também comporta riscos, com implicações em todas as áreas – desde logo para a segurança e defesa nacionais.

Neste ambiente estratégico, a análise e a ponderação sobre as opções a tomar não pode perder de vista as interações que existem entre o processo de globalização, os "*Global Commons*" – que são os espaços comuns onde esta funciona –, e as políticas de segurança e defesa nacionais.

A importância estratégica do ciberespaço foi bem evidenciada por Barry Posen. Este professor de ciência política do MIT elege o ciberespaço como um novo "*Global Common*", a juntar aos já tradicionais espaços comuns: as águas internacionais; o espaço aéreo internacional; e o espaço exterior. Posen define estes espaços comuns como "os espaços que não estão sob o controlo direto de qualquer Estado mas que são vitais para o acesso e ligação a quaisquer pontos do mundo". E atribui os fundamentos da hegemonia dos EUA à capacidade de controlarem os "*Global Commons*".

Nestes espaços assentam todas as redes de telecomunicações vitais, de transporte e de distribuição de energia das quais dependem o comércio global, a segurança energética e a prosperidade das sociedades modernas.

Segundo dados citados pelo Departamento de Defesa dos Estados Unidos da América, de 2000 para 2010 o número de utilizadores da internet passou de 360 milhões para 2 mil milhões de pessoas. O ciberespaço está aberto a quem quiser e comporta riscos em larga escala. Não se trata apenas de ataques de "*hackers*", de ações de propaganda extremistas e do crime organizado, já de si graves, mas também do apoio a ataques terroristas, como vimos tragicamente há dez anos, em Nova Iorque e Washington, e de ações ilegítimas de outras entidades estatais, como sucedeu recentemente na Estónia e na Geórgia.

De facto, a internet é a arma por excelência dos conflitos assimétricos (estatais e não estatais) que caracterizam a nossa era da informação: está acessível a todos e os seus efeitos podem ser tão demolidores como os das guerras clássicas. Como escreveu o General Loureiro dos Santos sobre o ciberespaço, "ao mesmo tempo que se tornou indispensável nas sociedades modernas, ele transformou-se numa das suas maiores vulnerabilidades atuais". O ciberespaço "favoreceu o militarmente fraco contra o militarmente forte, fazendo com que o conflito assimétrico assumisse o papel que nunca teve, mesmo entre atores fortemente desequilibrados em termos de poder."

Não surpreende, por isso, que a NATO, no seu novo conceito estratégico eleja como uma das maiores ameaças a competição e a denegação do uso do ciberespaço, enquanto espaço comum, face à crescente sofisticação dos ataques cibernéticos e aos danos que podem infligir no funcionamento dos sistemas dos governos, dos negócios, das economias, das redes de transporte e abastecimento e outras infraestruturas críticas.

E é neste sentido que, muitos países, a começar pelas grandes potências (mas também Estados de menores dimensões), estão a desenvolver "Políticas de Informação" e estratégias integradas com o objetivo de aumentar os seus recursos de informação, garantir a segurança e a proteção da sua infraestrutura de informação e potenciar o livre acesso e a utilização do espaço onde ela circula – o ciberespaço.

Nunca é demais lembrar que a internet é a base na qual assentam os sistemas de comunicação entre Governos, Forças Armadas, Serviços de Informações e de Segurança. Face ao espectro da ameaça, as infraestruturas críticas são um alvo potencial de ataques que, pela sua natureza disruptiva, poderão colocar em risco o normal funcionamento de um país e os interesses nacionais.

É este pano de fundo que torna indispensável a adoção, por parte dos Estados, de Estratégias de Informação devidamente enquadradas nas estratégias nacionais de segurança e defesa, que devem contemplar linhas de ação visando garantir a liberdade de ação no ambiente de informação e fazer face aos desafios colocados pela utilização segura do ciberespaço, com destaque para as relacionadas com a proteção das infraestruturas de informação críticas e com as estruturas e capacidades necessárias nos domínios da cibersegurança e da ciberdefesa.

A Informação e a Segurança do Ciberespaço perfila-se assim como um dos pilares de qualquer estratégia nacional no mundo contemporâneo. É por isso que esta é uma das linhas de investigação do IDN e é por isso que lhe dedicamos esta edição da *Nação e Defesa*. Ainda que não abrangendo todas as temáticas que estes pilares envolvem, o conjunto de artigos aqui reunidos vêm sensibilizar-nos para um conjunto de desafios que a sociedade da informação e do conhecimento comporta, e também alertar-nos para as vantagens que um qualquer ator, em especial os Estados, devem saber explorar neste mundo competitivo onde a informação e o conhecimento surgem como variáveis críticas.

Vítor Rodrigues Viana

Cibersegurança

Utopia, Liberdade e Soberania no Ciberespaço

José Pedro Teixeira Fernandes

Licenciado em Direito pela Universidade Católica, Mestre em Estudos Europeus, Doutor em Ciência Política e Relações Internacionais pela Universidade do Minho. Auditor do Curso de Defesa Nacional em 2003.

Resumo

Neste artigo são discutidos os desafios que o ciberespaço e o risco de ciberataques acarretam para a soberania do Estado e para a liberdade do cidadão. A utopia libertário-anárquica, que dominou nos primórdios da internet, está progressivamente a dar lugar a mecanismos de controlo e de afirmação da soberania estadual, nomeadamente através da criação de "fronteiras" no ciberespaço. Esta tendência, embora sob formas diferentes, pode detetar-se quer nos Estados autoritários, quer nas democracias liberais ocidentais. Encontra-se também na organização das forças armadas, através da criação de ciber-comandos, e nas OIG ligadas à segurança e defesa como a NATO, onde se passou a incluir ameaça de ciberataques no conceito estratégico.

Abstract
Utopia, Liberty and Sovereignty in Cyberspace

The author discusses the challenges that cyberspace and the risk of cyber attacks bring to statehood sovereignty and the freedom of the citizens. The libertarian-anarchic utopia, which dominated in the early days of the internet, is gradually giving way to mechanisms of control and affirmation of state sovereignty, including the creation of "borders" in cyberspace. This trend, albeit in different ways, can be detected both in authoritarian states and the western liberal democracies. It is also recognizable in the organization of the military by the creation of a cyber command. We also can find it in the IGO related to security and defense like NATO, which includes the threat of cyber attack in the new strategic concept document.

> "Governos do mundo industrial, vós sois uns gigantes enfadonhos de carne e aço, eu venho do ciberespaço, o novo mundo da mente. Em nome do futuro, peço-vos, a vós do passado, que nos deixem sós. Não são bem-vindos entre nós. Não têm soberania onde nos reunimos. Não temos governos eleitos, nem provavelmente iremos ter. Assim, eu dirijo-me a vós sem autoridade maior do que aquela que me dá a liberdade com que sempre falei. Eu declaro o espaço social global que estamos a construir naturalmente independente das tiranias que nos tentam impor. Não têm o direito moral de nos governar, nem têm métodos de coação que tenhamos verdadeira razão para temer."
>
> John Parry Barlow (1996)

Introdução[1]

No seu uso mais rigoroso, o termo "ciberespaço" – originalmente cunhado pelo escritor de ficção científica William Gibson na obra *Neuromancer* de 1984 (Till, 2011) –, designa hoje a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores. Num uso mais livre, a palavra tornou-se também uma designação conveniente para referir algo ligado à internet e às novas práticas sócio-culturais que lhe estão associadas. Pela sua própria natureza complexa e multifacetada, o ciberespaço, no referido sentido mais rigoroso do termo, é suscetível de uma abordagem multidimensional e de ser objeto de investigação a partir de disciplinas muito variadas. Para o seu estudo, convergem, entre outras, a perspetiva tecnológica, sociológica, jurídica, política, estratégica e de segurança. Este pode ser, também, objeto de estudo de forma mais geral, incidindo sobre questões transversais aos diferentes Estados, ou estudado, de forma mais focalizada, em questões específicas ligadas a uma realidade nacional. Neste artigo, a opção foi por uma ênfase numa perspetiva política – incluindo nesta aspetos estratégicos e de segurança –, associada a observações de enquadramento de tipo cultural-sociológico. Para além disso, a análise centra-se em aspetos transversais aos diferentes Estados, não considerando, especificamente, o caso português. Este é, sem dúvida, merecedor de uma análise própria que ultrapassa o âmbito limitado da abordagem que aqui nos propomos efetuar.

1 O autor agradece os comentários e sugestões efetuadas pelo *referee* anónimo, as quais contribuíram para valorizar a versão final do artigo.

Assim, o principal objetivo do artigo que a seguir se apresenta é avaliar em que medida a utopia libertário-anárquica dos primeiros tempos da internet está a dar lugar, a nível internacional, a crescentes mecanismos de afirmação da soberania estadual, nomeadamente à criação de "fronteiras" e de mecanismos de controlo do ciberespaço. O objetivo é também procurar avaliar em que medida a resposta securitária dos Estados ao crescente risco de ciberataques ou de uma ciberguerra, põe em causa a liberdade do cidadão. Para o efeito, são passados em revista casos de Estados autoritários (a China), mas também as tendências de domínio do ciberespaço que se encontram nas democracias liberais ocidentais, incluindo a sua principal organização de segurança e defesa coletiva (a NATO), onde a ameaça de ciber-ataques passou a ser parte integrante do seu último documento estratégico.

A Utopia Libertário-Anárquica[2] do Ciberespaço e os seus Críticos

Talvez nada exemplifique melhor a utopia libertária ou até de anarquia do ciberespaço, que o manifesto da autoria do ex-compositor de letras do grupo *rock* norte-americano, *Grateful Dead*, John Parry Barlow, *A Declaration of the Independence of Cyberspace* (1996). Nesse texto emblemático sustentou que os governos nacionais deveriam manter-se afastados do "novo mundo" acabado de criar. Estes não tinham o direito moral de o governar pelo que se deveriam abster de criar quaisquer imposições legislativas reguladoras do "espaço social global". Ainda segundo este, seria a própria comunidade *online* quem deveria formar o seu "contrato social" (numa alusão à ideia moderna de um contrato social, entre governantes e governados, teorizada por Locke e Rousseau no Iluminismo, a qual legitimaria o exercício do poder pelos governos). Nesta visão utópica, surgiria assim uma "nova civilização", mais humana e mais justa do que as criadas anteriormente, que eram dirigidas pelos governos.

Visto como lugar de realização do ideal libertário-anárquico, o ciberespaço tem, no supra citado manifesto de John Parry Barlow, uma proclamação imbuída de uma lógica "contracultural", no sentido que era dado à palavra nos anos 60 do século passado. Mas há outros protagonistas emblemáticos destes ideais, que adquiriram até maior notoriedade junto do grande público. No passado recente, embora por razões bastante diferentes, destaca-se o caso de Julian Assange, o principal criador do WikiLeaks (Leigh e Harding, 2011). Na ótica dos que se revêm

2 O título deste ponto (e do artigo) é livremente inspirado no livro de Nozick (1977) originalmente publicado em 1974.

nos ideais libertário-anárquicos este representa, provavelmente, não só um ativista carismático em prol de causas justas, como uma espécie de "mártir da transparência informativa", ou Némesis do secretismo, pela perseguição que os governos estaduais – sobretudo o dos EUA –, lhe têm movido.

Importa notar que a utopia libertário-anárquica do ciberespaço não gerou apenas uma onda de simpatia e a adesão entusiástica, difundindo-se através de "evangelizadores" carismáticos como Barlow ou Assange um pouco por todo o mundo. Como é normal nos fenómenos culturais e/ou políticos novos, deu origem, também, a dissidências e a algumas vozes críticas bastante cáusticas. Estas evidenciam os aspetos potencialmente negativos da revolução digital em curso. Neste contexto destaca-se Andrew Keen[3], um "evangelizador dissidente" da revolução digital que, de alguma maneira, condensa os principais argumentos dos críticos. Quais são, então, esses argumentos? Um primeiro é dirigido contra a própria utopia libertário-anárquica subjacente à internet, em especial à chamada Web 2.0., considerada como uma nova e perversa versão das clássicas utopias políticas dos séculos XIX e XX:

> "Desde a revolução francesa e russa até às revoltas contraculturais dos anos 60 e à revolução digital dos anos 90, temos sido seduzidos, repetidas vezes e texto após texto, pela visão de uma utopia política ou económica. Em vez de Paris, Moscovo, ou Berkeley, o grande movimento utópico na nossa época contemporânea situa-se em Silicon Valley, cuja grande sedução é verdadeiramente a fusão de dois movimentos históricos: o utopismo contracultural dos anos 60 e o utopismo técnico-económico dos anos 90. Aqui em Silicon Valley, esta sedução anunciou-se a si própria ao mundo como o movimento 'Web 2.0'."(Keen, 2006: 1).

Um segundo argumento crítico relaciona-se com o novo jargão associado à Web 2.0, que este considera ser uma linguagem absurda, herdada da contracultura *hippie* dos anos 60/70, agora embelezada e sofisticada numa fraseologia de tipo sociológico:

> "Termos de moda da antiga era dot.com – como *cool*, *eyeballs*, ou *burn-rate* – foram substituídos na Web 2.0 por uma linguagem que é, simultaneamente, ainda mais militante e absurda: conferir aos *media* dos cidadãos, democratizar radicalmente, esmagar o elitismo, redistribuição de conteúdos, comunidade autêntica… Este jargão sociológico, no passado uma preservação da contracultura *hippie*, é agora o léxico do novo capitalismo dos *media*." (Keen, 2006: 1).

3 Andrew Keen é um britânico ligado à nova economia que tem desenvolvido a sua atividade em Silicon Valley, na Califórnia, EUA.

Desenvolvendo as suas críticas, Keen argumenta que, em termos ideológicos, estamos perante uma fusão entre "o radicalismo dos anos 60 com a escatologia utópica da tecnologia digital". O resultado, ao contrário do que muitos supõem, poderá ser bastante negativo para a generalidade da sociedade. Isto porque a Web 2.0 está a abrir caminho àquilo que este chamou "o culto do amador"[4]. Desta forma estar-se-á a destruir o que usualmente se designa por "alta cultura"[5], bem como o conhecimento especializado, nas mais diversas áreas do saber. Este necessita de anos de formação e treino, não sendo compatível com a lógica "amadora" da Web 2.0. Keen (*ibidem*: 1) faz ainda uma curiosa comparação entre a atual utopia libertário-anárquica do ciberespaço e a bem conhecida utopia marxista da sociedade radicalmente igualitária, que marcou grande parte da luta política desde a segunda metade do XIX até finais do século passado:

> "Tal como Marx seduziu uma geração de idealistas europeus com a sua fantasia da autorrealização da utopia comunista, também o culto da autorrealização criativa da Web 2.0 seduziu toda a gente em Silicon Valley. O movimento faz a ponte entre os radicais da contracultura dos anos 60, como Steve Jobs, com a cultura contemporânea *nerd* do Google de Larry Page. Entre os extremos de Jobs e Page encontra-se o resto de Silicon Valley, incluindo comunitaristas radicais como Craig Newmark (da *Craigslist.com*), comunistas da propriedade intelectual como o professor de Direito da Universidade de Stanford, Larry Lessig, cornucopianos económicos como o editor da revista *Wired*, Chris "*Long Tail*" Anderson e novos mogóis dos *media* como Tim O'Reilly e John Batelle."

Ao contrário de distopias literárias bem conhecidas, como o *1984* de George Orwell, ou *Admirável Mundo Novo* de Aldous Huxley, onde a tecnologia permitia controlar a informação e a mente (era o caso do *Big Brother* no livro *1984*), o problema com a Web 2.0 poderá ser, paradoxalmente, o inverso. Keen configura um hipotético cenário de pesadelo provocado por uma superabundância de autores e de "informação". A consequência bizarra e extrema dessa hipotética ocorrência seria que, sendo todos autores, a audiência tenderia a desaparecer,

4 Estamos a referir-nos ao livro *The Cult of the Amateur: How Today's Internet Is Killing our Culture*, que Andrew Keen publicou no ano seguinte (2007).

5 A designação "alta cultura" refere-se normalmente a um conjunto de realizações culturais essencialmente no domínio das artes (arquitetura, pintura, escultura, música, literatura, etc.) tendencialmente consideradas os expoentes máximos de uma sociedade, de uma época histórica, de uma nação, ou até da própria humanidade. Supõe, implicitamente, a existência de realizações culturais mais elevadas do que outras, ou seja, a expressão só faz sentido por contraponto ao que não é "alta cultura". A conceção "elitista" que lhe está subjacente conflitua com a lógica pós-moderna do nivelamento dos saberes e com a ideia que "todas as culturas têm igual valor", difundida, sobretudo, pela via da antropologia cultural.

tornando-se o ato de não escrever, paradoxalmente, numa forma de rebelião quase kafkiana.[6]

O Controlo na Rede: a (im)Possível Realização da Distopia Orweliana?[7]

Em face das críticas anteriormente formuladas uma dúvida surge inevitavelmente: será plausível que a utopia libertário-anárquica da internet possa dar origem a uma espécie de distopia Orweliana? Será tal possibilidade um mero exagero especulativo, até por ser, em termos técnicos e políticos, algo inviável? Analisemos a questão nessa dupla faceta. Quando se fala de controlo e vigilância através da tecnologia, vem quase inevitavelmente ao pensamento a imagem do já referido sistema monstruoso imaginado por George Orwell. Neste, a liberdade e a privacidade do indivíduo eram completamente esmagadas e submetidas aos desígnios de um poder totalitário, que atuava como dono do corpo e da mente dos cidadãos. Quando este foi escrito, estávamos em 1948, numa era pré-internet, anterior à revolução digital das últimas décadas do século XX. Será que a evolução tecnológica posterior contribuiu para afastar o espectro do *big brother is watching you*, na famosa frase do *1984*? Ou, pelo contrário, a internet e a revolução digital potenciam (ainda) mais a implementação de mecanismos orwelianos de vigilância do cidadão? Conhecemos já a resposta de John Parry Barlow, secundada por outros, como por exemplo, Louis Rosseto, fundador da revista *Wired*, e a visão libertário-anárquica que lhes está subjacente. Estes encararam a internet e a Web como um promissor espaço de realização da utopia libertária, vendo a possibilidade de emergir no ciberespaço um "homem novo" e uma "civilização nova" à margem da "tirania" dos governos. Por outras palavras, algo à margem dos mecanismos tradicionais de poder e controlo do Estado.

Sejam quais tiverem sido as intenções dos criadores da internet – e, na grande maioria dos casos, estavam, de facto, próximas de ideais libertário-anárquicos que impregnavam a contracultura dos anos 60[8] –, quando olhamos para a evolução posterior deparamo-nos com uma imagem bastante mitigada. É inquestionável

6 *"In the Web 2.0 world, however, the nightmare is not the scarcity, but the over-abundance of authors. Since everyone will use digital media to express themselves, the only decisive act will be to not mark the paper. Not writing as rebellion sounds bizarre – like a piece of fiction authored by Franz Kafka. But one of the unintended consequences of the Web 2.0 future may well be that everyone is an author, while there is no longer any audience."* Keen (1996: 1-2).

7 Sobre a liberdade na internet e nos *media* digitais ver o relatório editado por Kelly e Cook (2011).

8 Sobre este assunto ver Turner (2006).

que o ciberespaço trouxe, de uma ou de outra forma, um espaço de liberdade, com alguns traços de anarquia à mistura. Na sua faceta mais benéfica, permite a expressão individual de gostos e preferências, facilita a troca de ideias, propicia o ativismo social e político. Esta é uma faceta facilmente observável, pelo menos nos Estados que se pautam por valores democráticos e admitem o pluralismo político e social. Todavia, em paralelo, existe também aquilo que pode ser designado como um "lado negro". Sob a capa do anonimato – por princípio possível nas sociedades democráticas –, o uso da internet tende a libertar também algumas das piores facetas do ser humano[9]. Para além disso, a própria difusão da internet e a digitalização da economia geram novas dependências, vulnerabilidades e riscos: o mais óbvio é o da possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de uma ciberguerra[10] envolvendo, direta ou indiretamente, atores estaduais (casos, por exemplo, da Estónia em 2007 e da Geórgia em 2008, envolvidas em conflitos com a Rússia)[11].

Neste contexto, importa notar que a possibilidade de aceder, sob anonimato, à rede, não é propriamente uma inevitabilidade ou fatalidade tecnológica, mas uma opção política e legislativa. Pelo contrário, utilizar a internet significa, quase sempre, deixar um "rasto", deixar uma "pegada" eletrónica. Esta pode ser usada comercialmente para detetar os gostos e preferências dos utilizadores por coisas mais ou menos inócuas como vestuário, comida ou vinhos; mas também por coisas que podem eventualmente já não ser tão inócuas como livros ou filmes dependendo, obviamente, do tipo de livros e filmes em questão; bem como outras, já muito menos inócuas, como gostos ou orientações sexuais, ou até nada inócuas como preferências político-ideológicas e causas sociais e políticas. Paradoxalmente, torna-se hoje mais fácil, e a custo mais baixo, fazer esse rastreio na internet do que no mundo real. Naturalmente que isto confere uma oportunidade de uso interessante, quer para as empresas, quer para os governos, sejam quais forem as intenções últimas desse rastreio.

9 O comentário insultuoso, a acusação gratuita e sem quaisquer provas, a opinião sem um conhecimento razoável, o rumor, a intriga, o plágio, a escrita de má qualidade, etc. ganharam igualmente um novo "espaço de liberdade" e de difusão.

10 No seu uso mais comum e livre, ciberguerra designa, vagamente, algum tipo de "ataque" ou "represália", intrusão ilícita numa rede e/ou computador ou uma situação de espionagem que ocorre usando meios informáticos. Tais situações poderão surgir, ou não, ligadas a conflitos políticos e/ou militares no mundo "real", ou seja, ocorrer em paralelo com uma conflitualidade "física" ou de forma totalmente autónoma (nesta última hipótese estaríamos perante uma ciberguerra "pura"). Por outro lado, poderão ter origem diretamente em Estados, ou, então, ser protagonizadas por atores não estaduais.

11 Sobre este assunto ver Klimburg (2011: 41-60).

O Caso da "Grande *Firewall* da China"

Em termos de seguir o "rasto" ou procurar a "pegada" eletrónica deixada pelos seus cidadãos o caso que, individualmente, mais chama à atenção é o da China, até pelo crescente impacto que o país está a ter na economia e na política mundial. Um curioso artigo de Oliver August (2007), publicado na revista *Wired*, retrata o *golden shield*/escudo dourado (também conhecido como *great firewall of China*/grande *firewall*[12] da China, num jogo de palavras com a grande muralha da China), que o país tem implementado internamente para vigiar o uso da internet. O seu objetivo é monitorar, filtrar e/ou bloquear conteúdos considerados sensíveis pelas autoridades chinesas. O sistema assenta num banco gigante de computadores e servidores a partir do qual se procura vigiar o tráfico gerado pelos 384 milhões de utilizadores[13] chineses da internet. Comentando a abordagem chinesa à revolução digital e os seus esforços de controlo e de vigilância na rede, Jack Goldsmith e Tim Wu (2006: 90), fazem notar que a visão típica da internet no Ocidente, como "espaço de liberdade", é apenas uma possibilidade, ou seja, é uma escolha social e política e não uma inevitabilidade que decorre da tecnologia[14]. Sobre a maneira como o sistema do *golden shield* foi posto em prática na China, estes mostram também o paradoxo de ter sido feito com a tecnologia de empresas norte-americanas – as quais, em teoria, se identificam com a democracia liberal e pluralista e atuam em respeito pelos seus valores:

> "A barreira de informação da China foi fundamentalmente construída pela Cisco, e empresa fornecedora de redes de Silicon Valley. No início dos anos 90, a Cisco e outras empresas desenvolveram produtos para deixar as empresas americanas filtrarem o acesso dos seus empregados à internet. As empresas queriam a internet, mas não queriam os seus empregados no ESPN ou na playboy.com, todo o dia. A Cisco demostrou há muito tempo às autoridades chinesas como os mesmos produtos poderiam ser usados para bloquear, de forma eficiente, materiais de entrarem na China. Mostrou como isso poderia ser feito de forma flexível, subtil e sem perda de *performance*. Por isso, a moderna "grande muralha China" é, com efeito, construída com tijolos americanos." (Goldsmith e Wu, 2006: 93)

12 Literalmente "parede corta-fogo".

13 Ver Internet World Stats (s.d.).

14 *"China is not only an extreme example of control; it is also an extreme example of how and why the internet is becoming bordered by geography. Only time will tell whether the China strategy will work, or whether the sheer volume of information will erode the government's influence and render the internet in China open and free. But so far, China is showing the opposite: that the internet enjoyed in the West is a choice – not fate, not destiny, and not natural law."* Goldsmith e Wu (1996: 90).

Para além disso, estes chamam também a atenção para o facto de o sistema de vigilância da internet da China não só ser subtil e sofisticado, como bastante mais eficaz do que se poderia pensar à primeira vista (*ibidem*: 94):

> "A censura chinesa é não só eficiente como também subtil. Não aparece nenhum écran a dizer "bloqueado pelo Estado Chinês." Em vez disso, o bloqueio assume a aparência de um erro técnico. Um utilizador que tente, por exemplo, aceder a free-china.net, encontrará um ecrã a dizer "*site* não encontrado", um écran de tempo de acesso de rede esgotado, ou um dos muitos códigos HTTP de erro. E pode ser difícil para um utilizador final (e investigadores) saber se o problema é de facto censura ou dificuldades técnicas. A lista mandatada de *sites* bloqueados muda à medida da evolução dos acontecimentos. Por exemplo, por vezes o *website* do *New York Times* está acessível nos computadores da China, outras vezes não está**.** Esta incerteza, ligada à falta de fiabilidade geral da internet, ajuda a mascarar os esforços de censura."

Quer dizer, o caso da China mostra claramente que a ideia da internet como espaço de (não) liberdade é, na sua essência, uma opção social e política e não uma "fatalidade" tecnológica. Não existe qualquer inevitabilidade de liberdade que decorra da própria tecnologia por esta utilizada. A consequência inevitável é que diversos cenários sobre a sua evolução futura, entre os quais o da perda de liberdade, estão necessariamente em aberto.

Rumo a uma Era de "Afirmação Vestefaliana" no Ciberespaço?

Uma das questões mais importantes sobre o futuro da internet é a de saber se os Estados vestefalianos irão afirmar, crescentemente, a sua soberania sobre o ciberespaço, ou se este se manterá um feudo libertário-anárquico, à margem poder do Leviatã[15] (Estado), como imaginaram muitos dos pioneiros. Será o referido caso da "grande *firewall* da China" a exceção constituída por um grande Estado

15 Referimo-nos, naturalmente, à obra de Thomas Hobbes, *Leviatã* (1651), cujo título evoca um monstro da mitologia da Antiguidade, dotado de uma força sobre-humana. Esta foi a metáfora usada por este pensador político britânico no século XVII para justificar a necessidade do poder do Estado. De facto, Hobbes via no estado de natureza não só um estado de máxima liberdade dos indivíduos, como também um estado de máxima insegurança e conflito. A nota dominante que o caracterizava era anarquia marcada pela "guerra de todos contra todos" (*bellum omnium contra omnes*). Por isso, Hobbes considerou que seria do interesse da generalidade dos indivíduos formar uma sociedade e aceitar uma espécie de "contrato social". Só através deste processo se poderia obter uma pacificação social e a segurança contra os inimigos internos e externos. Assim se justificava não só a existência do Leviatã (o Estado soberano) como, no contexto da época, o exercício de um poder tendencialmente absoluto.

capitalista autoritário[16]? Será antes revelador de uma tendência mais geral, de afirmação crescente do poder estadual, a qual ultrapassa a lógica do autoritarismo político? Em resposta a esta questão, Chris Demchak e Peter Dombrowski em *Rise of Cybered Westphalian Age* (2011), sustentam que está em marcha um processo de afirmação do poder dos Estados sobre o ciberespaço. Estes antecipam mesmo uma nova era de "afirmação vestefaliana" vista, em termos valorativos, como uma tendência necessária e desejável. Na sua ótica (2011: 32), estamos já hoje a assistir ao "início de um processo de criação de fronteiras". Este processo tem múltiplas facetas que vão desde "a tentativa chinesa de criar a sua própria internet, interna e controlada, até ao aumento dos filtros e das regras da internet nas democracias ocidentais". Isto denota uma tendência de os Estados estabelecerem "os limites do seu controlo soberano no mundo virtual, em nome da segurança e da sustentabilidade económica".

Demchak e Dombrowski consideram que o processo histórico que levou à afirmação do Estado soberano encerra uma analogia útil para se perceber a atual tendência de afirmação do poder de soberania sobre o ciberespaço. Assim, importa aqui recordar o conceito histórico de soberania, originalmente teorizado pelo francês Jean Bodin em finais do século XVI, numa obra intitulada *Les Six Livres de la République* (Bodin, 1993). A soberania foi apresentada como um poder, ou seja, a faculdade de impor aos outros um comando a que estes devem obediência. Tal poder revestia o caráter de um poder perpétuo, ou seja, sem limites de natureza temporal, dando substância ao princípio da continuidade do Estado que permanece para além das eventuais mudanças de regime político, ou de governo. Este poder era também absoluto, não estando a soberania sujeita a quaisquer condições ou limitações impostas por outrem. Quer dizer, o detentor da soberania não estava sujeito a instruções de ninguém nem era responsável perante nenhum outro poder[17].

Em termos de características, esta foi apresentada como sendo indivisível (de forma claramente contrastiva com a fragmentação política medieval); como sendo própria e não delegada (na conceção original de Bodin esse poder próprio não pertencia ao povo ou à nação – formulação que só apareceu mais à frente, no séc. XVIII –, mas ao monarca e não estava dependente nem de um processo eletivo nem de nomeação pelo Papa ou Imperador); como sendo irrevogável (nem o Papa, nem o Imperador, nem o povo ou nação poderiam retirar ao soberano esse poder político máximo). Além de tudo isto, a soberania era vista também como sendo suprema na ordem interna, quer dizer, representando um poder que

16 Ver o artigo do académico israelita Azar Gat (2007).

17 Na conceção original de Jean Bodin o poder de soberania pertencia ao monarca por direito próprio. Para mais desenvolvimentos sobre o pensamento político de Jean Bodin, ver Amaral (1998).

não podia admitir outra igual com o qual tivesse de partilhar a autoridade do Estado. Por sua vez, no plano internacional, era caracterizada como sendo uma expressão de plena independência, só lidando o Estado soberano com outros poderes iguais (no contexto da época, o Estado soberano só estaria vinculado pelas normas de Direito Internacional Público resultantes de tratados livremente celebrados com outros poderes soberanos iguais, ou de costumes internacionais voluntariamente aceites).

Obviamente que o conceito de soberania evoluiu bastante desde a teorização de Jean Bodin. Hoje, por um conjunto diversificado de razões – regime dos Direitos Humanos, organizações de integração económica e política para as quais são transferidas competências soberanas, etc. –, tende a ser entendido de forma bastante mais matizada e limitada. Em *Sovereignty: Organized Hypocrisy*, Stephen Krasner (1999) dá-nos uma panorâmica da sua evolução até ao mundo político contemporâneo. A análise foi efetuada numa perspetiva abrangente (histórica, política e jurídica) e colocou em evidência as múltiplas aceções em que este pode ser encarado (soberania interna, soberania interdependente, soberania legal internacional e soberania vestefaliana).

Quadro 1 – As Aceções do Conceito de Soberania segundo Stephen Krasner

Soberania interna	Soberania interdependente	Soberania legal internacional	Soberania vestefaliana
Organização da autoridade pública no seio de um Estado ligada ao controlo efetivo exercido pelos que detêm a autoridade	Capacidade de as autoridades públicas controlarem os movimentos transfronteiriços (de pessoas, bens, ideias, doenças, poluentes, etc.)	Estabelecimento do *status* de uma entidade política no sistema internacional através do reconhecimento mútuo dos Estados (regulação das relações interestaduais baseada no princípio da igualdade jurídica)	Exclusão dos atores externos da configuração e do exercício da autoridade interna (princípio da não ingerência externa nos assuntos internos dos Estados)

Fonte: José Pedro Teixeira Fernandes (2009: 103).

Krasner desmistificou também algumas ideias bastante em voga, não só no discurso mediático como na própria academia. Estas surgiram ligadas ao entusiasmo à volta da globalização, típico dos primeiros anos da última década do século passado, sugerindo, pelo menos até à crise financeira iniciada em 2007/2008, que estaríamos perante uma progressiva e inexorável perda de poder do Estado

soberano[18]. Naturalmente que há fenómenos contemporâneos que colocam sob tensão a ideia clássica da soberania do Estado, os quais não existiam na época em que Bodin teorizou. É inquestionável que estes desafiam, sob diversos moldes, o poder estadual soberano. Inserem-se aqui as já referidas convenções internacionais sobre os Direitos Humanos, o Direito Internacional Humanitário, a integração económica e política regional nas suas diferentes formas, e a incontornável globalização. Todavia, o estudo de Krasner acaba por evidenciar também uma certa fragilidade existente na argumentação da "inexorável" perda de poder do Estado soberano. Em parte esta baseia-se no pressuposto de que, em termos histórico-políticos, teria existido até à atual globalização uma espécie de "idade de ouro" das soberanias. Durante essa "época dourada", a soberania estadual teria sido respeitada pela generalidade dos atores estaduais (e não estaduais) e não teria enfrentado constrangimentos de relevo. A verdade é que essa ideia não tem uma base histórico-política sólida – apenas tem alguma consistência para as grandes potências. Não é difícil no período posterior aos Tratados de Vestefália de 1648 encontrarmos exemplos de "atropelos" à soberania estadual, por vias coercivas e de imposições – daí a "hipocrisia organizada" de que fala Krasner. Para além disso, não parece ser também este o destino do Estado vestefaliano no mundo pós-11 de setembro de 2001, e, sobretudo, pós crise financeira de 2008. Pelo contrário, o que se deteta é uma tendência geral para uma (re)afirmação do poder soberano, sendo provavelmente o ciberespaço, que nos ocupa nesta análise, uma nova frente dessa (re)afirmação de poder.

18 Ideia ventilada, por exemplo, no livro de Ohmae (1996).

Quadro 2 – Os Desvios à Soberania Legal Internacional e à Soberania Vestefaliana

Convenções (desvio voluntário)	Contratos (desvio voluntário)	Coerção (desvio involuntário)	Imposição (desvio involuntário)
Acordos através dos quais os Estados se comprometem a seguir determinadas práticas que envolvem relações entre governantes e governados no interior das fronteiras estaduais; permitem a atores externos exercer alguma influência interna (por ex.: a Declaração Universal dos Direitos do Homem, de 1948 e a Convenção Europeia dos Direitos do Homem, que entrou em vigor em 1953)	São atos negociados entre dois ou mais Estados, ou entre um Estado e uma organização internacional (por ex. um empréstimo do FMI), revestindo nos casos mais importantes normalmente a forma de tratados internacionais (por ex. o Tratado de Utrecht de 1713, no qual a França cedeu a Arcádia e a Baía de Hudson à Grã-Bretanha)	Ocorre quando um Estado (ou Estados) ameaçam impor sanções a outro Estado, a menos que o coagido aceite limitar a sua autonomia interna e praticar o ato pretendido (ou abster-se de uma determinada conduta); para ter credibilidade e eficácia pressupõe uma assimetria de poder entre as partes envolvidas. Os casos mais claros de coerção envolvem a ameaça de sanções económicas, ou sua efetiva aplicação (ex.: as sanções impostas pelos EUA a Cuba, na sequência da ascensão de Fidel Castro ao poder, em 1959; as sanções autorizadas pela ONU à África do Sul, para pôr fim ao *apartheid*, entre 1962-1994)	Tem sido empregue em casos associados aos direitos das minorias, aos empréstimos a Estados soberanos e às estruturas institucionais dos Estados mais fracos (a ação norte-americana em 1989, em território do Panamá, que levou à detenção do general Noriega, presidente da república, e ao seu envio para os EUA onde foi julgado e condenado por narcotráfico; a ação da NATO na província Sérvia do Kosovo, em 1999, para proteger a minoria albanesa)

Fonte: José Pedro Teixeira Fernandes (2009: 104)

Voltando à análise de Demchak e Dombrowski, em termos histórico-diplomáticos estes referem-se aos já mencionados Tratados de Münster e Osnabrücke (conhecidos como a Paz de Vestefália), celebrados em 1648 e que colocaram fim à Guerra dos Trinta Anos na Europa. Esses Tratados constituem o marco simbólico da progressiva afirmação da soberania territorial, a qual decorreu ao longo dos séculos subsequentes. Esta tem uma expressão visível na delimitação precisa e cartográfica das fronteiras[19] estaduais. Note-se que a pacificação das zonas limite entre diferentes comunidades políticas, bem como a segurança das respetivas populações, favoreceu a aceitação deste processo e a afirmação da soberania territorial nos moldes previstos nos Tratados de Paz de Vestefália. Para Demchak e Dombrowski (*idem*: 40), os desafios de segurança do mundo de hoje voltam a colocar similares circunstâncias, agora num terreno novo que é o ciberespaço. Assim, estes consideram que "uma ciberfronteira nacional é tecnologicamente possível, psicologicamente confortável, sendo também sistematicamente e politicamente gerível". Em reforço deste argumento, afirmam que "técnicos excecionalmente dotados discutem a necessidade de separação de sistemas críticos para os proteger de predadores da internet e atores hostis". Como resultado, mesmo se os políticos estão normalmente "inclinados a manter uma internet totalmente aberta, terão poucos argumentos técnicos para usar" na sustentação dessa posição.

Mas há outros argumentos relevantes a favor da instituição de fronteiras nacionais no ciberespaço. Desde logo, estes fazem notar que, ao contrário das teses de alguns "evangelizadores" dos primórdios da internet, não estamos perante uma realidade física que funcione fora da vontade humana, tipo força da gravidade – algo que já tivemos oportunidade de demonstrar quando assinalamos que não há qualquer inevitabilidade que torne automaticamente a tecnologia numa área de liberdade. Por outro lado, chamam ainda a atenção para uma distinção particularmente importante. Em Estados democráticos, a ênfase relevante em matéria de afirmação da soberania estadual é colocada nas "fronteiras". Ou seja, o que está em causa não é um "controlo" generalizado dos fluxos eletrónicos que ocorrem dentro do próprio Estado (a verificar-se algo deste tipo estaríamos a abrir a porta a formas de vigilância e controlo autoritárias) mas, por razões de segurança externa, afirmar "fronteiras" da comunidade política (*ibidem*: 40):

> "(...) as fronteiras físicas são conhecidas, aceites e desejadas pelos cidadãos nas modernas sociedades civis e esse conforto psicológico não será diferente na criação de fronteiras no ciberespaço. A ênfase relevante é nas "fronteiras", não no controlo universal de todos os fluxos na rede ocorrendo inteiramente dentro das fronteiras de um Estado-Nação democrático. Historicamente, os cidadãos aceitaram as fron-

19 Para uma visão histórica e geopolítica do problema das fronteiras estaduais ver Foucher (1991).

> teiras como uma necessidade de reforço da segurança contra incertezas externas que pusessem em causa regras aceites internamente de interação. Sem tais limites, o sentido coletivo de pertença é mais facilmente subvertido tal como as regras de comportamento civil."

Um terceiro argumento por estes avançado, é o de que as "fronteiras cabem na arquitetura existente de gestão dos sistemas nacionais". A maioria dos Estados faz uma distinção entre forças que defendem as fronteiras de um ataque externo (militares) e aquelas que protegem cidadãos individuais de um ataque interno, normalmente com origem criminosa (polícia). Esta distinção, que historicamente "é um dos resultados diretos da ascensão do Estado moderno após a Paz de Vestefália", tem sido "severamente posta em causa pelo caráter irrestrito da atual tipologia do ciberespaço". Entre outros problemas, confunde a separação entre a esfera interna e esfera externa da segurança. Para Demchak e Dombrowski (*ibidem*: 43), uma evolução para "fronteiras virtuais" no ciberespaço contribuiria positivamente para clarificar esta questão. Em defesa da sua posição, apontam o recente caso do vírus *Stuxnet* que afetou as instalações nucleares iranianas:

> "(...) Sem a legitimação e a clareza burocrática de uma fronteira virtual, por exemplo, disputas jurisdicionais entre nações, que respeitaram séculos de diferenciação entre crime e segurança nacional, as leis da sociedade civil ficam paralisadas na resposta. O vírus Stuxnet facilmente atravessou as fronteiras conforme pretendido por aqueles que o criaram. Se foi um ator não estadual, então a ação é criminal, invocando o poder das forças policiais. Se foi um ator de nível estadual, então os militares deverão atuar. Hoje, não é claro que grupos estiveram envolvidos, em grande parte porque o rasto eletrónico de possíveis atribuições move-se rapidamente através dos Estados. Estes não têm obrigação de sancionar um mau comportamento emanando de fora do seu território."

Estas zonas cinzentas e vazios podem trazer oportunidades a explorar por atores estaduais e não estaduais. Todavia, a verdade é que muitos Estados começam a ver esta "incerteza e a dificuldade em estabelecer a culpa e atribuir a responsabilidade do ataque como vulnerabilidades inaceitáveis". Como sublinham Demchak e Dombrowski, "em princípio, apenas de territórios não governados ou ingovernáveis podem grupos modernos lançar mísseis destrutivos, sem um apelo interestadual automático para sanções. Com fronteiras físicas, os Estados que querem ser aceites internacionalmente estão obrigados por lei e costume a parar o comportamento atacante dos seus residentes ou a permitir ao Estado ofendido atuar no seu interior para fazê-lo parar. Uma vez que os limites virtuais do poder soberano possam ser demarcados no ciberespaço global, os Estados que ignorem ou apoiem ataques massivos de negação de serviço a partir dos seus territórios serão inter-

nacionalmente responsáveis" (*ibidem*: 44). Mas a afirmação da soberania estadual, através de fronteiras virtuais no ciberespaço global, tem ainda outra vantagem que consiste em identificar "maus territórios não governados", ou seja, o equivalente a regiões físicas de Estados falhados ou em vias de se transformarem em tal.

Como estão a surgir e em que Estados se pode observar a implementação de fronteiras nacionais no ciberespaço? Desde logo, há a referir o já mencionado caso da China, que lidera a abordagem, mas numa lógica de Estado autoritário. Quer dizer, a sua atuação não se restringe a uma afirmação de soberania nas suas fronteiras externas do ciberespaço, mas prossegue, paralelamente, um controlo generalizado dos fluxos eletrónicos com origem nos seus próprios cidadãos. Ainda na década de 90, o Partido Comunista Chinês "declarou a internet como sendo uma quinta área de territorialidade" a ser objeto de segurança nacional. Para além disso, nos últimos anos a China tem estado a trabalhar na sua própria internet – no que é designada por "Internet da Próxima Geração Chinesa – onde o "limitado número de endereços da internet se expande enormemente (IPv6), fornecendo a cada computador ligado à internet o seu único endereço Web". Como fazem notar Demchak e Dombrowski (*ibidem*: 45), este novo sistema de endereços é mais "amigo da vigilância" permitindo ao governo chinês, ou a qualquer outro governo que o deseje, efetuar um controlo das suas fronteiras, sem ter de usar agentes ou recorrer a outras entidades".

Fora do contexto de Estados autoritários, encontramos diferentes formas de afirmação da soberania nacional sobre o ciberespaço. Uma das mais usadas no contexto das democracias liberais é o modelo da "empresa-chave". Este modelo impõe algumas obrigações legais às maiores empresas de telecomunicações, com o intuito de diminuir atividades maliciosas ou fraudulentas na rede. Encontra-se, por exemplo, na Austrália, e, em certa medida, também na Alemanha. Outro modelo – representado pela abordagem do Reino Unido –, assenta numa atuação coordenada de diversas agências governamentais em áreas económicas e sociais, com o objetivo de encorajar, monitorar e guiar as transações internas na internet. Há também outras abordagens com um enfoque mais securitário e que têm surgido nestes últimos anos em vários países. Por exemplo, em 2008, no contexto da aprovação de medidas antiterrorismo, a Suécia adotou uma legislação que permite aos serviços de informações da polícia nacional "monitorar todo o tráfico para dentro e para fora do país, tendo origem, ou não, em cidadãos suecos" (*ibidem*: 47).

O Ciberespaço na Organização Militar e no Conceito Estratégico da NATO

A tendência para a afirmação da soberania nacional no ciberespaço está também a ter implicações a outro nível. As forças armadas e de segurança nacionais – uma das expressões inquestionáveis da soberania do Estado –, estão a tentar

adaptar-se aos desafios do ciberespaço e aos riscos de uma eventual ciberguerra. Neste contexto assiste-se, sobretudo entre as principais potências mundiais e regionais, a uma tendência para instituir um cibercomando[20] no âmbito das suas forças armadas ou de segurança interna. A opção pela sua institucionalização no âmbito das forças armadas converte-o no "marcador singular mais óbvio de uma fronteira emergente". Trata-se de criar uma organização de tipo militar destinada "a proteger a nação de danos que, historicamente, só outro Estado, ou vizinho, poderia infligir". Por sua vez, o ato de "estabelecer tal unidade e publicamente declarar tê-lo feito" significa afirmar explicitamente que "existe um território a defender" e que a ameaça de ciberataques pode ser vista como uma "ameaça existencial". No plano simbólico, o estabelecimento de um cibercomando marca também o reconhecimento "de um espaço detido nacionalmente que a nação valoriza e vai proteger usando os recursos apropriados disponíveis". O facto de as "fronteiras não terem ainda sido reconhecidas por outros Estados – um resultado-chave do longo processo vestefaliano –, não diminui o significado desta declaração institucional de soberania a ser defendida, por inerência, no próprio ciberespaço." A afirmação do ex-primeiro ministro britânico, Gordon Brown de que "no século XIX tivemos de tornar seguros os mares para a nossa própria segurança e prosperidade nacional, no século XX tivemos de tornar seguro o ar, e no século XXI temos de tornar segura a nossa posição no ciberespaço de forma a dar às pessoas e aos negócios a confiança que estes necessitam para aí operar", é, provavelmente, a que melhor capta a tendência que descrevemos (*ibidem*: 47-48).

Uma outra área onde a crescente perceção da possibilidade de ciberconflitos ou de uma ciberguerra está a ter repercussões é a dos documentos estratégicos de segurança e defesa, quer nacionais, quer de OIG vocacionadas para essas tarefas. Pela sua importância, merece aqui uma referência especial o caso da NATO[21], que continua a ter na segurança (militar) dos seus membros o seu objetivo último. De facto, a garantia de assistência mútua entre os Estados signatários, em caso de agressão externa, consagrada pelo artigo 5.º do Tratado de Washington, o texto fundador da organização em 1949, mantém-se como elemento-chave. Nesse artigo afirma-se que "um ataque armado contra uma ou mais partes do Tratado, na Euro-

20 Ver "Meet USCybercom: Why the US is fielding a cyber army" em BBC News. Acessível em http://news.bbc.co.uk/2/hi/technology/8511711.stm (15/3/2010). Ver também U.S. Department of Defence/United States Cyber Command. Acessível em http://www.defense.gov/home/features/2010/0410_cybersec/. Sobre o caso alemão ver Fischer e Reissmann (2011).

21 North Atlantic Treaty Organisation (NATO), na sigla em língua inglesa. Esta organização intergovernamental é designada tradicionalmente por Aliança Atlântica, evidenciando o facto de o Tratado de Washington reunir numa aliança militar a generalidade dos Estados da Europa Ocidental e da América do Norte.

pa ou na América do Norte será considerado como um ataque dirigido contra todas as partes". Verificando-se tal situação "cada uma delas, no exercício do direito de legítima defesa, individual ou coletiva, reconhecida pelo artigo 51.º da Carta[22] das Nações Unidas, assistirá a parte, ou as partes, atacadas". Consequentemente serão adotadas "individualmente e de acordo com as outras partes", as ações julgadas necessárias incluindo o "uso da força armada para restabelecer e assegurar a segurança na região do Atlântico Norte" (NATO, s.d.).

Naturalmente que o objetivo da inicial de segurança militar que tinham em mente os fundadores da NATO – a ex-URSS e os seus aliados do extinto Pacto de Varsóvia –, se tornou obsoleto com final da Guerra Fria. Várias transformações e adaptações ocorreram entretanto, procurando dar resposta às circunstâncias e necessidades de segurança no mundo da Guerra Fria (alargamentos a novos membros, alterações na identificação de ameaças e área geográfica de atuação, etc.). Neste contexto evolutivo, múltiplos documentos estratégicos foram adotados nos últimos 20 anos, o último dos quais foi aprovado na Cimeira de Lisboa, ocorrida em finais de 2010. Sobre o atual ambiente de segurança e as ameaças que lhe estão subjacentes, diz-se o seguinte no novo documento estratégico:

> "Os ciberataques estão a tornar-se mais frequentes, mais organizados e mais custosos nos danos que infligem às administrações governamentais, negócios, economias e potencialmente também às redes de transporte e fornecimento, bem como a outras infraestruturas críticas; podem atingir um patamar que ameaça a prosperidade nacional e Euro-Atlântica, a segurança e a estabilidade. Serviços militares e de informações estrangeiros, organizações criminais, grupos terroristas e/ou extremistas podem ser fonte de tais ataques." (NATO, 2010).

Quanto às capacidades de defesa e dissuasão este documento prevê que a NATO, "deve assegurar a totalidade das capacidades necessárias para dissuadir e defender contra qualquer ameaça à segurança das populações". No caso específico da ameaça de ciberataques – os quais, pela primeira vez, são mencionados ao nível do conceito estratégico –, foi estabelecido que a organização deverá "desenvolver

22 O Artigo 51.º da Carta das Nações Unidas tem o seguinte teor: "Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais." Acessível em http://www.fd.uc.pt/CI/CEE/pm/Tratados/carta-onu.htm, consultado em 10/07/2011.

mais a capacidade de prevenir, detetar, defender e recuperar de ciberataques, incluindo através do uso do processo de planeamento". Acrescenta-se, ainda, que deverá reforçar e coordenar "as capacidades de ciberdefesa nacionais, colocando todos os organismos da organização sob uma ciberprotecção centralizada, e integrando melhor a ciberconsciencialização, aviso e resposta com os Estados-membros (NATO, 2010).

Reflexões Finais

A emergência do ciberespaço durante os anos 90, ligada à explosão do uso da internet – tornada possível, sobretudo, pela invenção da World Wide Web e pela progressiva difusão das comunicações móveis e de banda larga –, mostrou os limites da visão idealista ou utópica dos fundadores da internet. Em vez de um "novo mundo" de liberdade e autorregulado, funcionando com base numa lógica de solidariedade e comunitária, emergiu, essencialmente, um domínio marcado por interesses económicos-comerciais e por um crescente uso profissional feito por múltiplos organismos públicos e privados. No caso dos grandes Estados autoritários, de que a China é o exemplo mais evidente, o ciberespaço foi, desde o início, um novo "território" não só de afirmação de soberania estadual como de controlo das atividades dos cidadãos, através de um sofisticado sistema tecnológico de vigilância. Ao contrário de uma opinião muito comum no Ocidente, a internet, como espaço de liberdade, não é uma inevitabilidade da própria tecnologia, mas, fundamentalmente, uma opção política. Nas democracias capitalistas liberais, nomeadamente nos EUA e na Europa, o próprio sucesso da internet e a crescente digitalização da economia acarretaram novas dependências, vulnerabilidades e riscos. O mais óbvio é o da possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de uma ciberguerra, envolvendo atores estaduais e/ou não estaduais, causando sérios prejuízos e afetando o normal funcionamento de uma economia e sociedade. Assim, o crescente uso e dependência das economias nacionais da internet e das infraestruturas de comunicação (e outras) levaram também as democracias liberais a afirmar a sua soberania sobre este novo "território", adotando, paralelamente, medidas securitárias de diversos tipos. A NATO, a principal organização de segurança e defesa coletiva das democracias capitalistas liberais, denota esta tendência que podemos designar como uma espécie de "regresso do Leviatã". A questão em aberto é a de saber se a afirmação de soberania e a tendência para "securizar" o ciberespaço, não só vai dar um golpe fatal à utopia libertário-anárquica inicial, como asfixiar o território de liberdade que o cidadão tinha ganho, com ou sem a vontade dos Estados.

Referências Bibliográficas

Amaral, Diogo Freitas do (1998). *História das Ideias Políticas.* (Vol. 1). Coimbra: Almedina.

August, Olivier (2007). "The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online". *Wired* (23/10/2007). Disponível em http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all. Data de acesso 10/07/2011.

Barlow, John Perry (1996). *A Declaration of the Independence of Cyberspace.* Acessível em http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration. Data de acesso 10/07/2011.

Bodin, Jean (1993). *Les Six Livres de la République.* Acessível em http://classiques.uqac.ca/classiques/bodin_jean/six_livres_republique/bodin_six_livres_republique.pdf. Data de acesso 10/07/2011.

Demchak, Chris e Dombrowski, Peter (2011). "Rise of Cybered Westephalian Age". *Strategic Studies Quarterly*, vol 5, n.º 1, p. 32.

Fernandes, José Pedro Teixeira (2009). *Teorias das Relações Internacionais: da Abordagem Clássica ao Debate pós-Positivista* (2ª edição). Coimbra: Almedina.

Fischer, Sebastian e Ole Reissmann (2011). "Germany Arms Itself for Cyber War". *Der Spiegel Online International*, Acessível em http://www.spiegel.de/international/germany/0,1518,768764,00.html. Data de acesso em 10/07/2011.

Foucher, Michel (1991). *Fronts et Frontières. Un Tour du Monde Géopolitique*. Paris: Fayard.

Gat, Azar (2007). "The Return of Authoritarian Great Powers". *Foreign Affairs*, julho/agosto. Disponível em http://www.foreignaffairs.com/articles/62644/azar-gat/the-return-of-authoritarian-great-powers. Data de acesso 10/07/2011.

Hobbes, Thomas (1978). *Lheviatan or the Matter Form and Power of a Commonwealth Ecclesiastical and Civil*. Oxford: Oxford University Press.

Internet World Stats (s.d.). *Internet in Asia – 2009. Top Ten Countries.* Acessível em http://www.internetworldstats.com/stats3.htm. Data de acesso 10/07/2011.

Keen, Andrew (1996). "Web 2.0 – The second generation of the internet has arrived. It's worse than you think". *Weekly Standard.* Acessível em http://www.weeklystandard.com/Content/Public/Articles/000/000/006/714fjczq.asp. Data de acesso 10/07/2011.

Keen, Andrew (2007). *The Cult of the Amateur: How Today's Internet is Killing our Culture. London:* Nicholas Brealey Publishing.

Kelly, Sanja e Sara Cook (2011). *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media.* Washington DC: Freedom House/The United Nations Democracy Fund.

Klimburg, Alexander (2011). "Mobilising Cyber Power". *Survival: Global Politics and Strategy,* vol. 53, nº 1, pp. 41-60.

Krasner, Stephen (1999). *Sovereignty: Organized Hypocrisy*. Princeton-New Jersey: Princeton University Press.

Leigh, David e Luke Harding (2011). *WikiLeaks: Inside Julian Assange´s War on Secrecy*. London: Guardian Books.

NATO (2010). *Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation (Adopted by Heads of State and Government in Lisbon, 2010).* Acessível em http://www.nato.int/lisbon2010/strategic-concept2010-eng.pdf. Data de acesso 10/07/2011.

NATO (s.d). *The North Atlantic Treaty* (4/04/1949). Acessível em http://www.nato.int/cps/en/natolive/official_texts_17120.htm. Data de acesso 10/07/2011.

Nozick, Robert (1977). *Anarchy, State and Utopia*. New York: Basic Books.

Ohmae, Kenichi (1996). *The End of Nation-State: The Rise of Regional Economics*. New York: The Free Press.

Till, Scott (2011). "March 17, 1948: William Gibson, Father of Cyberspace" em *Wired*. Acessível em http://www.wired.com/thisdayintech/2011/03/0317cyberspace-author-william-gibson-born/. Data de acesso 2/10/2011.

Turner, Fred (2006). *From Counterculture to Cyberculture*. Chicago: The University of Chicago Press.

Ciberespaço: uma Nova Realidade para a Segurança Internacional

Marco Martins
Professor da Universidade de Évora. Investigador do NICPRI. Doutor em Relações Internacionais pelo ISCSP. Auditor de Política Externa Nacional.

Resumo

Assiste-se na arena internacional a novas formas emergentes de ameaças que cada vez mais se posicionam na rede cibernética, provocando a deslocação do campo de batalha para o ciberespaço. A internet representa uma realidade incontornável das relações internacionais no quadro político e da segurança internacional.
Não só as novas tecnologias revolucionaram o mundo como também provocaram um sentimento negativo em torno do fator de segurança, nomeadamente em questões de privacidade e garantia dos sistemas de informação do Estado.
Aliás, atualmente não é possível afirmar a existência de um sistema de informação totalmente seguro e invulnerável. Ao contrário, a emergência de novas ameaças localizadas no ciberespaço representa um novo rosto do inimigo que se tornou invisível perante os nossos olhos.

Abstract
Cyberspace: a New Reality for International Security

We are witnessing in the international arena to new emerging forms of threats that are causing the displacement of the traditional battlefield to the cyberspace. Internet represents an inevitable reality in international relations and in the political framework of international security.
Not only the new technologies have revolutionized the world but also have triggered a negative feeling about the safety factor, especially in matters of web navigation and also regarding the security of the state information systems.
Indeed, it is currently not possible to sustain the existence of an information system totally safe and impenetrable. Rather, the emergence of new threats that is located in cyberspace represents a new face of the enemy that is invisible to your eyes.

A Realidade Virtual

O século XXI tem vindo a ser paulatinamente assinalado pela afirmação da incerteza do tempo que, por sua vez, marca a inconstância dos factos na realidade internacional, provocando a gestação de uma mudança não só na natureza do ser humano como também na aceção clássica do papel do Estado enquanto entidade soberana e reguladora quer da ordem interna quer da externa. Procura-se identificar a real imagem do mundo a partir e em torno da capacidade de sobrevivência do Homem. Esta sociedade, agora qualificada de global, perspetiva uma observação da imagem real do mundo inserida numa cosmovisão do lugar do Homem na redefinição geopolítica da hierarquia das potências. A atenção focaliza-se na perspetiva do ser humano envolvido na sociedade civil para compreender a *complexidade crescente* da ordem internacional a que se encontra sujeito, tendo em consideração a multiplicidade de identidades, a proliferação de estruturas e de novos atores no sistema internacional.

Para além da multipolaridade, emerge um outro sistema que segundo Richard Haass (2008), presidente do *Council on Foreign Relations*, se diferencia dos restantes por se caracterizar pela não-polaridade e por surgir num momento de combate à tendência hegemónica ambicionada pelos Estados Unidos. A instabilidade no sistema não-polar pode contribuir para o incremento de ameaças, tais como o terrorismo, as operações no mercado financeiro, o investimento, o comércio, afetando consequentemente a estrutura do Estado, das finanças à política. A não-polaridade institui um ambiente perturbador e perigoso, sendo necessário optar por uma cooperação multilateral no intuito de incrementar o grau de integração global na promoção da estabilidade, dado que na rede económico-financeira a interdependência provoca uma reação institucional no sentido de que nenhum Estado se encontre autoimune à realidade neoliberal que acabou por agravar a pobreza à escala global.

Tornou-se numa evidência de que os dispositivos tecnológicos mudaram radicalmente e substancialmente o mundo e o lugar do Homem. Nesse sentido, o caminho do Homem converge e relaciona-se cada vez mais acentuadamente na necessidade de profetizar o futuro, tendo por base o passado situado na sua memória. A dimensão tecnológica implementada no ciberespaço superou a dimensão humana e social. Perante esta nova realidade, circulam novos valores em nome de uma sociedade mais aberta e democrática que tende a traduzir-se numa verdadeira ideologia técnica a qual tem vindo a revolucionar a forma como o ser humano se insere nesta nova sociedade considerada de virtual. Importa referir que na opinião

de Dominique Wolton (1999) epistemologicamente não é passível de confundir a técnica, a cultura e a sociedade visto estes últimos enquanto modelos culturais e organizacionais evoluem e definem-se a uma velocidade não comparável à do progresso tecnológico.

O Ciberespaço como uma Nova Dimensão Temporal

Para o Estado soberano o processo de decisão torna-se progressivamente de maior complexidade devido à dificuldade de adaptação e de conciliação no sistema internacional. Assim sendo, a projeção do tempo para a rede geograficamente localizada no ciberespaço renuncia às características tradicionais, nas quais o Estado operava e se baseava desde os tempos mais remotos na definição das suas políticas e na defesa do interesse nacional. Essa situação ocorre, por um lado, pela crescente interdependência resultante da globalização e, por outro lado, da própria velocidade comunicacional dos fluxos de informação que cruzam todas as fronteiras terrestres em tempo real e imediato sem sequer outorgar a possibilidade de filtrar ou de analisar todo o volume informativo. Resulta que a impossibilidade de filtrar devidamente a informação que circula no tempo mundial no ciberespaço constitui por si só e para qualquer sistema político um facto perturbador.

Aliás, diga-se de passagem que a velocidade dos fluxos de informação e a inovação tecnológica operada no ciberespaço incita em termos objetivos a uma modificação gradual do comportamento geracional que inevitavelmente terá consequências de cariz cultural e social junto da sociedade no seu todo. De acordo com Eric Delbecque (2007) a batalha para a aquisição de novas tecnologias e/ou inovação é reservada somente a determinados atores económicos e Estados que atempadamente conseguirão antever e decifrar os mais variados acontecimentos que ocorrerão na arena internacional. Perante tal facto, provoca um novo sentimento no Homem que terminará por agir e operar no seio de um ambiente a uma velocidade superior àquela a que no passado se submetia.

Portanto, a navegação em tempo imediato concebe a impossibilidade de distinguir em termos temporais o passado, o presente e o futuro, tendo o Homem neste caso concreto a consciência da necessidade de agir cada vez mais num ambiente a velocidade superior à escala global e não somente ao nível local. Além disso, registamos uma das mudanças no comportamento do ser humano no quadro do desenvolvimento tecnológico aplicado ao ciberespaço que consiste na questão de como o Homem e o respetivo ambiente externo, leia-se aqui no campo das relações internacionais, conseguem gerir a imagem que se projeta sistematicamente da realidade diária para a virtualidade da rede na qual a mesma outorga a possibilidade

de se assumirem novas identidades e consequentemente novos papéis a desempenhar. Note-se que esta questão termina por envolver a análise a um nível distinto na esfera das relações internacionais como sendo o caso da junção ou a amálgama no ciberespaço do espaço virtual e do meio físico (satélites, cabos de fibra ótica, servidores, computadores) dos mais diversos sistemas políticos, económicos, culturais e religiosos capazes de provocar e conceber novos sistemas de valor cuja imagem transmitida pode ou não traduzir efetivamente a realidade diária.

Com efeito, o presente processo introduz nem uma relativização da realidade virtual nem uma anulação da influência física, mas sim a edificação de um imaginário com consequências reais e por vezes nefastas no mundo concreto. Existe de facto uma projeção de uma realidade para outra, contudo em ambos os casos é introduzida uma nova dimensão de maior complexidade na qual as relações internacionais acabam por operar entre a virtualidade, o imaginário e a realidade. Mesmo que não se pretenda integrar o sistema cibernético, o ser humano termina por indiretamente e involuntariamente ver-se introduzido num terreno paralelo localizado espacialmente entre a ficção e a autenticidade. A presente transferência vem modificar as relações entre o ambiente interno e o ambiente externo, agregando o sentimento de liberdade absoluta, de navegabilidade e mobilidade virtual sem precedentes e sem sujeição hierárquica.

A realidade internacional move-se no interior desse tempo mundial, procurando controlar e monitorizar a emergência de novas ameaças que circulam pelas redes do ciberespaço. Todas estas transformações levam a que o Estado desenvolva um papel virtual no ciberespaço na procura constante do aperfeiçoamento tecnológico. Diga-se de passagem que o Estado perde a sua capacidade de controlar o poder derivado dos mecanismos relacionados com a utilização das novas tecnologias que pode de facto incrementar a distância entre a virtualidade e a realidade no terreno, produzindo consequentemente um processo de ineficácia política (Noya, 2010). A principal ideia advinda da utilização da internet reside na propagação da livre circulação do saber à escala planetária. Nesse contexto, a elite política ou os próximos líderes deverão demonstrar uma capacidade superior de interpretação do verdadeiro sentido da magnitude de transmissão de dados a velocidade imediata através da rede virtual. Todavia, a médio prazo, o poder de influência localizar-se-á gradualmente no ciberespaço, onde o destino do mundo se irá concretizar através de quem detiver a capacidade de dominar a rede virtual.

Neste caso concreto, evidenciam-se por um lado as clivagens entre os diversos atores na capacidade de acesso à tecnologia, dependendo de Estado para Estado e, por outro lado, as desigualdades socioculturais que se caracterizariam pela aceção de infoincluídos em contraponto com os infoexcluídos. Por conseguinte, formar-se-iam discrepâncias advindas do próprio conceito de informação/conhecimento com interligação ao grau de liberdade e de democracia na mera utilização dos

meios tecnológicos. De facto, a internet fornece os mais variados serviços ao indivíduo, em nome do conhecimento do Estado, como por exemplo: (1) serviços de compra e venda; (2) lazer, jogos em linha e em simultâneo; (3) serviços públicos no quadro da extensão da administração central do Estado; (4) ligação em rede de instituições, de empresas, de bancos; (5) a oferta de conhecimento enquanto tal, como o acesso a universidades, a centros de estudo, de investigação, a livros em formato digital, a textos, à imprensa internacional; (6) a disponibilização de redes sociais de contacto universal; (7) a possibilidade de ligar as mais diversas unidades móveis operadas independentemente do espaço físico.

Salientamos a capacidade que o ciberespaço possui em possibilitar o acesso a infinitas aplicações que terminam por se integrar no Estado, na vida de cada família à escala global sem diferenciação de pertença social ou de nacionalidade. Contudo, o acesso pleno ao ciberespaço dependerá evidentemente da capacidade do cibernauta quer no domínio da utilização quer nos meios financeiros de que dispõe, para além da sua localização geográfica. Anotemos por exemplo, a título comparativo, os casos de um utilizador num determinado país onde o acesso se encontre limitado por razões de desenvolvimento ou condicionado por motivos de controlo político ou simplesmente inexistente, e de outro que viva num ambiente cuja realidade virtual faça parte integrante da realidade física. Entendemos assim que os infoexcluídos consistem naqueles que não conseguem aceder, neste caso concreto, à realidade cibernética, derivada da própria condição de exclusão da sociedade ou da impossibilidade de navegar no ciberespaço por razões económicas ou políticas. Se porventura se tratar de consequências meramente de ordem económica, referimos o conceito de infopobres, abrangendo aqueles que se deparem em condições extremas de pobreza, por desemprego ou por impossibilidade de inclusão na realidade virtual cuja prioridade consiste não na obtenção de conhecimento e navegação no ciberespaço, mas sim na procura da sua sobrevivência. Assim, se o ciberespaço se encontra acessível em qualquer ponto do globo não significa porém que todos os indivíduos detenham a respetiva entrada ou sequer a possibilidade de utilizar o potencial que lhes é oferecido.

Apesar de ser passível separar cada um dos exemplos acima referenciados, numa perspetiva cibernética, o todo interliga-se numa rede de maior complexidade e interdependente formada numa unidade virtual que se desenvolve em três escalas simultâneas: (1) para além das fronteiras físicas dos Estados; (2) no indivíduo; (3) no âmbito coletivo. Por outras palavras, apesar de numa primeira análise se considerar a internet como um espaço por excelência de liberdade absoluta e sem fronteiras, a realidade porém, leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar, desde a invasão do computador sem sequer o utilizador comum ter a noção exata de que fora alvo da violação da sua

privacidade do seu espaço, à espionagem, à propagação de vírus e inclusive ao roubo de dados sensíveis na esfera governamental.

Consequentemente, o cibernauta ao consciencializar o risco e a possível ameaça emanadas da realidade virtual sente que efetivou a passagem de um sentimento de utopia para o de distopia em que afinal não se encontraria no "melhor dos mundos", recordando a obra *Brave New World* de Aldous Huxley, mas sim integraria um campo onde o desconhecido se revelaria na principal fonte de medo e de insegurança no qual o conceito de crime se transferira para a qualidade de cibercrime, colocando a "ciberliberdade" em causa com consequências nefastas do Estado ao indivíduo. Entendemos que o ideal democrático aplicado ao ciberespaço é afetado pela realidade adversa resultante da impossibilidade aparente de controlar globalmente o conteúdo da internet sem distinguir informação pública de privada, o que vem colocar problemas em matéria de segurança virtual e física visto que os dados obtidos na realidade virtual podem provocar danos irreversíveis quer na imagem de um Estado quer no próprio indivíduo em caso de rapto ou roubo.

Aliás, este problema advém no momento em que o cibernauta inocentemente constrói por exemplo uma página no *Facebook* na qual posteriormente fornecerá informação respeitante à sua vida, quer pessoal quer profissional, a um indeterminado número de supostos amigos mesmo sem os conhecer particularmente. Precisamente, essa transmissão de dados privados tornados públicos podem colocar em causa não só a sua vida mas também os próximos, arriscando-se as consequências a constituir uma primeira etapa da destruição da sua vida por representar uma ameaça à entidade empregadora, caso desempenhe funções de importância acrescida para entidades privadas ou para o Estado em setores sensíveis. Note-se que se regista um número elevado de setores profissionais que antes de contratarem um funcionário consultam a página pessoal das redes sociais para saber se, de facto, representa ou não uma ameaça. Perante esta situação, o ser humano encontra-se num processo de descontinuidade da sua existência real na conjunção com a virtualidade cibernética. O cibernauta tenderá a ver-se confrontado com a aquisição de uma dupla identidade resultante da sua nova condição na rede. No domínio psicológico, a dificuldade surgirá a partir do momento em que ambas as identidades se fundirão numa só o que trará inevitavelmente consequências e riscos quer para o cibernauta quer para o Estado na forma de *e.gov* enquanto entidade soberana visto a sua crescente dependência da web 2.0. na relação intragovernamental e extragovernamental, entenda-se para com o cidadão, as empresas, os serviços disponibilizados, o comércio, os setores vitais como a defesa, a saúde, a gestão de barragens e centrais elétricas ou nucleares, entre outros.

Com efeito, a gestão do saber acompanhada de capacidade criativa funcionará na forma de um agente catalisador de um novo poder situado na internet, esca-

pando por conseguinte ao mecanismo clássico do Estado, o que traduz a incapacidade de outorgar uma nacionalidade ao cibernauta por este navegar no território numérico sem estar sequer acompanhado pela correspondente bandeira nacional. Na opinião de Dennis Ettighoffer (2008) o saber penetrou a esfera do mercado, circulando livremente no ciberespaço, oferecendo uma nova forma de comunicabilidade. Torna-se inquestionável que o Homem se tenha convertido num membro do ciberespaço e atue em plena autonomia, criando empresas e comunidades virtuais cujas informações são transfiguradas pelo espírito humano numa mutação da informação com desideratos precisos, onde o saber requer a obtenção de conhecimento na forma de dados na rede virtual.

O Fator de Insegurança no Ciberespaço

Atualmente, a internet não possui uma bandeira nacional ou uma lei internacional que impeça a livre navegação. Contudo, existem casos pontuais como a Coreia do Norte, por sinal o único país do mundo cuja utilização da internet se encontra proibida à população, e permanece em exclusividade para a elite política; ou a República Popular da China (RPC) que quando se sente ameaçada decide optar pelo bloqueio de determinadas páginas ou motores de procura como o *Google* alegando a defesa do interesse nacional o que constitui para a comunidade internacional uma violação da liberdade. A postura de ambos os países traduz a necessidade de impedir quer o acesso quer a circulação da informação para que a mesma não influencie negativamente as estruturas governativas ou simplesmente para evitar que se tenha conhecimento da realidade para além fronteiras.

No quadro do controlo da internet a *OpenNet Initiative* (ONI) (Deibert, 2009: 323-337) tem por principal objetivo o levantamento exaustivo do comportamento e formas de censura e vigilância na rede. Importa referenciar que, ao contrário da perceção geral por parte dos internautas, a internet não representa uma infraestrutura aberta e descentralizada, pois as ligações efetuam-se via satélite, cabos submarinos e fibra ótica que se ligam localmente a servidores, a *routers* através do *Internet Service Provider* (ISP) e também por meio do *Internet Exchange Points* (IXP), pontos internacionais e companhias de telecomunicações. Se por um lado, a internet representa uma realidade virtual, por outro lado, encontra-se fortemente dependente de estruturas físicas de comunicações que por sua vez se localizam no interior dos Estados. A existência dessa interdependência para com os meios físicos gera a possibilidade de se controlar eficazmente o tráfego, os fluxos de informação pela utilização de filtros e de programas informáticos de vigilância, de *chokepoints* por razões políticas e/ou económicas. A título de exemplo, a RPC converge o seu controlo nas seguintes áreas: (1) direitos humanos; (2) movimentos independentistas;

(3) minorias; (4) grupos pró-democráticos; (5) motores de procura (nomeadamente o *Google*); (6) *e-mails*; (7) serviços de *webhosting*; (8) pornografia.

No âmbito da censura, para além do Irão e da Arábia Saudita, a RPC com 258 milhões de utilizadores, à data de 2008, surge segundo dados da ONI como o país que maior controlo exerce sobre a navegação no ciberespaço. A RPC utiliza um sistema de filtragem a múltiplos níveis que por sua vez envolvem um número considerável de agências e milhares de profissionais (*OpenNet Initiative*). Neste caso, é possível controlar através do bloqueio de acesso a um determinado *Internet Protocol* (IP), por exemplo, no caso de Estados que pretendam restringir ou até proibir o acesso a determinados conteúdos e/ou *sites* é possível com a tecnologia disponível bloquear e filtrar o tráfego utilizando os pontos de acesso internacional. Contudo, se enquadrarmos o conceito de *global commons* aplicado ao ciberespaço, a internet consiste por um lado num lugar onde qualquer individuo detém a possibilidade de aceder livremente e, por outro lado nenhuma entidade quer particular quer coletiva ou estatal pode reivindicar esse espaço como sendo da sua propriedade ou sequer tomar o seu controlo.

Acresce ainda que no quadro das relações internacionais, os seguintes países impedem estrategicamente o acesso a determinados *sites*: (1) a Coreia do Sul bloqueia *sites* relacionados com a Coreia do Norte; (2) a Índia impede o acesso a *sites* de grupos extremistas, concretamente islâmicos e hindus; (3) a Jordânia, a Síria, a Arábia Saudita, os Emirados Árabes Unidos e o Bahrein procedem pontualmente ao bloqueio de domínios israelitas. Diga-se de passagem que as autoridades locais nesses países concentram o controlo e a monitorização em blogs, em chats, no envio de SMS e em mensagens instantâneas e serviços de *Voice Over Internet Protocol* (VOIP). Note-se todavia que o controlo e o bloqueio por parte da RPC, da Índia, da Coreia, do Paquistão, do Uzbequistão, de Mianmar, da Tailândia, do Vietname, da Etiópia, da Líbia, da Tunísia, do Irão, dos Emirados Árabes Unidos, da Síria, e do Bahrein, são precedidos ao nível interno e local do que propriamente numa esfera mais alargada que poderia atingir o global.

É de salientar nesse sentido que o indivíduo transformado em cibernauta pode atuar na qualidade e em nome de um grupo de pressão com possibilidade de mudar ou de alterar o destino das relações internacionais a partir da internet. Revela-se de interesse o facto de a *primavera árabe* possuir como ponto de partida não só o acontecimento trágico de Mohamed Bouazizi, mas também a mensagem que o mesmo escreveu na sua página pessoal do *Facebook*, de pedido de perdão à sua mãe pelo ato que iria cometer e de culpabilização da realidade vigente que o levara à imolação pelo fogo no fatídico dia 17 de dezembro de 2010, na praça de central de Sidi Bouzid, na Tunísia. Note-se ainda o gesto, pouco antes de renunciar e de entregar o poder às forças armadas egípcias no dia 11 de fevereiro de 2011, do ex-Presidente Hosni Mubarak na tentativa de bloquear todo o tipo de acesso à inter-

net para evitar a propagação da revolta para o campo cibernético das redes sociais contra o seu regime. Frank La Rue (2011) refere expressamente no seu relatório *The Promotion and Protection of the Right to Freedom of Opinion and Expression*, apresentado no dia 16 de maio de 2011 perante a Assembleia Geral das Nações Unidas, que são utilizados sistemas de filtragem na China que bloqueiam o acesso a *sites* contendo palavras como "democracia" ou "direitos humanos". Salienta ainda a importância e a força que a internet possui em momentos cruciais e determinantes nas relações internacionais como por exemplo os acontecimentos no Norte de África, no Médio Oriente e concretamente nos casos da Tunísia e do Egito, nos quais a população utilizou a internet como um instrumento por excelência na defesa da liberdade.

Como se pode verificar, uma das consequências inevitáveis da expansão da internet resulta no facto de considerar, retomando o conceito de Adriano Moreira, que todo o facto doméstico sucedido no seio do Estado enquanto entidade soberana pode constituir um facto ou uma ação potencialmente internacionalizável pela sua transposição ou deslocalização do espaço físico para a realidade virtual. Trata-se de um dos riscos que os Estados enfrentam, quer internamente quer externamente, porque presentemente não se torna possível separar o Estado da internet e da respetiva projeção à escala global. Se por um lado, a internet significa conhecimento e traduz claramente a vantagem de beneficiar do acesso a partir de um ponto específico do globo a um número infinito de ligações em rede que conectam o planeta a uma outra realidade, por outro lado, a negatividade pode surgir a partir do roubo da identidade ou da invasão do domicílio virtual sem o consentimento do internauta o que provoca a suspensão temporária do sentimento de ciberdemocracia. A partir desse preciso momento, o internauta regressa à realidade ao tomar consciência da existência de uma nova ameaça em forma de crime no mundo virtual, o que consequentemente cria um sentimento de medo constante no simples teclar e navegar na rede.

Contudo, assiste-se paralelamente a uma transferência do campo convencional de batalha, onde as ameaças se identificariam com certa facilidade, para o ciberespaço, onde existe um novo rosto invisível denominado internauta. Assim, as novas ameaças representam um risco com implicações globais para os Estados e a humanidade. Para o Estado, o inimigo sem rosto e sem identidade provoca um sentimento de temor e de perigo superior ao das guerras ou conflitos ditos tradicionais. A internet incita nessa perspetiva à propagação da militância extremista e à formação de redes criminosas que operam em ambiente virtual.

A insegurança no ciberespaço transformou-se no mundo dos rostos invisíveis, onde aqueles que transgridem o espaço de liberdade do internauta comum e penetram as fronteiras físicas dos Estados terminam conhecidos como *hackers*. Neste caso, importa destacar os "*hackers de chapéu branco*" que se consideram no meio vir-

tual como aqueles que protegem a integridade do sistema sem pretender traduzir as suas ações em crime, ao contrário dos "*hackers de chapéu preto*". As principais vítimas são aquelas que se encontram perante uma posição de vulnerabilidade, caso das crianças quando não devidamente acompanhadas por um adulto e de indivíduos que se sentem isolados e/ou sozinhos. Para além deste tipo de vítima, o Estado, as suas instituições, o setor empresarial ou a banca simbolizam um novo alvo a explorar e a abater por representar um motivo de desafio para quebrar os sistemas de segurança ou uma forma de transmitir a revolta contra as políticas definidas ou um meio para denunciar as violações dos direitos humanos. Os cibercriminosos utilizam os dados recolhidos para posteriormente vender segredos de empresas, códigos de programação ou divulgar segredos de Estado que possam colocar em causa a segurança internacional. Portanto, o *hacker* não representa exclusivamente os adolescentes norte-americanos que a partir de uma garagem conseguiam atravessar qualquer tipo de barreira de segurança dos sistemas de informação na rede.

O caso *Wikileaks* de Julian Assange reproduz para a comunidade internacional um exemplo claro de guerrilha informática global que provocou a possibilidade de colocar em causa a segurança, através da ausência de efetivo controlo do ciberespaço, concretamente no acesso a informação estratégica, vital e sob segredo de Estado. Os mais de 250 mil documentos provenientes do Departamento de Estado Norte-americano e do *Secret Internet Protocol Router Network* (SIPRNET) trazidos a público comprometem a esfera de atuação quer militar quer diplomática e causam danos irreparáveis de elevado impacto nas relações internacionais, nomeadamente na perceção por parte da sociedade civil. Trata-se sobretudo de uma denúncia pública comprometedora de segredos de Estado, tanto militares como diplomáticos. Neste campo, a problemática foca-se sobretudo no acesso a documentação supostamente classificada e restrita a um delimitado número de indivíduos, de decisores governamentais e na generalidade de atores políticos e diplomatas.

Com efeito, o *hacker* opera num mundo paralelo à realidade diária do ser humano no qual a sua motivação expressa um sentimento de revolta em nome de uma causa. Esta mudança que se regista revela uma nova forma de defender os direitos humanos e compreende uma perspetiva do sentimento de ciberdemocracia que consiste no ciberactivismo por envolver a sociedade e projetar o movimento em desobediência civil por vezes com ligações a organizações como a Greenpeace ou a Amnistia Internacional. A esse ciberactivismo torna-se possível acrescentar hacktivismo por subverter ou infetar determinados sítios na internet através da construção de sítios espelhos como sendo os casos do *World Bank*, transformado em *Whirled Bank* com o desígnio de "*our dream is a world full of poverty*" para denunciar justamente a pobreza e o sistema financeiro (McCaughey, 2003).

O Reforço da Cibersegurança

A internet tem vindo a converter-se num novo campo de batalha não convencional cujos rostos invisíveis tendem paulatinamente a dominar o ciberespaço, dotando-se de uma arma que representa uma maior perigosidade e ameaça do que a nuclear num cenário virtual dotado de soldados digitais devidamente preparados para atuar em ambiente de ciberguerra. A arma por excelência no ciberespaço reside na capacidade de enviar códigos que consigam quebrar todo o tipo de protocolos de segurança nas mais diversas redes informáticas. No campo de ação do ciberespaço, a obtenção de informação não representa somente um objetivo concreto, verifica-se assim a constituição de outros, como por exemplo, detetar vulnerabilidades em redes estratégicas para a sobrevivência do Estado.

Neste contexto, a administração norte-americana liderada por Barack Obama decidiu no ano de 2009 proceder à criação do cargo de "ciberczar", referente ao coordenador para a cibersegurança na Casa Branca, ocupado por Howard Schmidt, tendo igualmente indicado em 2010 o General Keith Alexander para representar a nova estrutura cibermilitar do Pentágono, a US Cybercommand (USCYBERCOM ou CYBERCOM), localizada em Fort George Meade que conta com um total de 90 mil profissionais civis para proteger os sistemas informáticos (Macon, 2009; Lawson, 2010). Note-se que desde 2006, a *Doutrina Conjunta de Operações de Informação* do Pentágono estabelece a necessidade de obter a superioridade das forças militares devidamente preparadas para qualquer tipo de intervenção em tempo mundial no ciberespaço. Estas operações defensivas e ofensivas pretendem garantir a integridade do sistema informático norte-americano e dos aliados. Para isso, o objetivo último para vencer uma ciberguerra abrange o controlo da informação e a neutralização dos rostos invisíveis. Aliás, a *Comprehensive National Cybersecurity Initiative* do *Executive Office of the President of the United States*, tem por princípios: estabelecer uma linha de defesa contra ameaças imediatas que possam colocar em causa o governo; defender contra todo o tipo de ameaças através do incremento de operações de contrainformação; reforçar o futuro ambiente de cibersegurança concretamente pelo desenvolvimento de ações de formação, de educação em ambiente ciber e pela definição de estratégias para dissuadir atividades hostis e maliciosas no ciberespaço.

Estipula ainda a necessidade de consolidar uma rede com *Trusted Internet Connections* (TIC); implementar um sistema de deteção de intrusão dotado de sensores passivos como parte integrante da rede governamental; desenvolver um sistema de prevenção de intrusão operado em tempo real denominado de EINSTEIN 3 para identificar e caracterizar o tráfego da internet para reforçar a segurança do ciberespaço; incrementar a segurança e a respetiva classificação da informação sensível para garantir a integridade do sistema e da defesa do interesse nacional; inves-

tir na educação do ciberespaço para que a sociedade civil possua o conhecimento adequado quanto à utilização do espaço virtual e, por último, definir o papel do governo na segurança de infraestruturas críticas e vitais do Estado. Nesse sentido, à data de 15 de abril de 2011, a administração Obama determinou a *National Strategy for Trusted Identities in Cyberspace* para intensificar a segurança e estabelecer os princípios fundamentais no desenvolvimento do comércio eletrónico.

O Pentágono assume o reconhecimento oficial deste novo campo de batalha não convencional do século XXI. Desde 2010 que o *US Cyber Comand* se encontra operacional, tendo o apoio dos *Marine Corps Forces Cyberspace*. Nos dois últimos anos, os Estados Unidos intensificaram operações de simulação de ataques denominados por *cyberstorm* para incrementar a capacidade defensiva em tempo real, tendo em consideração o facto de a ciberguerra partir de um ataque em qualquer ponto do globo não previamente identificado. Sublinhe-se que o *US Cyber Comand* tem o apoio da comunidade de informações dos países aliados. Neste momento, a principal preocupação por parte desta nova força que é constituída por homens e mulheres não dotados de capacidade de resistência para sobreviver em ambientes hostis extremos de um campo de batalha convencional, mas sim detentores de conhecimentos técnicos específicos para combater em situação de ciberguerra cujo propósito, reside na defesa e proteção dos domínios ".gov" e ".com", para além de todo o tipo de infraestruturas governamentais, do setor de educação à defesa (Lynn, 2010).

Na esfera europeia, com o apoio da Europol, pretende-se dotar os Estados-membros de condições tecnológicas suficientes para combater em ambiente de ciberguerra. Contudo, ao contrário da posição norte-americana que apesar de defender e de demonstrar certa preocupação, a União Europeia tem vindo a defender o reforço não só dos efetivos, mas também do desenvolvimento de ferramentas jurídicas e penais para condenar criminalmente em sede própria, o cibernauta que cometa infrações e viole inequivocamente a lei. No tocante ao cibercrime, a União Europeia procede igualmente com o auxílio da *European Cybercrime Task Force* e da *European Union Cybercrime Unit*. Assim sendo, para as autoridades europeias e respetivos governos tornam-se evidentes a introdução de um direito penal específico ao ciberespaço e do reforço do controlo da navegação dos cibernautas o que levaria inevitavelmente à violação do direito à privacidade do internauta, visto a possibilidade de monitorizar a sua navegação em ambiente virtual consistir numa clara violação do espaço de liberdade. Por seu turno, o novo conceito estratégico da NATO considera no seu articulado respeitante ao ambiente de segurança que os ciberataques, dotados de maior organização, têm por um lado vindo a incrementar e, por outro lado, causado danos de elevado custo a determinados setores como o administrativo, as empresas, as infraestruturas vitais. Anotemos ainda que se traduz numa ameaça para a prosperidade, a segurança e a estabilidade dos Estados. Assinala igualmente que os serviços de informações, as forças armadas, a

criminalidade organizada, grupos terroristas e/ou extremistas constituem fontes de possíveis ataques.

Importa destacar que o ciberespaço representa uma ferramenta por excelência para comunicar por canais não detetáveis, por vezes encriptados, que atravessam todo o tipo de barreiras sofisticadas de segurança, o que permite conceber operações de ataque a alvos essenciais como as estruturas vitais do Estado. Note-se ainda que a junção de ciber com terrorismo forma o conceito de ciberterrorismo que, quer para a elite política quer para a sociedade civil, induz o medo pelo sentimento da deslocalização geoespacial do território físico para a rede virtual. O ciberterrorista ao contrário do *hacker* tem por aspiração e missão causar o maior número possível de danos não reparáveis aos sistemas informáticos, do setor estatal ao privado, com a possibilidade de envolver danos físicos e psicológicos em civis.

Portanto, procura-se um equilíbrio entre as forças tradicionais militares para garantir a defesa das fronteiras e intervir em caso de conflitos internacionais e entre a componente civil ao serviço do Estado na defesa do ciberespaço e das múltiplas redes informáticas. O ciberterrorismo opera igualmente na internet para a obtenção de fundos financeiros que lhe permitam levar a cabo as respetivas missões. Essa angariação de fundos compreende por exemplo o roubo de dados financeiros dos internautas registados em contas bancárias ou em números de cartões de crédito. Evidencia-se a utilização e a exploração por parte de grupos terroristas projetados para a esfera da rede virtual de *software* ou de sítios na internet que permitam a edição ou o *upload* de ficheiros sem custos adicionais, evitando assim a identificação através de transações bancárias e mantendo consequentemente o anonimato.

Além disso, o ciberespaço para os grupos qualificados de terroristas serve de base para a troca de comunicação entre os diversos grupos sem qualquer tipo de risco em ser detetado (Lewis, 2002). Recorde-se que Abu Musab al-Zarqawi, o autoproclamado líder da *Al Qaeda* no Iraque, transmitia e divulgava as suas mensagens via *fora* e *video streaming* na internet, o que provocava e fomentava uma nova atração para os seguidores *jihadistas* (Kohlmann, 2006). Um outro exemplo, abrange o caso do *Hezbollah* que reclama a utilização da internet como fonte de informação e de propaganda na luta contra Israel através do sítio <www.hizbollah.org> que por sua vez foi alvo de ataques por parte de *hackers* israelitas. Nesse contexto, em nome de uma *e-jihad*, o *Hezbollah* reconhece a utilidade e a vantagem da internet numa possível ciberguerra árabe-israelita. Sublinhe-se a criação do sítio UNITY <www.ummah.net/unity>, presentemente inativo, para implementar estratégias específicas no sentido de causar o maior impacto e danos ao governo israelita, substancialmente na desativação de sítios pertencentes à rede governamental ou no colapso de sítios ligados a setores financeiros como a banca ou o *Israel's Stock Exchange* (Trendle, 2002).

Importa referir, numa outra perspetiva, o facto de se considerar o conflito do Kosovo como a primeira guerra localizada na internet, na qual se assistira por parte dos diversos atores desse conflito a operações de informação quer na versão de *InfoOps* ou de *PsyOps*, criticando inclusive abertamente os opositores. Acresce a intervenção de *hackers* ao dar voz à escala mundial contra a situação na Jugoslávia e à postura da NATO perante o escalar do conflito, tendo determinados sítios governamentais sido alvo de ataques no sentido de desativar os mesmos. Neste caso, o ciberactivismo praticado consistiu sobretudo na exploração e na denúncia na arena internacional a partir do ciberespaço na divulgação do sentimento de horror de um conflito geograficamente localizado em território europeu. Comparativamente para um grupo terrorista um ataque perpetrado em território não virtual outorga um sentido de superioridade em termos de danos e de impacto dramático junto das entidades políticas e da sociedade civil do que uma ação ocorrida no ciberespaço que terminaria circunscrita naquele espaço. Porém, acompanha-se gradualmente um escalar de tensão e de hostilidade na utilização deste novo poder operado no espaço cibernético. Um ciberataque por parte de um grupo terrorista pode manifestar-se na interrupção de serviços em infraestruturas críticas, do aprovisionamento de água à gestão e manutenção de uma central nuclear. Em ambos os casos as consequências implicam e visam estruturas físicas com impacto junto da população civil.

Entre janeiro e março de 2011, ocorreram dois ataques por parte de *hackers*: o primeiro visava o acesso a informação estratégica de defesa do *Defence Research and Development Canada* e o segundo contra a rede do governo francês para a obtenção de informação vital que eventualmente pudesse representar uma ameaça para as próximas cimeiras do G20. Regista-se que recentemente o Departamento de Justiça norte-americano anunciou o desmantelamento de uma rede criminosa que se servia da internet para roubar dados pessoais através da propagação de um vírus espião denominado de *coreflood* que tinha por incumbência o registo das teclas utilizadas pelo utilizador aquando da sua navegação. O *coreflood* terminou por infetar cerca de 2,3 milhões de computadores.

A título exemplificativo, numa investigação levada a cabo por entidades norte-americanas e canadianas, identificou-se uma rede cibernética localizada e sediada em Chengdu, em Sichuan, na China, denominada de *Shadow* cujo alvo consiste em aceder a computadores, a sistemas informáticos, a contas do *gmail*, a plataformas de redes sociais e a *blogs* não só a nível mundial como também pertencentes a instituições governamentais indianas e a bases militares (Lemon, 2010). Um outro caso, consistiu no *worm Stuxnet*, descoberto em julho de 2010, cujo propósito residiu no ataque ao sistema operacional *Scada*, da Siemens, que controlava nas centrais nucleares as centrifugadoras de enriquecimento de urânio, tendo como alvo o reator da central de Bushehr no Irão (McMillan, 2010). Aliás, segundo o relatório *Did*

Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? do *Institute for Science and International Security* presume-se que o *Stuxnet* tenha destruído cerca de mil centrifugadoras em Natanz derivado da alteração da velocidade dos motores, o que vem afetar substancialmente o programa nuclear iraniano (Albright, Brannan, Walrand, 2010). Nesse sentido, na opinião da empresa russa *Kasperky Labs* considerar-se-á que se trata de um protótipo de uma nova ciberarma dotada de capacidade de provocar uma corrida armamentista no âmbito da possibilidade de uma ciberguerra. Respeitante a custos, o cibercrime coloca em evidência as repercussões da propagação de vírus, de ataques a alvos como as praças financeiras, a degradação dos sistemas de comunicação. Os custos financeiros representam por um lado, perdas na ordem dos mil milhões de dólares respeitantes à propriedade intelectual, a fraudes financeiras, à destruição de dados confidenciais no setor bancário e empresarial, e, por outro lado, denote-se que na fase posterior a um ataque, a dificuldade reside na recuperação da confiança perdida quer internamente quer externamente.

As Implicações: do Ambiente Terrestre ao Virtual

Tendo em consideração a dimensão do ciberespaço, torna-se evidente a impossibilidade de se pretender ou possuir sequer a intenção de o controlar na globalidade por representar o lugar por excelência de liberdade na sua plenitude, apesar de operar num novo espaço geopolítico, na senda de Solveig Godeluck (2002) ao depender de estruturas físicas e de territórios que por sua vez são controlados por Estados, para além de reproduzir e transpor os conflitos reais para uma nova fronteira no ciberespaço. Verificamos, por conseguinte, uma crescente interdependência entre duas realidades ou ambientes distintos, por um lado, o ciberespaço e, por outro lado, o mundo no qual vive o ser humano. O *linkage* comprovado entre ambos os ambientes emerge nas mais diversas formas como os casos da comunicação, da aviação, dos serviços governamentais, das finanças, da banca, das instituições público-privadas, do comércio, da medicina e da segurança, entre outros setores. A conexão de toda esta interdependência origina a possibilidade de colocar em causa e em risco não só informação irrelevante mas, sobretudo, dados estratégicos e vitais do Estado à sociedade civil.

Assumindo que o ciberespaço detém, por um lado, a capacidade de alocar um número infinito de páginas em linha sem custo adicional e, por outro lado, a possibilidade de desenvolver e de acompanhar os fluxos de informação em tempo mundial, pode considerar-se que representa uma ferramenta superior à de uma bomba nuclear dotada de capacidade de destruição global, não para o internauta comum mas para aqueles que pretendam desenvolver ações criminosas. Estas novas ame-

aças emergentes que começam a operar para além do alcance das fronteiras físicas têm vindo a fomentar o incremento da segurança e a gestão de risco do Estado, nomeadamente no tocante ao sistema informático localizado nas estruturas vitais institucionais bem como a constituição de uma nova força não militar representada por civis que saibam operar em caso extremo de ciberguerra.

Assim, presencia-se uma transformação da configuração dos setores da segurança e defesa que se projetam do Estado soberano para a realidade virtual, o que gera uma modificação da definição da política interna numa perspetiva internacional, dado que o ciberespaço não possui uma nacionalidade e/ou um território. Torna-se por conseguinte necessário, no sentido de proteger o Estado e respetivos cidadãos, o desenvolvimento de mecanismos de segurança e o reforço do papel do Estado enquanto entidade soberana e ator das relações internacionais, daí a perspetiva de David Rothkopf (1998) ao referir que a *realpolitik* de hoje não é mais do que a *ciberpolitik* de amanhã, concretamente por derivar do fator de poder, concernente a relevância estratégica e política do papel que o ciberespaço possa vir a desempenhar quer numa perspetiva das relações humanas quer nas relações internacionais. Diga-se de passagem que o poder que outrora seria reservado a determinadas potências com capacidade de projetar a ambição de domínio é na atualidade transferido e facultado no ciberespaço para aqueles que não detinham sequer essa possibilidade à escala global.

Por último, anotemos que garantia de um ambiente de segurança no ciberespaço significa o equilíbrio do sistema internacional na realidade contemporânea das relações internacionais. A emergência de novas ameaças que possam colocar em causa o equilíbrio mundial e provocar uma ciberguerra fora do campo de batalha convencional traduz-se num perigo não só para os Estados, mas para toda a humanidade. Todavia, acresce ainda que no quadro da gestão de risco, que constitua uma ameaça à segurança do território ou da sociedade civil, torna-se imperativo uma política de prevenção e de planeamento para tornar eficaz a ação perante o espectro da conflitualidade a levar a cabo quer numa perspetiva doméstica quer internacional. Daí que as Nações Unidas, através da *United Nations Interregional Crime and Justice Research Institute*, tenham na sua agenda a elaboração de um código de conduta internacional referente à utilização do ciberespaço e da envolvente política e jurídica do Estado em caso de intervenção na internet, concretamente na identificação do criminoso que poderá encontrar-se fisicamente localizado fora do domínio jurisdicional.

Bibliografia

Albright, David, Paul Brannan e Christina Walrond (2010). "Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?" Disponível em http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, data de acesso 18/9/2011.

Deibert, Ronald J. (2009). "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace" em Andrew Chadwick e Philip Howard (eds), *Routledge Handbook of Internet Politics*. London: Routledge, pp. 323-336.

Delbecque, Eric (2007). *L'Intelligence Économique: Une Nouvelle Culture Pour un Nouveau Monde.* Paris: PUF.

Ettighoffer, Denis (2008). *Netbrain, Planète Numérique: Les Batailles des Nations Savantes*. Paris: Dunod.

Godeluck, Solveig (2002). *Géopolitique d'Internet*. Paris: La Découverte.

Gray, Chris Hables (2005). *Peace, War, and Computers*. London: Routledge.

Haass, Richard (2008). "The Age of Nonpolarity: What Will Follow U.S. Dominance". *Foreign Affairs,* vol. 87, n.º 3, pp. 44-56.

Haraway, Donna (1991). *Simians, Cyborgs, and Women: The Reinvention of Nature.* London: Routledge.

Kohlmann, Evan (2006). "The Real Online Terrorist Threat". *Foreign Affairs*, vol. 85, n.º 5, pp. 115-124.

Lawson, Sean (2010). *General Alexander's Confirmation and the Failure of Cyberwar Transparency*. Disponível em http://www.forbes.com/sites/firewall/2010/05/13/general-alexanders-confirmation-and-thefailure-of-cyberwar-transparency/, data de acesso 19/7/2011.

Lemon, Sumner (2011). "Researchers track cyber-espionage ring to China". Disponível em http://www.csoonline.com/article/589717/researchers-track-cyber-espionage-ring-to-china?page=1, data de acesso 11/10/2011.

Lewis, James A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Disponível em http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, data de acesso 12/07/2011.

Lynn, William J. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy'". *Foreign Affairs*, vol. 89, n.º 5, pp. 97-108.

Mccaughey, Martha e Michael Ayers (2003). *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge.

Mcmillan, Robert (2010). "Was Stuxnet built to attack Iran's nuclear program?" Disponível em http://www.infoworld.com/d/security-central/was-stuxnet-built-attack-irans-nuclear-program110, data de acesso 15/10/2011.

National Strategy for Trusted Identities in Cyberspace. Disponível em http://www.whitehouse.gov/blog/2011/04/15/president-obama-releases-national-strategy-trusted-identities-cyberspace?utm_source=related, data de acesso 22/8/2011.

Noya, Javier e Beatriz Rodríguez (2010). *Teorias Sociológicas de la Globalización*. Madrid: Tecnos.

OpenNet Initiative. Disponível em http://opennet.net/. Data de acesso 26/9/2011.

Phillips, Macon (2009). *Introducing the New Cybersecurity Coordinator*. Disponível em http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cyber-security-coordinator, data de acesso 19/7/2011.

Rothkopf, David. (1998). "Cyberpolitik: The Changing Nature of Power in the Information Age" em *Journal of International Affairs*, vol. 51, n.º 2, pp. 325-359.

Rue, Frank La (2011). *Report of the Special Rapporteur on the Promotion and Protection of the rRght to Freedom of Opinion and Expression*. Disponível em http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, data de acesso 11/10/2011.

The Comprehensive National Cybersecurity Initiative. Disponível em http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative, data de acesso 23/07/2011.

Trendle, Giles (2002). "Cyberwar". *The World Today*, vol. 58, n.º 4, pp. 7-8.

United Nations Interregional Crime and Justice Research Institute. Disponível em http://www.unicri.it/, data de acesso 17/7/2011.

Whirled Bank. Disponível em http://www.whirledbank.org/, data de acesso 21/9/2011.

Wolton, Dominique (1999). *Internet et Après? Une Théorie des Nouveaux Médias.* Paris: Flammarion.

Diplomacia, Tecnologia e Informação

António Sérgio Mendonça

Licenciado em Economia e Mestre em Desenvolvimento e Cooperação Internacional (ISEG-Universidade Técnica de Lisboa). Pós-Graduado em Guerra da Informação/Competitive Intelligence pela Academia Militar e Mestre em Sistemas de Informação pela Escola de Engenharia da Universidade do Minho.

Resumo

O conservadorismo que tradicionalmente caracteriza os Ministérios dos Negócios Estrangeiros representa um desafio importante no contexto da Revolução da Informação. A existência de uma multiplicidade de concorrentes não estatais, indivíduos ou grupos, muito dinâmicos e ágeis, representa uma nova concorrência no exercício da atividade diplomática que, face às possibilidades de intervenção que os desenvolvimentos tecnológicos têm permitido, consegue obter uma influência política a nível global.

Neste contexto, questiona-se até que ponto tal não implicará, por parte dos agentes tradicionais, uma menor rapidez face aos novos concorrentes na resposta aos desenvolvimentos tecnológicos que vêm ocorrendo.

Por outro lado, a complexificação do ambiente comunicacional implica investimentos crescentemente mais fortes em tecnologias de comunicação e monitorização que, países com menos recursos poderão ter dificuldade em acompanhar, colocando em causa a tradicional superioridade estatal no domínio da informação.

Abstract
Diplomacy, Technology and Information

The conservatism that traditionally characterizes the Ministries of Foreign Affairs represents a major challenge in the context of the Information Revolution. The existence of a multiplicity of non-State competitors, individuals or groups, very dynamic and agile, represents a new competition in the exercise of diplomatic activity that, given the intervention possibilities that technological developments have allowed, manages to get a political influence at a global level. In this context, one have to ask to what extent this new communicational environment does not imply a slower response to technological developments by the traditional agents, when compared to the new competitors.

On the other hand, the complexity of the communicational environment requires stronger investments in communication and monitoring technologies, prohibitive to poorer countries, threatening the traditional State information superiority.

O conservadorismo que tradicionalmente carateriza os Ministérios dos Negócios Estrangeiros e uma nova concorrência no exercício de funções diplomáticas, constituem desafios importantes num contexto comunicacional de muito rápida evolução tecnológica. Constata-se hoje a existência de uma multiplicidade de concorrentes não estatais, muito dinâmicos e ágeis, que vêm aproveitando as possibilidades de intervenção política global que os desenvolvimentos tecnológicos têm permitido a indivíduos e grupos privados.

Neste contexto, questiona-se até que ponto não ocorrerá em alguns casos uma menor rapidez das estruturas estatais ou organizações internacionais face aos novos concorrentes na resposta aos desenvolvimentos tecnológicos que vêm ocorrendo.

Por outro lado, a complexificação do ambiente comunicacional implica inovação nos *media* e investimentos crescentemente mais fortes em tecnologias de comunicação e vigilância que países com menos recursos poderão ter dificuldade em acompanhar, colocando em causa a tradicional superioridade estatal no domínio da informação.

Tecnologia e Informação

A Revolução da Informação, em curso desde as décadas de 1960 e de 1970 veio revolucionar todo o ambiente comunicacional a um ritmo muito elevado obrigando a um esforço permanente de adaptação de todos os atores sociais. O nível de adaptação "será determinante no seu posicionamento relativo num contexto em que novas hierarquias se definem de modo cada vez menos dependente de fronteiras geográficas" (Mendonça, 2009: 14). Os rápidos avanços tecnológicos associados à Revolução da Informação, a nível informático, das comunicações e *software*, tal como sublinha Nye (2011: 114) vieram diminuir o custo de criar, processar, transmitir e procurar informação.

De entre os avanços tecnológicos deve ser destacada a importância assumida por evoluções tecnológicas nos modos de comunicação e que assentaram na "digitalização da comunicação, nas redes informáticas, no *software* avançado, na difusão em banda larga de grande capacidade e na comunicação local e global através de redes *wireless*, cada vez mais com acesso à internet" (Castells, 2009: 56).

Uma alteração fundamental refere-se à Web 2.0, que ao implicar uma comunicação nos dois sentidos requer uma adequada capacidade de escuta. A lógica 2.0 alterou também o modo de dar notícias, sendo crescente o número de cidadãos que acaba por ser fonte para canais noticiosos, através de blogues, *posts* ou comentários (Babst, 2011).

A maior expansão da internet a partir da última década do século XX justifica-se, em parte, por inovações tecnológicas como a banda larga ou a utilização generalizada de computadores pessoais que vieram gerar um crescimento exponencial da produção de informação.

Este crescimento rápido da informação produzida e partilhada veio criar um problema adicional, o do excesso de informação disponível.

Joseph Nye (2011: 115) realça que a quantidade de informação digital aumenta dez vezes a cada cinco anos. Os custos de transmitir informação tornaram-se dispensáveis, e a quantidade de informação que pode ser transmitida mundialmente é virtualmente infinita, o que vem gerar novos desafios como o da sobrecarga da informação.

O problema da sobrecarga da informação implica que mais importante que ter ou controlar a informação é saber como usá-la de forma objetiva com um fim específico.

Outra característica fundamental é sublinhada por Zanini e Edwards (2001: 35) e refere-se à importância da integração de tecnologias de informação e comunicação.

A integração tecnológica é uma das inovações tecnológicas mais significativas a nível da informação e comunicação. Traduz-se na convergência "de redes de telecomunicações, redes informáticas e redes de transmissão em redes digitais e novas tecnologias de transmissão e armazenamento de dados, particularmente de fibra ótica, comunicações via satélite e *software* avançado" (Castells, 2009: 58), aumentando significativamente o volume de informação disponível e a sua complexidade.

Redes

As redes estão na base do novo ambiente comunicacional existente que veio revolucionar a relação entre indivíduos, grupos e Estados.

Uma das caraterísticas fundamentais da Era da Informação é a conexão de computadores em rede com implicações na organização da sociedade. Para entender a sociedade, é hoje fundamental entender o funcionamento das redes. A disseminação de organizações rivais em rede obriga a que estas sejam combatidas por outras organizações estruturadas na mesma forma. Como afirmam Ronfeldt e Arquilla (2001: 15) "são precisas redes para combater redes".

Castells (2009: 19) define rede como um conjunto de nós interligados, sendo que esses nós podem ter uma importância diversa para a rede, sendo os nós particularmente mais importantes chamados de centros. A função de cada nó depende dos programas da rede e da sua interação com outros nós na rede.

Este autor sustenta que o processo de globalização só se tornou possível pela existência de capacidade de agir em rede globalmente possibilitada por tecnologias de comunicação digitais e sistemas de informação incluindo rápidas redes de transporte de informação por computador de alcance ilimitado, sendo este o elemento de distinção fundamental do atual processo de globalização em tamanho, velocidade e complexidade face a formas distintas de globalização em períodos anteriores.

A sociedade em rede global é altamente flexível e moldável a forças sociais, cultura e estratégias económicas e políticas, havendo um domínio sobre pessoas e atividades fora da rede sendo que o global sobrepõe-se ao local.

Outra inovação fundamental ocorrida a partir da última década do século XX refere-se à explosão da comunicação sem fios com capacidade crescente de conectividade e largura de banda em gerações sucessivas de telefones móveis. Foi "a tecnologia de difusão da comunicação mais rápida da história, atingindo hoje mais de metade da população mundial" (Castells, 2009: 62).

São múltiplas as aplicações que distribuem capacidade comunicativa através de redes sem fios, multiplicando os pontos de acesso à internet, pelo que no novo modelo de comunicações, a comunicação sem fios tornou-se na forma predominante de comunicação por todo o mundo. A capacidade de aceder à internet de um dispositivo sem fios tornou-se o fator crítico para uma nova onda de difusão da internet no planeta. Tal dependerá da construção de infraestruturas sem fios, de novos protocolos para a internet sem fios e da difusão de capacidade avançada de banda larga.

A explosão da comunicação sem fios vem adensar as preocupações quanto à possibilidade de o desenvolvimento das redes constituir uma ameaça cada vez mais séria à privacidade dos cidadãos (Mendonça, 2009: 50).

Castells (2009: 63) refere já existir a possibilidade tecnológica de uma rede quase ubíqua sem fios de banda larga, aumentando o potencial para comunicação multimodal de qualquer tipo de dado em qualquer tipo de formato entre quaisquer pessoas em qualquer lugar. No entanto, tal requererá a construção de infraestruturas e regulamentação adequada nacional e internacionalmente.

Tecnologia, Diplomacia e Governação

O trabalho de um diplomata, em boa parte, respeita ao uso da informação, trata-se da matéria-prima da diplomacia que fundamenta o trabalho de um diplomata. A Revolução da Informação veio, naturalmente, influir de forma significativa no modo como deve ser exercida a atividade diplomática.

Um dos efeitos mais importantes das tecnologias de informação e comunicação (TIC) refere-se às suas implicações nas estruturas das organizações.

Uma das implicações óbvias refere-se à necessidade de adaptação a uma sociedade em rede e de estruturar as organizações em rede, flexibilizando-as em detrimento de estruturas mais hierarquizadas e rígidas.

A este respeito, Rana (2011: 206) refere que as TIC requerem fluidez da informação do topo para a base e da base para o topo. Tentativas de controlo muito apertado da informação geram ineficiências para a organização. Situações em que funcionários controlam informação de forma apertada persistem em várias organizações, o que lhes pode dar uma vantagem no curto prazo, mas gera ineficiência e prejudica o conjunto da organização.

A prevenção deste tipo de desvios na organização requer a valorização mais objetiva das competências pessoais dos elementos da organização, competências essas que deverão preceder as profissionais.

Por outro lado, deverá valorizar-se a comunicação mais horizontal, diminuindo as chefias intermédias, fomentando-se a autonomia dos funcionários e a sua comunicação com o exterior.

Uma das questões fundamentais é a da redução do custo de transmitir informação. Nye (2011: 115) considera que a característica fundamental da Revolução da Informação não é a da velocidade mas a redução do custo de transmitir informação, baixando as barreiras à entrada.

Potenciou-se assim um poder acrescido para que os atores não estatais capturem funções tradicionais dos Estados. O acesso generalizado a fontes de informação e à computação em rede veio gerar concorrência à atividade diplomática tradicional (organizações não-governamentais, *media*, organizações terroristas, organizações ambientais, agentes individuais). São diversos os atores que aproveitam os recursos propiciados pelas TIC para interferir em acontecimentos de natureza global.

O exemplo do Irão é muito relevante pelo modo como o Twitter deu forma aos protestos estudantis, tendo o Departamento de Estado norte-americano solicitado o adiamento de uma operação de manutenção do *site*.

Na "Primavera Árabe" o papel das redes sociais foi também fundamental na mobilização de manifestações e na passagem de informação (Mendonça, 2011: 41).

Tal como sublinha Babst (2011), as pessoas, como ativistas, académicos, jornalistas e políticos usam a tecnologia de que dispõem (telemóveis, portáteis) para se informarem, para divulgar assuntos de interesse tanto local como global, para discutir questões políticas, organizar protestos públicos e para fugir à censura estatal.

Isto reflete uma maior interdependência mundial, a agenda política internacional é mais vasta com múltiplos atores transnacionais. Rana (2011) refere a existência de "um efeito de David" em que os mais pequenos se tornaram mais poderosos interferindo com as decisões dos tradicionalmente mais fortes, em que a Web 2.0 desempenha um papel importante sublinhando a importância dos blogues e das redes sociais.

Babst (2011) sustenta também que a internet transformou-se na praça pública virtual do século XXI em que ações individuais ou coletivas no Facebook, Twitter ou no *site* de vídeos YouTube têm um impacto no curso de eventos políticos internacionais.

A evolução das tecnologias de informação e comunicação está assim a mudar a natureza da governação aumentando a difusão do poder. "Muitas possibilidades de comunicação entre os cidadãos um para um (e-mail), um para muitos (página pessoal, blogues, Twitter), muitos para um (Wikipedia) e mais importante, muitos para muitos (Facebook, LinkedIn)" (Nye, 2011: 115).

Castells (2009: 27) considera mesmo que as redes globais de informação e tecnologia são as dominantes sobrepondo-se às "tecnologias/armas" militares. Considera que a mais importante fonte de influência hoje no mundo é a transformação das mentes das pessoas, pelo que, neste contexto, os *media* serão redes chave, por serem a primeira fonte de mensagens e imagens que chegam às mentes das pessoas.

Por outro lado, a tecnologia, nos tempos de hoje, permite que indivíduos e grupos marginais tenham ao seu alcance poderes que eram apenas públicos. Embora ciberespaço não substitua a escala geográfica e não vá abolir fronteiras, irá complexificar-se o que significa ser um Estado soberano ou um país poderoso no século XXI (Nye, 2011: 121-2).

No que se refere às consequências da Revolução da Informação ao nível das desigualdades entre os diferentes países não é claro qual o efeito predominante. Vimos que a diminuição dos custos de transmitir informação diminuem, possibilitando a multiplicação do número de atores dando poder a agentes individuais e coletivos que, *a priori*, dispunham de um poder reduzido. No entanto, podemos ter também um efeito contrário, existindo um aumento das desigualdades entre países pelos custos que as TIC implicam.

Como sublinha Rana (2011) a complexificação do ambiente comunicacional implica aumento dos riscos de interceção das comunicações, mecanismos de vigilância, que podem dissuadir os países com menos recursos de usar algumas das tecnologias.

Vulnerabilidades

A "Revolução da Informação" trouxe um conjunto de vulnerabilidades e novos desafios para os Estados como a alta dependência em sistemas complexos, a instabilidade política e possível perda de reputação.

A influência da internet em domínios políticos como a privacidade, a encriptação, a censura, o comércio eletrónico, o comércio internacional, a proteção da

propriedade intelectual, a fiscalidade, o cibercrime ou a guerra da informação requerem um acompanhamento diplomático atento (Denning, 2001: 250). Trata-se de domínios com uma componente externa relevante.

Outras vulnerabilidades características da era da informação e às quais deverá ser prestada atenção referem-se ao ativismo e ao "*hacktivismo*".

No âmbito do ativismo, Denning (2001: 243) sublinha a importância da internet para atores internacionais, facilmente acessível para atores não estatais permitindo a recolha de dados, a publicação, o diálogo, a coordenação da ação e o *lobbying* direto sobre os decisores políticos.

O "*hacktivismo*" definido como a combinação de "*hacking* com ativismo", com o *hacking* a referir-se a operações em computadores, por vezes ilegais, com a ajuda de *software*. "O *hacktivismo* inclui a desobediência civil no ciberespaço: *e-mail bombs*; *web hacks, computer break-ins*; vírus informáticos e *worms*" (Denning, 2001: 261).

Os Estados face às Redes Globais de Comunicação

A formação de uma sociedade em rede a nível global constitui um desafio exigente para os Estados. Esse processo, impulsionado por inovações tecnológicas tem como uma das suas traduções mais claras a formação das redes globais de comunicação. Existe assim uma "contradição entre a estruturação das relações em redes globais e o confinamento da autoridade do Estado-nação às suas fronteiras territoriais" (Castells, 2009: 39).

No entanto, como defende Castells, os Estados-nação continuam a ver as redes de governação como oportunidade para maximizar os seus interesses, olhando para a governação global como uma oportunidade de maximizar os interesses próprios, em vez de ser um contexto em que as instituições políticas partilham a governação em projetos comuns. "Pelo que quanto mais o processo de globalização avança mais contradições gera (crises de identidade, crises económicas, crises de segurança) levando a um fortalecer do nacionalismo e tentativas de restabelecer o primado da soberania" (Castells, 2009: 41).

Castells (2009: 44) considera que a influência das redes complexas de governação global imperfeita é tão grande que os Estados são condicionados por pressões de grupos de interesse, tendo de negociar com os *media* que transmitem as suas ações para os cidadãos.

Por outro lado, e numa tentativa de evitar a supremacia de novos competidores, Castells (2007: 191) sustenta que os governos põem obstáculos à difusão da tecnologia de encriptação como tentativa de manter controlo sobre os fluxos de informação em que fundamentaram durante séculos o seu poder.

Deste modo, no contexto da era da informação, a diplomacia adquire novas responsabilidades podendo corresponder ao que Ronfeldt e Arquilla (2001) apelidaram do exercício da *noopolitik*, um novo paradigma para a diplomacia que transcende a *realpolitik* e está mais adaptada a lidar com uma relação de forças reequilibrada entre Estados, mercado e atores da sociedade civil, estando mais apta a lidar com as redes globais. Num mundo interdependente, configurado pela informação e pela tecnologia, a capacidade para responder aos fluxos de informação é uma ferramenta essencial para fomentar uma agenda política.

Conclusão

A revolução da informação, a integração tecnológica e a formação de redes globais de comunicação representam um desafio enorme no exercício da atividade diplomática.

O controlo da informação já não é uma prerrogativa do Estado, podendo esse controlo estar também a passar em certa medida para agentes privados, eliminando o tradicional monopólio estatal neste domínio.

Por outro lado, ao desafio tecnológico corresponde também um desafio organizacional, no que se refere à adaptação das organizações a uma sociedade estruturada em rede. O exercício da *noopolitik* poderá ser uma forma eficaz de lidar com esses desafios, potenciando capacidades individuais das organizações diplomáticas, libertando os seus elementos, evitando bloqueios de informação dentro das organizações e adaptando-as ao novo ambiente comunicacional.

É essencial que os Ministérios dos Negócios Estrangeiros acompanhem as mudanças tecnológicas; existem indícios que apontam para o facto de que as múltiplas possibilidades oferecidas pelas TIC são ainda desaproveitadas (Mendonça, 2009).

É fundamental que os Estados se adaptem eficazmente aos desafios da sociedade em rede e ao ambiente comunicacional global para conseguirem defender os seus interesses face a um conjunto cada vez mais alargado de redes globais de atores que ameaçam muitas das suas competências tradicionais, tendo presente a regra enunciada por Ronfeldt e Arquilla (2001: 15) há mais de uma década "são precisas redes para combater redes".

Bibliografia

Arquilla, John e David Ronfeldt (2001). *Networks and Netwars: The Future of Terror and Militancy*. Santa Monica: RAND Corporation.

Babst, Stefanie (2011). "Security Policies 2.0: Can Facebook, Twitter and Co. Make an Impact?" (acedido 25 de julho de 2012 em www.atlantic-community.org/index/articles/view/Security_Policies_2.0%3A_Can_Facebook%2C_Twitter_and_Co_make_an_Impact%3F.)

Castells, Manuel (2007). *A Galáxia Internet, Reflexões sobre Internet, Negócios e Sociedade*. Lisboa: F.C. Gulbenkian.

Castells, Manuel (2009). *Communication Power*. Oxford: Oxford University Press.

Denning, Dorothy (2001) "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" in Arquilla, John e David Ronfeldt (eds), *Networks and Netwars: The Future of Terror and Militancy*. Santa Monica: RAND Corporation

Mendonça, António S. (2009). *Diplomacia na Era da Informação e Gestão do Conhecimento*. Dissertação de Mestrado em Sistemas de Informação defendida na Escola da Engenharia da Universidade do Minho sob orientação da Professora Doutora Isabel Ramos. Guimarães, 14 de dezembro de 2009.

Mendonça, António S. (2011). "Diplomacia Pública, Redes Sociais e Perspetivas Futuras da Atividade Diplomática". *Revista Segurança e Defesa*, nº 18 (Julho-Setembro de 2011), pp. 38-44.

Nye, Joseph (2011. *The Future of Power*. New York: Public Affairs.

Rana, Kishan (2011). *21st Century Diplomacy: a Practitioner's Guide*. London: Continuum Books.

Zanini, Michele e Sean Edwards (2001) "The Networking of Terror in the Information Age" in Arquilla, John e David Ronfeldt (eds), *Networks and Netwars: The Future of Terror and Militancy*. Santa Monica: RAND Corporation.

National Security Zone in International Cyber Affairs

Eneken Tikk-Ringas

The author has worked on different areas of technology and law as attorney, adviser to numerous Estonian authorities and lecturer at several universities. After building up and later heading the Legal and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn from 2006 to 2011, she joined Citizen Lab and the University of Toronto as a post-doctoral fellow for a year, also serving as strategic cyber security adviser to ICT4Peace Foundation in Switzerland. Eneken holds a PhD in law from the University of Tartu, Estonia.

Resumo

A Área da Segurança Nacional em Questões de Cibersegurança Internacional

O artigo descreve como os interesses nacionais no plano da cibersegurança estão interligados com instrumentos jurídicos, explicando como diferentes interpretações de conceitos como liberdade de informação, cooperação internacional ou direito à privacidade são contemplados em termos de Direito internacional. Analisam-se ainda ramificações quanto a abordagens governamentais relativas ao conceito de "segurança nacional", concluindo-se que nas atuais circunstâncias de fragmentação dos instrumentos legais associados à cibersegurança e ante a inexistência de acordo quanto ao que deve ser o comportamento aceitável dos Estados no plano do ciberespaço, os governos detêm uma larga latitude de discrição jurídica quando dela se socorrem para impor as respetivas perspetivas nacionais quanto a um equilíbrio entre a liberdade e a segurança.

Abstract

This article explains how national cyber security interests are entwined into international legal instruments and explains how different interpretation of concepts like freedom of information, international cooperation or the right to privacy can occur under international law. The article discusses the ramifications of governmental approaches to shaping and furnishing the concept of "national security" and concludes that under the circumstances of fragmentation of cyber security related legal instruments and in the absence of detailed agreement on acceptable state behaviour in cyberspace governments have a wide margin of legal discretion when using international legal and policy instruments to impose their national approaches to the balance of freedom and security.

Computers and networks have come to matter strategically. The emergence of the term "cyber security" itself represents an acknowledgment that turning back from a way of life powered by information technology is no longer conceivable. Whatever we have chosen or happened to connect to the Internet over time – our governments, homes, pets and passports – we now need to secure and protect. Dozens of deliberate, politically motivated confidentiality, integrity and availability disruptions known from the recent past confirm the emergence of vulnerabilities and threats on a strategic level.

Despite developing consensus on the potentially grave and wide-spread consequences of uses of ICTs for promoting political and military goals developing strategic responses has not turned out an easy task for the international community. While several governments have successfully handled large-scale cyber incidents in the recent past, international organizations are only starting to discuss acceptable state behavior and remedies available under international law. Given the natural cyber security divide stemming from the still considerable digital divide regional organizations seem to get better traction when developing confidence building measures and consolidating best practices.

An essential factor in international cyber security discussions is the concept of national security and how it relates to international peace and security concerns. While the former describes the margin of governmental discretion over a state's internal and external affairs, the latter is a representation of collective peace and stability interests. Neither of the two is a constant.

This article looks at the implementation of selected international legal instruments from a national security perspective, emphasizing that national security derogations from seemingly agreed international values can vary considerably. It addresses national security as an essential and practical element of collective cyber risk management and emphasizes the considerable margin of interpretation that governments have, at least theoretically, under international law when it comes to choosing appropriate means and methods for cyber security.

In the first part of the article freedom of information is used as a sample showcase of national approaches to balance freedom with security. After introducing a simplified outline of the right of individuals to receive and impart information and the limitations of such freedom under international legal instruments the article elaborates on the concept of "national security" in the second part and then highlights further national security exceptions in international legal instruments to frame governmental margin of discretion in addressing uses of ICTs from a national security perspective.

The author concludes that in the absence of international consensus regarding the applicability of international law in and to cyberspace, the still pending agreement on what would constitute responsible state behavior and a conclusion of which measures are necessary to increase transparency and confidence among state actors, national governments are in charge of legal and policy tools to impose their own approaches to balancing security with freedom.

Differences to Scoping Freedom and Security

What constitutes a "national security" issue is far from agreed among the international community. In fact, the degree of imposing national jurisdiction on persons, objects and events is often subject to tension and disagreement between governments.

In the context of uses of ICTs the extent of the freedom of information currently constitutes an apple of discord among three leading "cyber powers" – the United States, Russia and China. A brief look at international regulation of free flow of information offers a good example of possible margins of interpretation. To explain some inconsistencies and confrontation around the freedom of information, a simplified look at relevant legal instruments is useful.

In 1948 the Universal Declaration of Human Rights[1] articulated for the first time on an international level everyone's right to seek, receive and impart information and ideas through any media and regardless of frontiers in Article 19. It is further acknowledged under the Declaration that in conjunction to exercising the rights and obligations, everyone has duties to the community in which alone the free and full development of his personality is possible. Therefore, in the exercise of his rights and freedoms, everyone can be made subject to such limitations as are determined by law for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.[2]

A similar construct has been introduced in the International Covenant on Civil and Political Rights[3] (ICCPR), whereby everyone shall have the right to receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice (Article 19 (2)). Article 19 (3) notes that the exercise of this freedom carries with it

1 Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948.

2 Article 29 (1) and (2).

3 Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49.

special duties and responsibilities and may therefore be subject to certain restrictions, for respect of the rights or reputations of others and for the protection of national security or of public order (*ordre public*), or of public health or morals.

The European Convention of Human Rights[4] (ECHR) of 1950 similarly provides for the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Art. 10 (1)). Art. 10 (1) adds that this freedom shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. Article 10 (2) further admits that the performance of the freedom of information may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 (2) in broad terms explains the tools at governments' disposal to regulate or *ad hoc* mitigate situations that threaten national security. While the implementation of this freedom by the signatories to the ECHR is supervised and harmonized by the European Court of Human Rights, established to ensure the observance of the engagements undertaken under the Convention, not all countries are parties to the ECHR and therefore share the same views on the exercise and limitations of the freedom of expression.

The United States has proclaimed a seemingly unrestricted exercise of the freedom of information on the Internet, referring to Article 19 of the UDHR as a premise on an international level of the First Amendment, whereby Congress shall make no law abridging the freedom of speech. While limitations to the freedom of information are imposed by the U.S. to certain harmful content and obscene materials, the U.S. legal traditions reflect relatively high tolerance for offensive political and symbolic speech.[5]

China is the most widely discussed example how governments have effectively imposed restrictions on certain Internet content and services that are readily available in all countries members to the ECHR, not to mention the U.S. Restrictions on content and free flow of information have also been imposed by, *e.g.* Belarus, Saudi Arabia, Uzbekistan, and Thailand.[6]

4 Rome (1950), 4.XI.

5 For more detail about relevant court rulings, see http://www.uscourts.gov/EducationalResources/ClassroomActivities/FirstAmendment/WhatDoesFreeSpeechMean.aspx.

6 Freedom House, 2012. Freedom on the Net 2012: A Global Assessment of the Internet and Digital Media. Available at www.freedomhouse.org.

In justification of its approach to the freedom of the Internet China has referred to another UN General Assembly Resolution[7] from 1965. In this resolution the First Committee has concluded that no State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State and that all forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned. China has referred to the cultural traditions of its society as a justification to impose restrictions to "western" flow of information.

More recently, additional arguments presented by China and Russia in defense of imposing national restrictions to content highlight the Declaration of Principles on Building the Information Society: a global challenge in the new Millennium adopted by the World Summit on the Information Society (WSIS) in 2005. This instrument, reaffirming the freedom of information as an essential foundation of the Information Society, acknowledges that the exercise of this freedom can be limited by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.[8] It is noteworthy that the mandate of WSIS was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake.[9]

This simplified outline of the freedom of information in international law illustrates the potential margins of governmental discretion in establishing a national doctrine of free flow of information. The differences between nations highlight deviating considerations and rationale for governments to regard certain issues as a matter of national security or internal affairs. Further, having in mind the rise of politically motivated and increasingly organized nature of cyber incidents, one must critically ask if the WSIS principles from 2003 still reflect the full spectrum of national and international security concerns related to the uses of ICTs. Between the First Amendment approach of the US and the Great Firewall of China there are considerable shades of gray to operate in. While most governments seem to accept that the free flow of information is subject to certain limitations, the extent and even nature of such limitations are far from common sense.

7 United Nations General Assembly Resolution 2131(XX). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.

8 Paragraphs 4, 5 and 6.

9 UN GA Resolution 158/56.

The concepts of national security, public order as well as the balance between different rights and obligations are to be set by governments, at least while any more precise international consensus and widespread state practice is pending.

Cyber Security: What's in the Word?

"Cyber security" is a word pair coined to cover aspects of uses of ICTs that in the light of incidents with large-scale effects and political context go beyond technical security. One rarely encounters this term in computer and network security jargon as "cyber" is highly indistinctive of any subject matter it potentially pertains to. After all, according to popular meaning of "cyber"[10] it can encompass unmanned aerial vehicles, military command and control systems, cars, bridges, home appliances, toys and even animals and humans with certain type of implants.

"Cyber security" in contemporary government use emphasizes a strategic need or rationale behind technically securing certain assets and functions. According to the UK's 2009 strategy "cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers. /…/ Government's ultimate goal is to enable the full benefits of cyber space for the UK".[11] More often than not it invokes strategic questions and decisions about the ends, ways and means of technical security, thus adding the national security (and potentially the international peace and security) dimension to it.

While all uses of ICTs bring up the need of technical protection, their vulnerabilities and exposure to threats and threat vectors as well as the strategic rationale and prioritization of protection from a national security perspective are different for potential military objectives, civilian objects, commodities of different criticality and goods and services of convenience. This, however, does not always follow from the use of words in national strategies and agendas of international organizations.

For some time, international community used to exploit the word to primarily reflect military security concerns and remedies. These days, national and international security concerns are equally, if not more, focused on terrorism, energy, climate and economy. Although some see "cyber" as a separate category of new security challenges,[12] it would be equally correct to regard information technology

10 According to the Merriam-Webster Dictionary, "cyber" refers to "of, relating to, or involving computers or computer networks (as the Internet)."

11 Cyber Security Strategy of the United Kingdom (2009).

12 See, e.g. Tackling New Security Challenges, NATO Briefing from January 31, 2012. Available at http://www.nato.int/cps/en/natolive/topics_82708.htm.

as a component and factor part of an increasing amount of contemporary state, industry and private functions.

Based on Wolfers (1952), Ullman (1983), Baldwin (1997), Nye (2012) and others it seems to be acknowledged that the scope and focus "national security" are not constant and that military is but one dimension of security and national power shaping today's international affairs. The realities of the Great Depression, Cold War, control over technologies and now cyber, all have raised national security concerns at their own times.

Despite the haziness of "national security", it is possible to delineate it from other interests. National security serves the fundamental and persistent interests of a nation that are expected to rise above the narrow and special interests of parts of the nation yet stay below the concern of "interests of all mankind". Therefore, exercising national security naturally conflicts with international peace and security concerns. The concept of international peace and security would counterweigh national security in cases where ambitions or action of one nation threaten the peace and security of others. The mechanisms of international peace and security related measures and decision-making have been conveyed to the UN Security Council. Uses of and concerns surrounding ICTs differ considerably depending on the geopolitical, economic and societal factors characterizing the "Information Society" in different regions and states.

One needs to note that even with the event of computer security rising to the interest threshold of national security not all concerns related to uses of ICT become a strategic issue *per se*. Wolfers (1952: 481) notes that when specific policy formulas gain popularity (as "cyber security" is today) one must carefully scrutinize such concepts to avoid permitting everyone to label whatever policy he favors with an attractive name.

A look at national input to the UN First Committee discussions on International Information Security reveals that governments are equally or even more concerned with Internet governance, CERT development and law enforcement issues than they are with politico-military uses of ICTs. It is definitely questionable if all those issues are of same strategic relevance. It is essential to observe that national security remedies present themselves as (weighed and identified) alternatives to principles and policies governing the same topic if they fall within this particular area of interest.

The importance of categorizing certain objectives and issues as relevant to national security invokes a set of legal consequences empowering governments with considerable additional discretion as to balancing freedoms with security. As Nissenbaum notes, in the face of securitized threats and times of national crises, even liberal democracies accept breaks from "business-as-usual" including: (1) reduced restraints on government powers, frequently manifested in the curtailment of civil

liberties; (2) breaks from normal democratic procedure, including government secrecy normally not tolerated by citizens and (3) steep incremental funding for security agencies and infrastructures.

The flabellum of all contemporary cyber security interests is impossible to describe in meaningful detail. A few to address would be a general disagreement between liberal democracies and the Shanghai Cooperation Organization countries as to what extent is state control justified over content and the free flow of information; a principal disagreement on how the Internet should be governed and to what extent and how the international legal instruments apply to state and non-state behavior online.

Added to it nations have different immediate concerns and interests. Some are entering the curve of growing organized cyber crime, some are just building up their information infrastructure while others have started developing and deploying information technology for military use. It is therefore challenging to find a common denominator for all national concerns.

There is, however, more and more common ground to cover. The emergence of semi-political cyber protest movements like Anonymous, persistent growth of systematic and sophisticated cyber crime, concerns of cyber conflict escalation and avoidance of collateral damage of state-sponsored cyber operations represent but a small set of issues to be settled collectively for the continuous prosperity and economic benefits of the Internet. For some countries the threat has materialized more than for others.

National Security in Selected International Legal Instruments

Assuming nations are increasingly going to make use of their sovereign right to exercise control over their area of jurisdiction and use the argument of national security to enforce their strategic goals, a peek into other international treaties will offer some ideas about the potential of such arguments.

Article 27 (4) of the Budapest Convention on Cyber Crime entitles a Party to refuse assistance under the Convention if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or if the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests. This means that at least from a purely legal perspective a state can choose not to apply the Convention in case such a decision supports its national interests.

Article 34 of the ITU Convention allows Member States to cut off, in accordance with their national law, telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.

The relevance of the ITU Convention to cyber security is currently under debate. Even if ITU is not seen as a strategic security player, an exercise of the right of stoppage of telecommunications on simply technical infrastructure level by a government may result in considerable consequences for the international community.

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 9 (2)) allows derogation from the provisions of this convention as provided for by the law of the Party when it constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences or is necessary for protecting the data subject or the rights and freedoms of others.

When it comes to the involvement of Internet Service Providers (ISPs) in security of services on their networks, the general exception of ISP liability is also only limited to non-national security matters. Article 3(4) of the E-Commerce Directive allows Member States to derogate from its provisions in the interests of public security, including the safeguarding of national security and defense. Considerable obligations for cooperation are established to communication providers under the Data Retention Directive.

These exceptions represent just a small selection of legal tools supporting the exercise national power over persons, events and objects constituting a national security concern. Although the legitimacy of such concerns may be and often is subject to an international debate, it will be the primary task of states to define their scope of national interests and applicable remedies to protect such interests. Laws and policies addressing critical information infrastructure represent an approach taken by several countries to identifying objects of heightened protection value.

It seems to be accepted in the international community that making uses of national security derogations requires support from national law. Only under extraordinary circumstances governments can exercise their authority *ad hoc* to characterize an incident as one of national security concern. Generally, however, it is expected that governments act transparently and adopt national laws that explain the margins of authoritative engagement n case of a threat to or breach of national security.

As observed in above considerable differences may occur in national interpretation of different tights and freedoms. Such differences are expected to be less drastic among allied, regionally and circumstantially connected state actors. Still, the currently evident cyber security divide should remind the stakeholders of the importance of uniform implementation of international legal instruments and about potential issues related to overlaps and contradictions in legal instruments.

Conclusion

How to have a free, open, peaceful and stable cyberspace is a question with security and defense on the flip side. Internationally balancing relevant interests can only go half way as it is virtually impossible to unify, prioritize and remedy national and regional issues on a global scale.

This article has used the freedom of information as an illustration of the margin of interpretation involved in implementation of international law. It has emphasized the zone of national security responsibilities between individual and corporate obligations and regional and international organizations' involvement in cyber incident handling, warning that the concept of national security may not offer a broad consensus as to its scope and accepted margins.

Further drawing the reader's attention to several provisions in multilateral legal instruments that provide for derogations from criminal cooperation, availability of telecommunication services and other rights and freedoms established on international level, the author concludes that in the absence of international consensus regarding the applicability of international law in and to cyberspace, a still pending agreement on what would constitute responsible state behavior and a conclusion of which measures are necessary to increase transparency and confidence among state actors, national governments are in charge of legal and policy tools to impose their own approaches to balancing security with freedom.

References

Baldwin, David (1997). "The Concept of Security". *Review of International Studies* n. 23, pp. 5-26.

Nye, Joseph (2012). *TED Talks. Cyber Influence and Power*. iTunes University podcast.

Ullman, Richard (1983). "Redefining Security". *International Security* n. 1, pp. 129-153.

Wolfers, Arnold (1952). "National Security as an Ambiguous Symbol". *Political Science Quarterly* n. 4, pp. 481-502.

Russia and Cyber Security

Keir Giles

Keir Giles is a director of Conflict Studies Research Centre (CSRC), a UK think tank specialising in Eurasian security affairs. After a firstdegree in Russian, Keir worked in aviation in the former Soviet Union before joining the BBC Monitoring Service to report on Russian economic and military affairs. A secondment to the UK Defence Academy led to work with CSRC, which Keir took into the private sector in 2010.

Resumo
A Rússia e a Cibersegurança

O artigo examina os conceitos russos de "guerra da informação" e a forma como afetam a política da Rússia face ao ciberespaço, através da análise de documentos oficiais recentemente tornados públicos, a saber: uma proposta de uma convenção internacional, e uma proto-doutrina militar de cibersegurança. Procura-se demonstrar que existe um fosso conceptual face ao Ocidente, o qual mina as possibilidades de um acordo mútuo baseado em princípios e regras comuns de utilização do ciberespaço, apesar das repetidas tentativas russas em sujeitar estas normas a aprovação por parte de outros Estados. Assim, serão necessários mais esforços no sentido de um maior e melhor entendimento conjunto se se pretender estabelecer e fortalecer uma confiança e segurança mútuas.

Abstract

This paper examines Russian "information warfare" concepts, and how they affect the Russian approach to cyberspace, through the analysis of recently released public statements of Russian policy on cyberspace: one proposed international security convention, and one military cyber proto-doctrine. It will show how the conceptual gap with the West undermines attempts to reach agreement on common principles or rules of behavior for cyberspace with Russia, despite repeated Russian attempts to present norms of this kind to which other states are invited to subscribe. Further efforts to achieve mutual understanding are essential if meaningful confidence and security building measures are to be realized.

Introduction

Russia and a range of Western nations have expressed the desire to cooperate more closely in cyber security, in particular in order to build confidence and security in cyberspace (Gorman, 2010; Blitz, 2012). But there are significant differences between the Russian and Western (for example US, UK, NATO) approaches to cyber warfare, and even between definitions of basic cyber terminology, and this severely hampers mutual understanding and cooperation in this area (Giles, 2011a). According to Russia's Communications Minister Igor Shchegolev, "for the time being, in the West not everybody always understands what rules we are following" (Interfax, 2011). This remains true despite the fact that Russia has for over a decade been attempting to gather international support for these rules in a variety of international *fora* including the United Nations (Maurer, 2011) and others (Gjelten, 2010).

In particular Russia has deep concerns on the principle of uncontrolled exchange of information in cyberspace, and over the presumption that national borders are of limited relevance there. Circulation of information which poses a perceived threat to society or the state, and sovereignty of the "national internet", is a key security concern in Russia, but not recognized as such in the West. Russia is not alone in this, and similar concerns inform the Chinese approach to information security, which makes the achievement of mutual understanding with China on cyber security issues similarly challenging (Hagestad, 2012).

This paper examines Russian "information warfare" concepts, and how they affect the Russian approach to cyberspace, by means of studying recently released public statements of Russian policy on cyberspace: one proposed international security convention, and one military cyber proto-doctrine. It will show how the conceptual gap with the West undermines attempts to reach agreement on common principles or rules of behavior for cyberspace with Russia, regardless of the repeated Russian attempts to present norms of this kind to which other states are invited to subscribe.

Definitions and Concepts

When attempting to have a conversation about cyber issues across the language gap between English and Russian, literal translations of common terms used in discussing cyber are almost always unhelpful and misleading. In the most fundamental example, Western states talk about cyber security as a stand-alone issue, while Russia considers it more sensible to discuss information security as an

overall holistic concept, implicitly including cyber security as a subset of concerns. The lack not only of a common vocabulary but even of common concepts relating to cyberspace means that even when attempts are made to find common ground, these attempts soon founder.

In at least one instance, intensive and sincere efforts to bridge the divide have only succeeded in sowing further confusion. The "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations" published by the EastWest Institute in April 2011 appeared at first sight to be a major step forward in achieving a common basis of understanding for the 20 key terms it selected for definition in both Russian and English; it only became clear on closer inspection that neither was this a "Russia-US bilateral" document, nor did the definitions in Russian and English actually match up with each other[1] – so in fact, the document represents a step backward by giving the impression of agreement where in fact none exists (East-West Institute, 2011b). Perhaps fortunately, an attempt in October 2011 to expand the list of definitions to a further 20 terms does not as yet appear to have borne fruit (EastWest Institute, 2011a).

The failure to achieve a common understanding of even the most fundamental concepts in cyberspace between the US, Russia and China to name but three is recognised, and is the subject of ongoing work at a number of levels. One of the topics chosen for the flagship annual conference of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2013 is "Defining cyber conflict, cyber war, cyber attack, cyber weapon, etc.; (non-)essentiality and (non-)feasibility of a common terminology" (CCDCOE, 2012).

The Problem of Content

Dialogue between Russia and Western partners on cyberspace issues is hampered not only by a difference in understanding of specific concepts, but also in fundamental assumptions and in norms which are taken for granted by one side but seen as threatening by the other. One such assumption regards the free circulation of information on the internet.

1 To take one example, the definition of "Cyber Warfare" in English reads "cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign". The Russian text, however defines cyber warfare as "cyber attacks carried out by states or groups of states or organised political groups against cyber infrastructure and which are part of a military campaign" (кибератаки, проводимые государствами (группами государств, организованными политическими группами), против киберинфраструктур, и являющиеся частью военной кампании).).

The consensus among Western states is voiced at international events like the London International Conference on Cyberspace on 1-2 November 2011, and is also expressed in a number of published international documents, for example the Organisation for Economic Cooperation and Development (OECD) recommendations on principles for internet policy making. (OECD, 2011). It is regularly stated as a fundamental principle in the West "that cyberspace remains open to innovation and the free flow of ideas, information and expression", as put by UK Foreign Secretary William Hague (2011) and others at the London Conference. The Western consensus recognises the threat from hostile code, but generally discounts the issue of hostile content. The OECD (2011) recommendations, for example, include:

> "free flow of information and knowledge, the freedom of expression, association and assembly, the protection of individual liberties, as critical components of a democratic society and cultural diversity".

Yet at the same conference, Russian Communications Minister Igor Shchegolev (2011) attached important caveats to the principle of free flow of information. This illustrates a key divergence between Russian and Western approaches to cyber security, namely the Russian perception of content as threat (Giles, 2011a). In Russian documentation, this is expressed as the "threat of the use of content for influence on the social-humanitarian sphere."

In part this results from Russian concerns that the internet can be used as a tool against Russia. The notion of content as threat is reinforced by projection onto foreign partners of Russia's own preconceptions of how international relations work, and by the presumption that a primary aim of Western powers is to disrupt and undermine Russia. As renowned expert on Russian information warfare theory Timothy Thomas (2011) points out:

> "Disinformation is a Russian technique that manipulates perceptions and information and misinforms people or groups of people. Some disinformation techniques are quite obvious, some are unconvincing, and others work through delayed perception, rumours, repetition or arguments. Specific persons or particular social groups can serve as disinformation targets... In Russia today, where an unstable public-political and socio-economic situation exists, the entire population could serve as the target of influence for an enemy disinformation campaign. This is a major Russian fear".

This extends to the promotion of democratic ideas: at a U.N. disarmament conference in 2008 (UNIDIR, 2008), a Russian Ministry of Defence representative suggested that any time a government promoted ideas on the internet with the intention of subverting another country's government, including in the name of democratic reform, this would be qualified as "aggression" and an interference in internal affairs (Gjelten, 2010).

Behind and beyond direct Russian concern about targeted information attack lies a deeper and more nebulous unease about the vulnerability of Russia's national culture to outside influences – perhaps understandable in a nation which, as Timothy Thomas (2010) puts it, is "armed mentally with the experience of losing an ideology at the end of the Cold War (described by some as 'World War III')". This is another facet of the holistic approach to information security in Russia which is largely unrecognized in the West, but is expressed in Russia's Information Security Doctrine, the underpinning document defining Russia's approach to cyber issues, which includes as threats:

> "the devaluation of spiritual values, the propaganda of examples of mass culture which are based on the cult of violence, and on spiritual and moral values which run counter to the values accepted in Russian society" (Security Council of the Russian Federation, 2000; Sheynis, 2010).

Thus while both sides publicly espouse the freedom of exchange of information, and thus occasionally give the illusion of consensus, the Russian reservations on how far this principle can safely be extended mean that in practical terms the two views are poles apart.

Internet as Threat

This is symptomatic of a still deeper dissonance between attitudes to the internet in Russia and the West. Put simply, while the Western view of the internet is almost universally that of an opportunity and an enabler, significant sections of the Russian authorities see it instead as a threat.

In 1996, Russia faced a strategic choice of whether to embrace or reject the internet. At parliamentary hearings entitled "Russia and the Internet: The Choice of a Future," the internet as a whole was characterized as a threat to Russian national security by Vladimir Markomenko, First Deputy Director General of FAPSI, the Russian security body which at the time was responsible for cyber affairs (State Duma, 1996). This attitude can still be detected today. Speaking in April 2011, the head of the Federal Security Service (FSB) Information Protection and Special Communications Centre, Aleksandr Andreyechkin, said that:

> "Recently the problem of usage on public communications networks of encryption mechanisms, primarily of foreign manufacture, has been causing the FSB increasing concern... in particular services like Gmail, Hotmail and Skype… The uncontrolled use of these services could lead to a large-scale threat to the security of Russia".

While the real extent of this concern has been called into doubt, with some suggesting that the comments were a canard intended to lull transgressors who were using foreign internet services to exchange dubious content into a false sense of online security, the public statement does point to a continuity of views among the security structures, which continues to inform Russian attitudes to online activity and to cooperation with foreign partners.

Information Warfare and Information Weapons

Debates in the West over the nature of cyber conflict are followed with interest in Russia (Shavayev and Lekarev, 2003; Sharikov, 2009) but are not mirrored in the Russian public narrative. For example, considerations of whether cyberspace is the "fifth domain" for warfare, or simply is a common factor to the other four, did not feature in discussion visible in open sources, except in citations of Western thinking – in fact the word "cyber" is strikingly absent from home-grown Russian analysis, which until recently portrayed "cyber warfare as a purely American phenomenon, with the Chinese People's Liberation Army in a supporting role" (Sidorov, 2008; Shcherbakov, 2010).

Instead, the Russian view of "information war" (*informatsionnoye protivoborstvo, informatsionnaya bor'ba*, or increasingly commonly, *informatsionnaya voyna*) is a more holistic concept than its literal translation suggests, carrying cyber operations implicitly within it alongside disciplines such as electronic warfare (EW), psychological operations (PsyOps), strategic communications and Influence. At a time when the term has been written out of US information operations doctrine (Joint Chiefs of Staff, 2006), "information war" is still alive and thriving in Russian security considerations (Thomas, 2000; 2002; 2010).

This principle in Russian writing extends to the notion of "information weapons" – signifying a much broader tool than what we might call a cyber weapon. One characteristic study issued in 2001 noted that "propaganda carried out using the mass media is the most traditional and most powerful general-purpose information weapon," but furthermore that "information weapons are being actively developed at the present time based on programming code" – a definition which we would more readily associate with our own view of cyber weapons. As a further illustration that the Russian concept is broader and more holistic than in the West, the study went on to note that "information weapons also include means that implement technologies of zombification and psycholinguistic programming"(Fedorov and Tsigichko, 2001).

Treaty Initiatives

These Russian concerns and specific Russian views of cyberspace inform the long-standing Russian attempts to introduce international treaties or agreements to restrain the activities of states in cyberspace. As put by Professor Igor Panarin (2004) of the Russian Ministry of Foreign Affairs (MFA) Diplomatic Academy, the author of one of the standard works on Russian theory of information war, Russia needs to use "the mechanisms of the UN and the mechanisms of Russian-American consultations to create new rules of the game, rules of information balance and rules for protecting our sovereign national information space" (Panarin, 2009).

At roughly the same time as the Western consensus was being expressed by events such as the London International Conference on Cyberspace and the OECD recommendations for internet policy referred to above, a "Draft Convention on International Information Security" was released at an "international meeting of high-ranking officials responsible for security matters" in Yekaterinburg, Russia. The draft neatly illustrates many divergences between Western and Russian preconceptions about the nature of the internet and the basic assumptions on how it should be governed.

- The principle of indivisibility of security is highlighted in the draft Convention. This is a principle also espoused by Russia's foreign partners, including the US – but here again apparent consensus hides fundamental disagreement, simply because this common phrase has entirely different meanings in Russian and in English. Despite recognition and patient explanation that use of the identical phrase to refer to widely differing concepts leads to misunderstanding and frustration (NDC, 2010), the phrase continues to occur in both Western and Russian discourse leading to each side embarking on their own separate conversation (Monaghan, 2011).
- The draft's mention of a "dominant position in cyberspace" refers to the idea of "information space [being] a place of competition over information resources... The USA is currently the only country possessing information superiority and the ability significantly to manipulate this space" (Modestov, 2003). This is a concern largely unrecognised in the West.
- "Internet sovereignty" is another key area of disagreement. Russia, along with a number of like-minded nations, strongly supports the idea of national control of all internet resources that lie within a state's physical borders, and the associated concepts of application of local legislation - or as worded in the draft Convention itself, "each member state is entitled to set forth sovereign norms and manage its information space according to its national laws" (Article 5.5). These like-minded nations are to be found primarily among the Collective Security Treaty Organisation (CSTO), the

Commonwealth of Independent States (CIS) and the Shanghai Cooperation Organisation (SCO) – groups of states which have already made progress in formulating a common approach to cyber security. The CSTO has a "Program of joint actions to create a system of information security of the CSTO Member States" (Collective Security Treaty Organisation, 2012) while the SCO has concluded an "Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security" (Shanghai Cooperation Organisation, 2009; Giles, 2011b). Yet this sovereignty approach is in direct opposition to the approach of, for example, the USA, as expressed firmly by US Secretary of State Hillary Clinton (2011) in December 2011, saying that countries like Russia wished to:

> "empower each individual government to make their own rules for the internet that not only undermine human rights and the free flow of information but also the interoperability of the network. In effect, the governments pushing this agenda want to create national barriers in cyberspace. This approach would be disastrous for internet freedom".

- A section in the draft Convention covers states ensuring that information infrastructure within their own jurisdiction is not used for offensive activity, and cooperating in order to identify the source of such activity (Article 6.2). Consideration of the practical implications of a stipulation of this kind, and the obligations it entails, leads quickly to the realisation of an enormous legislative and administrative burden on states which might wish to subscribe to the draft Convention. Not only must they supervise the legality of content within their own jurisdiction, but also ensure that it is considered inoffensive and non-hostile in the jurisdictions of all other signatories – otherwise, they can immediately be accused of permitting hostile activity in breach of the Convention.

Another key stipulation which is gravid with misunderstanding is the provision for taking "necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party which are legally implicated in being employed for the perpetration of terrorist activities in information space" (Article 9.5). Two important areas of conceptual divergence arise here: first, the word "terrorist", and second, the issue of access to a foreign state's information space.

Conceptual differences in the understanding of the nature of "terrorism" between Russian and other states provide an additional layer of complexity and indeterminacy to the already muddied picture of what constitutes "cyberterrorism". As described by Anna-Maria Talihärm (2010), Alex Michael (2010) and others,

"there is a great abundance of different definitions of the idea of 'terrorism'... the addition of the prefix "cyber" has only extended the list of possible definitions and explanations". Thus without consensus with Russia on what precisely is covered by "perpetration of terrorist activities in information space", this clause remains unusable. Such consensus is unlikely to be achieved given the fundamental and unresolved differences between the two sides on what constitutes both terrorism and counter-terrorist activity (Monaghan, 2010).

At the same time the call for authorised access to information infrastructure in another state's jurisdiction is reminiscent of the text of Article 32 of the Council of Europe Convention on Cybercrime (the Budapest Convention):

> "A Party may, without the authorisation of another Party... access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system" (Council of Europe, 2001).

Yet this text constitutes Russia's main objection to ratification of the Budapest convention (Sherstyuk, 2011). The key phrase which prompts Russian objections is "without the authorisation of another Party". In the Russian view, this is an intolerable infringement on the principle of sovereignty as described above. In addition, the range of options covered by "the person who has the lawful authority to disclose the data" is a source of concern, including as it may organisations other than the State. Russian concerns over practical application of the Budapest convention are illustrated by a report in the official government newspaper which highlighted the "dubious provision for foreign special services to invade our cyberspace and carry out their special operations without notifying our intelligence services" (Borisov, 2010).

It should come as little surprise, therefore, that while the provisions of the draft Convention appear perfectly sensible to Russia and other states holding similar views on the nature of the internet, they are largely incomprehensible to the Euro-Atlantic community and are therefore receiving a less than sympathetic hearing there.

The Russian Military and Cyberspace

Another recently-released document illustrating key differences between the Western and Russian approaches to cyber issues is the "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space", released in December 2011 (Russian Ministry of Defence, 2011). This, the first official doctrinal statement on the role of the Russian military in cyberspace, describes cyber

force tasks which bear little resemblance to those of equivalent commands in the West. The differences from published doctrine in the US or UK are substantial. In particular, the "Views" contain no mention of the possibility of offensive cyber activity. The document is entirely defensive in tone, and focuses on force protection and prevention of information war, including allowing for a military role in negotiating international treaties governing information security.

At first sight, this would seem a continuation of the pattern whereby offensive cyber activity is not seen as the domain of the military. Following mixed performance in the information aspects of the armed conflict with Georgia in 2008, there was intense discussion of the possible creation of "Information Troops", whose role would include cyber capability; but this initiative was publicly scotched by the Federal Security Service (Giles, 2011a).

Indeed the vast majority of Russian public writing on cyber conflict is defensive in tone, and focused on information security and information assurance. This is at least in part a response to official discussion of cyber issues in the US in particular, where reference to defense against hostile cyber operations is balanced with references to carrying out offensive cyber operations in return. It remains the case that the stated aim of US information operations is "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own" (Joint Chiefs of Staff, 2006) – and despite careful avoidance by the USA of casting the Russian state in the role of an adversary in cyberspace, this language is mirrored in Russia's Information Security Doctrine, which emphasizes:

> "the development by certain states of 'information warfare' concepts that entail the creation of ways of exerting a dangerous effect on other countries' information systems, of disrupting information and telecommunications systems and data storage systems, and of gaining unauthorized access to them" (Security Council of the Russian Federation, 2000).

The "Conceptual Views" is a specifically Russian document, and does not resemble its foreign counterparts, for example the US Department of Defense Strategy for Operating in Cyberspace (US Department of Defense, 2011) – not only through references to supporting doctrinal documents (the Military Doctrine and Information Security Doctrine of the Russian Federation) but also in its underlying presumptions and definitions of information challenges. It reflects a long-standing Russian presumption not only that potential operations in information space pose an entirely new set of challenges (Lisovoy, 1993), but also that foreign concepts of information security, along with those of other areas of military endeavour, are not applicable to Russian circumstances – as expressed in 1995 by prominent Russian military commentator Vitaliy Tsymbal (1995):

> "It is false to presume that we can expediently interpret and accept for our own use foreign ideas about information warfare (IW) and their terminology in order to avoid confusion and misunderstanding at international discussions, during information exchanges, or during contact between specialists. Quite the opposite, it makes no sense to copy just any IW concept. Into the IW concept for the Ministry of Defence of the Russian Federation (RF) must be incorporated the constitutional requirements of the RF, its basic laws, specifics of the present economic situation of the RF, and the missions of our Armed Forces".

With the exception of references to the economic situation, this is precisely what the "Views" have done. They echo the defensive theme of other Russian documents relating to cyberspace, including the draft Convention described above, and cite in their preamble a statement of the external threat to Russia's information security arising from other states developing information warfare concepts (Giles, 2011a). Further, they state that "a targeted system of activity has been established in the Armed Forces of the Russian Federation intended to provide for effective deterrence, prevention and resolution of military conflicts in information space".

The definition of the information war which the Armed Forces are called upon to deter and prevent is worth citing in full, as it illustrates once again the enduring holistic nature of the Russian perception of information warfare and cyber conflict as an integral part of it. Information war, according to the "Views", is "conflict between two or more states in information space with the aim of causing damage to information systems, processes and resources, critically important and other structures, subverting the political, economic and social systems, mass psychological work on the population to destabilise society and the state, and coercing the government to take decisions in the interests of the opposing side" (Section 1, Fundamental Terms and Definitions - emphasis added).

Legality (or, we should say, conforming to Russian law and international law as interpreted by Russia) is emphasised as the first principle governing military activity. Along with customary references to the primacy of international law, and the principle of non-interference in the internal affairs of other states, the Views note that use of the Armed Forces outside the Russian Federation is subject to a process of Federal Assembly approval, and states that "this provision should also be extended to the use of the Armed Forces of the Russian Federation in information space" (Section 2.1, Legality). The "Views" also make provision for "deploying forces and resources to provide for information security on the territories of other states" (Section 3.2, Resolving Conflicts) – which leads progressively-minded non-military Russian internet experts to speculate wryly on the picture of "commandos parachuting into server centres, iPads in hand".

The first priority for the Armed Forces is stated as "striving to collect current and reliable information on threats" and developing countermeasures - but this is explicitly for military purposes. The aim is primarily to protect military command and control systems and "support the necessary moral and psychological condition of personnel". This has become essential since "now hundreds of millions of people (whole countries and continents) are involved in the unified global information space formed by the internet, electronic media and mobile communications systems". What is absent is mention of a military role in assessing or countering threats to broader society or the Russian state (Section 2.2., Priorities).

Russian military activity in information space "includes measures by headquarters and actions by troops in intelligence collection, operational deception, radioelectronic warfare, communications, concealed and automated command and control, the information work of headquarters, and the defence of information systems from radioelectronic, computer and other influences". Yet once again, in common with other Russian public statements, and in contrast to similar statements from other nations (Miles, 2011a) and overt preparations by those states (Miles, 2011b), what is absent from the Views is any mention of offensive cyber activity (Section 2.3, Complex Approach).

Also in contrast to foreign doctrinal statements, the "Views" list "the establishment of an international legal regime" regulating military activity in information space as the main aim of international cooperation with "friendly states and international organisations" (Section 2.5, Cooperation).These friendly organisations are later defined: the priorities are the CSTO, CIS and SCO, which as noted above have already made substantial progress in formalising their shared views on information security; views which are in line with those of Russia. But in addition to this, the military are supposed to "work for the creation under the United Nations of a treaty on international information security extending the remit of commonly-accepted norms and principles of international law to information space". The Russian military is thus intended to have an explicit political role in promoting initiatives like the draft Convention on International Security referred to above, beyond simply having a voice in their drafting or having places on delegations; not a role which would sit naturally with most Western militaries.

In fact, although it was announced in March 2012 that Russia intended to create a "Cyber Security Command" (billed as a response to the creation of similar entities abroad, with particular reference to the US), references to tasks for the potential new command which tally with those foreign counterparts have to be sought elsewhere than in the published proto-doctrine. The defensive tone of the "Views" was belied by comment by Russian Chief of General Staff Nikolay Makarov (*et al.*, 2012) at a briefing which gave a very different picture of the new command's three main tasks:

- "Disrupting adversary information systems, including by introducing harmful software;
- Defending our own communications and command systems;
- Working on domestic and foreign public opinion using the media, Internet and more".

The reference to "introducing harmful software" appears to be the first official avowal of an offensive cyber role for a Russian government body, and is more in keeping with overseas concepts of the purpose of cyber commands. At the same time the third task, influencing public opinion, is a further reminder that as noted in the discussion of information weapons above, unlike some other nations with advanced cyber capabilities, Russia deals in cyber warfare only as an integral component of information warfare overall.

Russia's Information Security Doctrine

Both of the public documents discussed above build on principles established in the Information Security Doctrine of the Russian Federation, the fundamental document governing Russia's approach to information security, and as an integral subset of information security, cyber issues (Security Council of the Russian Federation, 2000).

Once again, when compared to foreign counterparts, this document appears at first sight to contain the same liberal provisions for free exchange of information as called for by William Hague and Hillary Clinton as cited above. It is intended, inter alia, to "ensure the constitutional rights and freedoms of man and citizen to freely seek, receive, transmit, produce and disseminate information by any lawful means" (Article I, Part 1). It is only on closer inspection that the divergences with Western concepts and practices become clear.

A prime example lies in treatment of the media, whether state-owned or independent. The Doctrine stipulates "development of methods for increasing the efficiency of state involvement in the formation of public information policy of broadcasting organizations, other public media" (Article I, Part 4). The underlying concept, reflected in other doctrinal statements, is that media are a tool of the state for shaping public opinion in a manner favourable to the authorities. As tellingly explained by one leading Russian security specialist in the Ministry of Defence's "Red Star" newspaper:

> "How can you successfully wage an information struggle if during [conflict in] Chechnya a significant part of the mass media is taking the side of the terrorists? We need a law on information security" (Miranovich, 1999).

The implicit assumption being that information security must necessarily involve ensuring that the views transmitted by media, independent or not, are favourable to the government.

The Doctrine deals with issues such as these by stating that "the main activities in the field of information security of the Russian Federation in the sphere of domestic policy are … intensification of counter-propaganda activities aimed at preventing the negative effects of the spread of misinformation about the internal politics of Russia" (Article II, Part 6) as well as "development of specific legal and institutional mechanisms to prevent illegal information-psychological influences on the mass consciousness of society" (Article II Part 7).

This doctrinal concern over the circulation of information gives rise to doubt over the precise boundaries of freedom of expression in cyberspace. A highly topical issue at the time of writing which illustrates precisely this point is the passing in the Russian State Duma of a so-called "internet blacklist" bill. This widely misrepresented law is portrayed by opponents as a tool for censorship of public opinion in Russia, and in particular of dissent, whereas in fact the bill was substantially modified to address precisely these concerns (Giles, 2012). At the same time, state media reporting continues to betray unease over the uncontrolled use of social media in particular, and statements by officials convey mixed views over the basic issue of whether the internet should be viewed by Russia as an opportunity or a threat (Russia Today, 2011; 2012; Panarin, 2011).

Conclusion

Russia will continue to push for international agreements regulating cyberspace, along the lines of the consensus already achieved with like-minded states in the CSTO and SCO. Until now, the basic premises of these agreements have been largely rejected, or indeed ignored, by the Euro-Atlantic community (Conflict Studies Research Centre, 2012). But as Russia continues to gain support for its view of the internet among those states that discern similar threats to their security emanating from more advanced cyber powers, this competing consensus will become ever harder to disregard.

The challenge for any Western interlocutor seeking to engage with Russia on these issues is to understand that in cyber, as in so much else, the fundamental assumptions governing the Russian approach are very different from our own – and in many cases, once again as in other areas of relations with Russia, similar language with divergent meaning employed by the two sides serves only to mask these differences. Further efforts to achieve mutual understanding are essential

if meaningful confidence and security building measures are to be realized in accordance with the newly-emerging Euro-Atlantic ambition (Blitz, 2012).

These mixed views are reflected in the manner in which the Russian authorities already possess extremely strong legislative tools for controlling content, and have at their disposal all the necessary methods for a clampdown on freedom of expression should they choose to use them, but contrary to reputation, ordinarily apply these with a very light touch. The protests over election results in Russia at the end of 2011, in large part organized using social media, provoked an example of this apparent mixed response from the authorities (Deutsche Welle, 2011; FIIA, 2012). Pressure on websites, including allegedly government-sponsored online attacks, was occasional and unsustained (Krebs, 2011) and in at least one case, subject to successful legal challenge: the Russian Facebook equivalent VKontakte (now renamed VK) refused to supply subscriber information to the Federal Security Service on the grounds that the request was illegal (Forbes Russia, 2011). Meanwhile sections of the Russian authorities defaulted to more old-fashioned, offline methods of smearing and discrediting opposition leaders (Kramer, 2012; Zeenews, 2011; Faulconbridge, 2011). This provides an indication that far from being rigid, the overall Russian attitude to online dissent is still to crystallize – a factor as applicable to domestic politics as to international initiatives. As put by Prime Minister Dmitriy Medvedev, the internet "should be regulated by a set of rules, which mankind has yet to work out. It's a very difficult process."

References

Anatomiya Protesta (2012) [Film] s.l.: NTV.

Anon. (2011a). *Challenges in Cybersecurity - Risks, Strategies, and Confidence-Building*. Berlin: s.n.

Anon. (2011b). *International Code of Conduct for Information Security*. s.l.:Annex to the letter dated September 12, 2011, from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359).

Argumenty i Fakty (2011). *Nikolay Patrushev: SShA prikryvayutsya skazkami o pravakh cheloveka*. [Online].

Blitz, J. (2012). "UK Seeks Deal to Counter Cyber Attacks". *Financial Times*, 2 October.

Borisov, T. (2010). "Virtual'nyy mir zakryt". *Rossiyskaya Gazeta*, 12 November.

CCDCOE (2012). *Call for Papers Announced for CyCon 2013.* [Online] Available at http://ccdcoe.org/cycon/400.html [Accessed 1 October 2012].

Clinton, H. (2011). *Remarks by Hillary Rodham Clinton at Conference on Internet Freedom.* The Hague, Netherlands. [Online] Available at http://www.state.gov/secretary/rm/2011/12/178511.htm.

Collective Security Treaty Organisation (2012). *CSTO Website.* [Online] Available at http://www.odkb.gov.ru/start/index_aengl.htm.

Conflict Studies Research Centre (2012). *Russia's "Draft Convention on International Information Security" – A Commentary.* Oxford: Conflict Studies Research Centre.

Council of Europe (2001). *Convention on Cybercrime.* [Online] Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Deutsche Welle (2011). *Russia Holding Back Online Shutdowns for Now, Expert Says.* [Online] Available at http://www.dw.de/dw/article/0,15599135,00.html.

EastWest Institute (2011a). *EWI's Eighth Annual Worldwide Security Conference.* [Online] Available at http://www.ewi.info/wsc8 [Accessed 1 October 2012].

EastWest Institute (2011b). *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations.* New York: EastWest Institute.

Falaleyev, M. (2011). *Politseyskoye upravleniye "K" predlozhilo zapretit anonimnyye vystupleniya v Internete.* [Online] Available at http://www.rg.ru/2011/12/08/moshkov.html.

Faulconbridge, G. (2011). *Phone Hacking Russian Style: Opposition Under Fire.* [Online] Available at http://in.reuters.com/article/2011/12/20/russia-phone-hacking-idINDEE7BJ0AE20111220

Fedorov, A. V. and Tsigichko, V. N. eds. (2001). *Information Challenges to National and International Security.* Moscow: PIR Center.

FIIA-Finnish Institute of International Affairs (2012). *Russian Society Through the Prism of Current Political Protests.* Seminar, Helsinki: s.n.

Forbes Russia (2011). *Durov: FSB prosit "VKontakte" blokirovat oppozitsionnye gruppy*. [Online] Available at http://www.forbes.ru/news/77291-durov-fsb-prosit-vkontakte-blokirovat-oppozitsionnye-gruppy.

Gazeta.ru (2011). *Ne pokazyvat i ne upominat (Don't Show and Don't Refer)*. [Online] Available at http://www.gazeta.ru/politics/elections2011/2012/01/30_a_3979953.shtml.

Giles, K. (2012). "Still writing the online rulebook". *The World Today*, October-November, p. 21.

Giles, K. (2011a). "Information Troops: A Russian Cyber Command?", in *Third International Conference on Cyber Conflict*. s.l.:CCDCOE.

Giles, K. (2011b). *The State of the NATO-Russia Reset.* Oxford: Conflict Studies Research Centre.

Gjelten, T. (2010). *Seeing The Internet As An "Information Weapon"*. [Online] Available at http://www.npr.org/templates/story/story.php?storyId=130052701

Gorman, S. (2010). "U.S. Backs Talks on Cyber Warfare". *Wall Street Journal*, 4 June.

Hagestad, W. (2012). *Information Security in the People's Republic of China,* s.l.: Forthcoming publication.

Hague, W. (2011). *Chair's Statement.* [Online] Available at http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282.

Interfax (2011). *Shchegolev: tsenzury Interneta v Rossii ne dopustyat.* [Online] Available at http://www.interfax.ru/print.asp?sec=1448&id=226823.

Interfax (2000). October12.

ITAR-TASS (2009). 29 January.

Joint Chiefs of Staff (2006). *Joint Publication 3-13: Information Operations.* [Online] Available at http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [Accessed 2012].

Kramer, A. (2012). *Smear in Russia Backfires, and Online Tributes Roll In*. [Online] Available at http://www.nytimes.com/2012/01/09/world/europe/smear-attempt-against-protest-leader-backfires-in-russia.html?_r=1.

Krebs, B. (2011). *Twitter Bots Drown Out Anti-Kremlin Tweets*. [Online] Available at http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/.

Lipien, T. (2012). *VOA harms Putin opposition in Russia*. [Online] Available at http://www.washingtontimes.com/news/2012/feb/8/voa-harms-putin-opposition-in-russia/.

Lisovoy, V. M. (1993). "O zakonakh razvitiya vooruzhennoy bor'by i nekotorykh tendentsiyakh v oblasti oborony". *Voyennaya Mysl',* Issue 5.

Makarov, N. (2010). "Kharakter vooruzhennoy borby budushchego" (The Character of Future Armed Conflict). *Vestnik Akademii Voyennykh Nauk (Bulletin of the Academy of Military Science).*

Makarov, N., Ostapenko, O., Rogozin, D. and Falichev, O. (2012). "We Await Help from Military Science and Defence Industrialists; Without This, Creation of Modern Armed Forces Will Not Be Successful". *Voyenno-promyshlennyy kuryer*, 8 February, Issue 5 (422).

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations.* [Online] Available at http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

Medvedev, D. (2011). *Dmitriy Medvedev provel vo Vladikavkaze zasedaniye Natsional-nogo antiterroristicheskogo komiteta.* [Online] Available at http://www.kremlin.ru/transcripts/10408.

Michael, A. (2010). *Cyber Probing: the Politicisation of Virtual Attack.* Shrivenham: Defence Academy of the United Kingdom.

Miles, D. (2011a). *Doctrine to Establish Rules of Engagement Against Cyber Attacks.* [Online] Available at http://www.defense.gov/news/newsarticle.aspx?id=65739.

Miles, T. (2011b). *Army Activates First-of-Its-Kind Cyber Brigade.* [Online] Available at http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/.

Miranovich, G. (1999). "Voyennaya reforma: problemy i suzhdeniya" (Military Reform: Issues and Judgements). *Krasnaya Zvezda*, 31 July.

Modestov, S. (2003). "Prostranstvo budushchey voyny" (The Space of Future War). *Vestnik Akademii Voyennykh Nauk* (Bulletin of the Academy of Military Science) n.º 2.

Monaghan, A. (2012). *Flattering to deceive? Change (and continuity) in post election Russia.* [Online] Available at http://www.ndc.nato.int/research/series.php?icode=3.

Monaghan, A. (2011). *NATO and Russia: Resuscitating the Partnership.* [Online] Available at http://www.nato.int/docu/review/2011/NATO_Russia/EN/index.htm.

Monaghan, A. (2010). *The Moscow Metro Bombings and Terrorism in Russia*. [Online] Available at http://www.ndc.nato.int/research/series.php?icode=1.

NDC (2010) *The Indivisibility of Security: Russia and Euro-Atlantic Security.* Rome: NATO Defense College.

Novostey, G. (2012). *I don't get upset with you when you pour diarrhoea on me: Putin chats with media leaders.* [Online] Available at http://www.city-n.ru/view/296196.html.

OECD (2011). *OECD Council Recommendation on Principles for Internet Policy Making*. [Online] Available at http://www.oecd.org/dataoecd/11/58/49258588.pdf

Panarin, I. (2011). *December 2011: Information War Against Russia*. [Online] Available at http://rt.com/politics/information-war-russia-panarin-009/.

Panarin, I. (2009). *Russian pundit interviewed on US information operations conference*. [Interview] 27 April 2009.

Panarin, I. (2004). *Informatsionnaya voyna i diplomatiya (*Information Warfare and Diplomacy*)*. Moscow: Gorodets.

Russia Today (2012). *Social networks – a threat for Russia?*. [Online] Available at http://rt.com/news/social-networks-bullying-russia-695/.

Russia Today (2011). *Stallman: Facebook Is Mass Surveillance*. [Online] Available at http://rt.com/news/richard-stallman-free-software-875/.

Russian Ministry of Defence (2011). [Online] Available at http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

Security Council of the Russian Federation (2000). *Information Security Doctrine of the Russian Federation (2000).* [Online] Available at http://www.scrf.gov.ru/documents/6/5.html.

Shanghai Cooperation Organisation (2009). [Online] Available at http://www.sectsco.org/EN/show.asp?id=182.

Sharikov, P. A. (2009). "Evolyutsiya gosudarstvennoy strategii v sfere informatsionnoy bezopasnosti" (Evolution of state strategy in the sphere of information security). *SShA – Kanada. Ekonomika, politika, kul'tura*, December, pp. 95-108.

Shavayev, A. G. and Lekarev, S. V. (2003). "Spetssluzhby i informatsionnoye prostranstvo" (The Special Services and the Information Space). *Razvedka i kontrrazvedka*, pp. 350-354.

Shchegolev, I. (2011). s.l., s.n.

Shcherbakov, V. (2010). "Prostranstvo virtual'noye, bor'ba real'naya" (Virtual Space, Real Combat). *Voyenno-promyshlennyy kur'yer*, 13 October.

Sherstyuk, V. P. (2011). *Presentation.* Brussels: s.n.

Sheynis, V. L. (2010). "Natsional'naya bezopasnost' Rossii. Ispytaniye na prochnost'" (National Security of Russia. Testing for Strength). *POLIS. Politicheskiye issledovaniya*, Issue 1.

Sidorov, V. (2008). "Kibervoyny: ot dozhdya k uraganu" (Cyber War: From Rain to Hurricane). *Krasnaya zvezda*, 26 March.

Soloveitchik, R. (2011). *Twitter Becomes Key for Moscow Protests*. [Online] Available at http://www.themoscowtimes.com/arts_n_ideas/article/twitter-becomes-key-for-moscow-protest s/450350.html.

State Duma (1996). *Proceedings.* s.l.:s.n.

Talihärm, A. M. (2010). "Cyberterrorism: in Theory or in Practice?". *Defence Against Terrorism Review,* Vol. 3, No. 2, pp. 59-74.

Thomas, T. (2011). *Recasting the Red Star.* Fort Leavenworth: Foreign Military Studies Office.

Thomas, T. (2010). "Russian Information Warfare Theory: The Consequences of August 2008". In S. Blank and R. Weitz eds., *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald.* Carlisle, PA: US Army War College Strategic Studies Institute.

Thomas, T. (2002). *Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?.* Fort Leavenworth, KA: Foreign Military Studies Office (FMSO).

Thomas, T. (2000). *The Russian View Of Information War.* Fort Leavenworth, KA: Foreign Military Studies Office (FMSO).

Tsymbal, V. (1995). *Concept of Information Warfare.* Moscow: s.n.

UNIDIR (2008). [Online] Available at http://www.unidir.org/audio/2008/Information_Security/en.htm.

US Department of Defense (2011). *Strategy for Operating in Cyberspace.* [Online] Available at http://www.defense.gov/news/d20110714cyber.pdf.

Zeenews (2011). *Russian website publishes vote monitor's e-mails*. [Online] Available at http://zeenews.india.com/news/world/russian-website-publishes-vote-monitor-s-e-mails_746183.html.

Media e (Ciber)Terrorismo

Rui Alexandre Novais

Doutor em Communication and Image Studies pela Universidade de Kent/Canterbury. É investigador, docente e conferencista na Universidade do Porto, na Universidade do Minho e na Universidade de Liverpool.

Resumo

Este artigo versa sobre o relacionamento simbiótico entre o (ciber)terrorismo e os media. Assumindo que a comunicação assume um papel central na publicitação dos atos terroristas, problematiza se os *media* continuam a constituir os melhores amigos dos terroristas ou apenas aliados desintencionais. Conclui que o sucesso dos atentados terroristas ainda está dependente da publicidade oferecida pelos *media* apesar de uma progressiva desterritorialização da utilização por parte dos grupos terroristas para as plataformas digitais, reapossando-se das funções habituais dos *media* convencionais e complementadas com novas competências. Na verdade, ao invés de uma temível arma de atentados ciberterroristas, a internet constitui-se como um poderoso recurso utilizado com perícia com finalidades mundanas, designadamente as de coordenação e planeamento das atividades que se assumem como a principal potencialidade *online* atual.

Abstract
(Cyber) Terrorism and Media

This paper dwells on the symbiotic relationship between the media and (cyber) terrorism. Assuming that communication is a key feature in terms of the publicizing and fuelling of terrorism, it discusses whether the media are still the terrorists' best friends or mere unintentional allies. The work concludes that the success of the terrorist attempts is still dependent upon the publicity offered by the media, although there are signs of a progressive de-territorialisation of the terrorism to the digital platforms, repossessing the conventional functions of traditional media and complemented with new competencies. Indeed, au lieu of a terrific cyber-terrorist weapon, the internet assumes itself as a powerful tool skillfully employed by terrorists to coordinate and cyber-planning, which is becoming its current pivotal online potential.

Apesar da sua importância nas questões políticas contemporâneas, uma definição consensual de terrorismo, e por arrastamento de ciberterrorismo, assume contornos de uma tarefa hercúlea quase impossível de atingir. Em parte, tal pode ser o resultado da diversidade e multiplicidade das formas, tipos e manifestações do terrorismo (Stepanova, 2008), dado que tal como Yasser Arafat reconhecia em 1974, o terrorista pode também ser denominado de lutador da liberdade, dependendo da perspetiva e da codificação da mensagem por parte do emissor.

Em face da ausência de uma definição consensual existem, em alternativa, interpretações socialmente construídas no sentido de veicular perspetivas específicas. Schmid e Jongman (2005) contabilizaram mais de 100 definições distintas, tendo como elementos comuns o facto de serem pautadas por alusões ao recurso à violência, eivadas de motivações do foro político, bem como, contendo elementos de ameaça geradores de medo.

A título de exemplo, a definição concreta avançada por Hoffman (2006: 40) que congrega esses denominadores comuns, concebe o terrorismo enquanto "a criação e exploração deliberada do receio através da violência ou a ameaça de violência com fins de mudança política". Apesar de paradigmática, tal proposta conceptual não inclui o objeto nem os sujeitos do terrorismo. Para preencher tal vazio teremos de recorrer a outras definições alternativas e complementares que apontam para os não-combatentes ou civis como os alvos dos atentados terroristas, ainda que os detentores de poder também possam ser objeto desse tipo de ataques. Similarmente, no que concerne aos sujeitos dos atos terroristas, estes incluem por norma tanto os atores estatais como os não estatais, apesar da ênfase atual ser na maior parte dos casos nos últimos. De uma forma salomónica, Freedman e Thussu (2012) apelam para uma definição mais inclusiva sem discriminações envolvendo a possibilidade de atores estatais e não estatais, originários de regimes democráticos ou não, independentemente do tamanho e da causa que representam.

Por fim, a conceptualização de terrorismo depende igualmente da época histórica. Walter Laqueur (1999) sugere a este propósito que houve uma transformação radical no terrorismo 'antigo' caracterizado por alvos claramente definidos para outros indiscriminados que visam causar o maior número de vítimas com o intuito não só de satisfazer as solicitações políticas mas também almejando a destruição da sociedade. Tal mudança ficou patente com a ocorrência dos atentados no World Trade Center em Nova Iorque, em 1993, e o ataque com gás sarin no metro de Tóquio, dois anos depois. O 'novo' terrorismo também surge muito mais associado

a questões de índole religiosa, em particular ao radicalismo islâmico, próximo da noção de choque de civilizações.

Em alternativa à classificação anterior, Ganor (2002) propõe a distinção entre os períodos 'clássico', 'moderno' e 'pós-moderno'. No caso do primeiro, o terrorismo era dirigido a alvos específicos, com poucos danos e visando objetivos políticos concretos. No que concerne o terrorismo moderno, os ataques passam a ser indiscriminados e o nível de destruição muito mais considerável. E por último, no que ao pós-moderno diz respeito, visa alterar a realidade do conflito – por norma assimétrico – através do próprio ato terrorista com recurso a armas químicas, biológicas ou nucleares contra símbolos do inimigo e com o objetivo de eliminar a causa do conflito infligindo o maior dano possível.

Em face do exposto, a definição adotada neste artigo prende-se com o uso da violência não convencional e inesperada em atos criminosos (*mala prohibita*) e imorais (*mala in se*) com intuitos de natureza política, religiosa ou ideológica visando intencionalmente alvos não combatentes (civis ou icónicos) para criar receio (terror ou medo psíquico). E no sentido de evitar igual discussão em torno do conceito correlacionado de ciberterrorismo, a noção prevalecente neste texto refere-se à definição de terrorismo agora propostas com recurso a meios digitais, ou uma nova forma de conseguir os mesmos intentos do terrorismo convencional.[1] Dito de outra forma, o ciberterrorismo resulta em termos simples da convergência do terrorismo e do ciberespaço e refere-se àquilo que se designa igualmente por 'terrorismo eletrónico'. Convirá nesta altura distinguir tal conceção de ciberterrorismo das de cibercriminalidade e de ciberativismo. Apesar do seu uso indiferenciado e desplicente em muitos quadrantes – com reflexos na própria cobertura mediática, em resultado da prática jornalística de objetividade e dependência das fontes de informação (Cavelty, 2007) – todas recorrem ao uso das tecnologias de informação digitais, diferindo nos motivos e nos objetivos a que se propõem.[2]

Esclarecida a questão conceptual, importa sobretudo centrar o foco analítico deste artigo em torno da questão do terrorismo (e ciberterrorismo) do ponto de vista dos *media*, ou mais concretamente na relação simbiótica entre ambos.

1 O Gabinete Federal de Investigação norte-americano define enquanto ataque premeditado e politicamente motivado contra informação, sistemas de computadores, programas e dados que resultem em violência contra não combatentes por grupos subnacionais ou agentes clandestinos (disponível em http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/). Para definições alternativas ver Conway (2007) e Denning (2000).

2 Maura Conway (2007) define e distingue os conceitos tendo como critério diferenciador o grau crescente e progressivo de distúrbio e de destruição que provocam, sendo que o ativismo prende-se com a utilização normal (não-disruptiva) da internet em prol de uma causa, enquanto o "*hacktivismo*" refere-se ao recurso a *hackers* com propósitos ativistas sem o intuito de provocar danos consideráveis.

Relação Simbiótica de Conveniência e Exploração Mútua

De acordo com Wieviorka (2004), o relacionamento entre os *media* e o terrorismo pode assumir diversas facetas, começando pela completa indiferença, na medida em que os terroristas pretendem apenas amedrontar as vítimas desconsiderando qualquer envolvimento mediático. De forma semelhante, no cenário da relativa indiferença as ações terroristas são executadas com a firme consciência da existência e possível ajuda dos *media*, mas ainda assim indiferentes relativamente a estes últimos. Num sentido diametralmente oposto, os *media* podem ser considerados inimigos passando a constituir um alvo enquanto parte integrante do sistema que se pretende atingir. Finalmente, surge a estratégia orientada para os *media* ou integrando os mesmos, na qual os terroristas pretendem explorar ou manipular estrategicamente os *media* na transmissão da sua mensagem.

Como facilmente se depreende é no âmbito deste último domínio (exploração dos *media*) que se verifica a interação efetiva entre o terrorismo e os *media* deste artigo. Por conseguinte, isto importa ser destacado uma vez que um dos principais objetivos deste artigo prende-se com a intenção de contribuir para a compreensão da relação simbiótica entre os *media* e o terrorismo.

Uma breve panorâmica relativa aos estudos existentes no âmbito do processo negocial entre os *media* e o terrorismo revela que para além daqueles que tendem a centrar-se nas construções discursivas presentes na promoção de mensagens dramáticas ou nos enquadramentos utilizados na construção da realidade social (Freedman e Thussu, 2012; Bowen, 2008), existe uma quantidade considerável de obras dedicadas à relação simbiótica entre os *media* e o terrorismo (Hoffman, 2006; McNair, 1999; Wardlaw, 1989; Wilkinson, 1997). Esta relação resulta da mútua conveniência dos terroristas (que procuram a atenção das audiências) e dos *media* (que buscam factos noticiosos dramáticos que aumentem o público e a popularidade). De acordo com Miller (1982: 1) trata-se mesmo de uma relação inexorável na medida em que "*terrorism is capable of writing any drama – no matter how horrible – to compel the media's attention (…). Terrorism, like an ill-mannered enfant terrible, is the media's stepchild, a stepchild which the media, unfortunately, can neither completely ignore nor deny*".

Nesse sentido, os *media* constituem na atualidade tanto um alvo como um recurso por parte dos grupos terroristas. Na verdade, coexistem duas possibilidades na literatura relativamente ao desempenho dos *media* nesse contexto específico. Por um lado, preconiza-se que ao oferecerem o necessário oxigénio que mantém acesa a causa do terrorismo, estes se assumem como os melhores amigos dos terroristas (Laqueur, 1976). Tal sucede em virtude do *rationale* básico do terrorismo consistir em enviar uma mensagem com o intuito de persuadir, e que esta mensagem só atinge audiências globais, de forma intencional ou não, através dos *media*. Esta

conceção da culpabilidade dos *media* encerra em si mesma, para além da relação de causalidade com o terrorismo, uma outra de proporcionalidade direta. Isto é, ao noticiarem o terrorismo, os *media* incitam à ocorrência de mais atentados que, por sua vez, asseguram mais cobertura mediática (Barnhurst, 1991: 125)[3]. Por outro lado, no extremo oposto, surge a versão alternativa da vulnerabilidade dos *media* enquanto meras vítimas do fenómeno do terrorismo.

De facto, da parte dos *media*, o objetivo existencial consiste em obter e divulgar informação relevante junto da opinião pública. No desempenho das suas funções primordiais – informativa e social – os *media* empenham-se na prossecução do direito das pessoas a serem informadas acerca dos acontecimentos, de preferência em primeira mão, num contexto crescente de pressão de proporcionar notícias em cima do acontecimento ou em tempo real (com implicações em termos da edição e avaliação dos eventos noticiados).

Concomitantemente, em resultado da aplicação dos valores-notícia (ou critérios noticiosos que determinam os eventos que merecem atenção noticiosa bem como a orientação do conteúdo informativo) os *media* tendem a veicular acontecimentos de natureza dramática, algo que potencia que os atos terroristas mereçam atenção constante e recorrente. Ao integrar os ingredientes preferenciais das notícias – drama, violência, medo, conflito e ameaça para o público – o terrorismo constitui por norma uma história potente para os *media*. A noticiabilidade jornalística dos atentados terroristas é reforçada pela contingência de coincidir com as pressões económicas e políticas que fixam o terror como narrativa decisiva nos *media* contemporâneos (Lewis, 2012: 260). Neste caso, e de forma algo irónica, o terrorismo pode ser considerado um produto da liberdade dos *media* (Jenkins, 1983: 160).

A literatura deste domínio científico descreve igualmente, de uma forma geral, um conjunto de objetivos associado aos *media* do ponto de vista dos terroristas, começando pelo objetivo primordial da publicidade que aparece de forma omnipresente na predisposição de obter visibilidade gratuita através dos *media* relativamente à causa subjacente a um determinado grupo terrorista. Na realidade, o terrorismo depende do oxigénio da publicidade (McNair, 1999; Wilkinson, 1997), sem o qual seria impotente (Chalfont, 1980). Concordemente, os grupos terroristas pretendem obter através dos *media* um entendimento favorável relativamente à sua *cause célèbre*. Sobretudo em vista do seu padrão de atuação que habitualmente envolve a violação das leis e dos padrões convencionais das normas de conduta, torna-se fundamental para os grupos terroristas que as audiências percebam, de algum modo, o motivo pelo qual enveredam por essa forma de ação, e a justificação para tal.

3 Outra possibilidade correlacionada prende-se com a ideia de alguém ser vítima do terrorismo através dos *media*, também designado de terrorismo em segunda mão.

Tal publicidade pode proporcionar benefícios imediatos (táticos) e a longo prazo (estratégicos), tanto de um ato ou atentado, em particular, como da causa terrorista, em geral (Combs, 2011). Desde logo, a publicidade positiva por parte dos *media* possibilita a afirmação da identidade e legitimidade das causas terroristas que, por sua vez, garante não só a sobrevivência do grupo terrorista mas permite obter dividendos adicionais em termos do recrutamento de novos membros. A publicidade favorável poderá ser igualmente determinante no sentido da angariação de fundos por parte de quem partilhe os ideais ou a motivação do grupo terrorista.

Por conseguinte, Brigitte Nacos (2007) propõe o conceito de terrorismo mediado pelos meios de comunicação para descrever o papel central desempenhado pelos *media* nas estratégias terroristas. Através deles, os terroristas pretendem primordialmente desestabilizar o inimigo por gerar um sentimento de insegurança e de incapacidade das autoridades de protegerem e garantirem o bem-estar das populações. E, dessa forma, não só exporem as limitações e inadequações do sistema ou regime como deslegitimar a sua autoridade. Mas no cálculo por parte dos terroristas acerca das consequências dos seus atos, constam igualmente a necessidade de obterem destaque mediático e atingirem os demais atores da comunicação política (grupos de interesse, decisores governamentais e a opinião pública).

Em face dos motivos acima expostos, percebe-se a necessidade dos grupos terroristas construírem e manterem um bom relacionamento com os *media* e, de forma preferencial, que o façam ao longo do tempo. Tal relação de conveniência é ainda mais fundamental na medida em que os grupos terroristas estão conscientes e levam em consideração que, pelo menos nalguns casos, dependerá em última análise da parte dos atores mediáticos o enquadramento e a visibilidade atribuídas às questões terroristas (Calhaghan e Schnell, 2001). Adicionalmente, e de forma menos habitual, esse relacionamento de interdependência com os *media* pressupõe algum tipo de vantagens na obtenção de informação de interesse estratégico para os grupos terroristas (Yungher, 2008).

Da parte das autoridades governamentais há também um conjunto de expectativas relativamente ao papel dos *media* nas questões que dizem respeito ao terrorismo. Ainda que em grande medida semelhantes às dos grupos terroristas enunciados anteriormente, são no entanto por norma incompatíveis (Nacos, 2007), desde logo na questão do objetivo a atingir relativamente à publicitação dos atentados terroristas. Ao contrário dos terroristas cuja ênfase reside no medo e no pânico, a ênfase na mensagem das autoridades, por seu turno, reside sobretudo em reassegurar o controlo da situação. Interessa neste caso que os *media* divulguem a forma de pôr cobro à situação criada pelo atentado terrorista e promovam as ações implementadas pelas autoridades.

Por outro lado, o interesse das autoridades consiste em recusar ou negar o acesso e utilização por parte dos grupos terroristas dos *media* enquanto plataforma de

divulgação da sua propaganda que possa redundar na compreensão, simpatia ou apoio tangível do terrorismo (Combs, 2011). Os governos esperam que os *media* enfatizem a criminalidade e a natureza ilegal dos eventos, algo que terá implicações na forma como os grupos terroristas são percecionados junto da opinião pública. E como por norma os atentados infligem danos em vítimas inocentes, tal facto é explorado pelas autoridades que procuram obter a cooperação dos *media* no sentido de veicularem essa versão específica dos acontecimentos.

Assim sendo, nas intenções dos decisores governamentais a solução ideal consistiria na exclusão total do tratamento noticioso dos *media* deste tipo de cenários. Na maior parte dos países ocidentais, contudo, tal prospeto afigura-se impraticável. Dado que a censura não só não é aceitável como de difícil implementação em vista da liberdade de informação, na prática o que prevalece é não só a presença usual dos *media* mas também o *modus operandi* da cooperação e da partilha de informação com as autoridades.

Por conseguinte, não raro as autoridades solicitam discrição e bom critério aos *media* aquando da divulgação da informação nestes casos, no sentido de não prejudicar as operações em curso ou então evitar o fenómenos de imitação ou contágio dos atos terroristas por colocar a tónica nos detalhes de um atentado bem-sucedido. No extremo, em circunstâncias excecionais, poderá ser instada a cooperação dos *media* no sentido da desinformação, isto é, na divulgação propositada de informação inexata. Apesar da censura ser inaceitável, a autorrestrição e comedimento por parte dos *media* neste tipo de situações costuma ser uma prática aconselhável e recorrente. Dito de outra forma, não sendo linear e absoluto, os *media* tendem a assumir uma atitude cooperante com as autoridades neste tipo de contextos em virtude de estar envolvida a proteção da segurança nacional.

As Potencialidades dos *Media*: Comunicação, Amplificação e Espectacularização

O terrorismo é essencialmente um processo comunicativo dado que, tal como reconhecem Schmid e de Graaf (1982: 9), sem comunicação não há terrorismo. Trata-se, isso sim, de um veículo violento de comunicação, uma vez que as imagens e temas associados ao terror ativam uma das emoções mais profundas no cérebro humano: o medo da morte (Castells 2009: 169). Os atentados terroristas, enquanto manifestações extremas de violência política visam, através das vítimas e destruição causadas, veicular mensagens e criar imagens mentais associadas ao medo. Ou seja, os terroristas são emissores de uma mensagem coletiva (atentado), para recetores coletivos, com recurso a ações controversas ou ruidosas que simultaneamente fascinam e amedrontam o público (Simonson, 2001).

Mais recentemente, o terrorismo assumiu os contornos de espetáculo para as audiências, convertendo-se numa espécie de género dramático ou teatral (De Bord, 1995). Parece também consensual entre os académicos, a crescente sofisticação de alguns grupos terroristas em visarem em simultâneo audiências gerais do mundo do espetáculo global (Kellner, 2002) e outras mais específicas (Low, 2003). Socorrendo-se do poder excecional do impacto visual e da imagem, o terrorismo contemporâneo logra comunicar o indescritível e o inconcebível – a cultura do terror – sob a forma do espetáculo, através do choque e do espanto. Isto é algo que contribui para a intensificação do medo (Bowen, 2008), bem como para o infoentretenimento (Thussu, 2008) e a espectacularização da cobertura mediática (Bruck, 1992).

Na verdade, é sobretudo a espetacularidade dos atos que suscita a atenção mediática, dado que em termos de mortalidade (excetuando o caso dos atentados de 11 de setembro de 2001) é relativamente insignificante quando comparado com desastres naturais, conflitos, guerras ou acidentes de viação. Nesse sentido, os *media* funcionam como amplificadores do impacto do terrorismo, algo que se aplica com igual propriedade ao foco repetido de imagens violentas enquanto entretenimento popular. Aliás, um dos objetivos do terrorismo mediado consiste em inflacionar a ameaça terrorista, bem como apoiar ou autenticar a descrição social do terrorismo como sendo maior, mais mortífero e mais ameaçador.

Convirá ressalvar nesta altura que esta tendência exageradora do pânico social, não é da exclusiva responsabilidade dos grupos terroristas, nem tampouco das contingências relativas às práticas e rotinas de funcionamento dos *media*. Na verdade, pode ser gerada intencionalmente por outros agentes interessados na amplificação da ameaça terrorista (governos, indústrias do armamento) e ligação a uma narrativa mais generalizada do cenário geopolítico (Kitzinger, 2000) quer em contextos específicos almejando obter mais apoios financeiros e/ou políticos ou com vista à diminuição e restrição das liberdades civis (Boyns e Ballard, 2004).

O advento das tecnologias de informação e comunicação, e dos *media* digitais em particular, não só intensificaram a espetacularidade do terrorismo, assumindo-se crescentemente como um ato comunicacional (Schmid e Graaf, 1982; Hoskins e O'Loughlin, 2007), como também confirmaram o primado da mensagem sobre as vítimas dos atos. Conforme admite Der Derian (2005: 24) graças ao imediatismo da internet, televisão e o mecanismo de informação em rede, é possível aceder ao terrorismo em tempo real e em toda a parte tendo este assumido facetas icónicas e de impacto visual.

Implícito nesta última asserção surge um outro aspeto digno de destaque, a saber: o facto dos adventos tecnológicos no campo da informação e comunicação terem sido favoráveis ao terrorismo, permitindo-lhe a propagação dos seus atos e atentados a audiências globais. Na verdade, os *media* promoveram a erosão da distinção entre terrorismo nacional e internacional, e adotaram uma agenda global

em que os fenómenos dessa natureza merecem cobertura independentemente do local geográfico onde ocorram e atingindo audiências maiores do que as que afetam diretamente os atentados terroristas (Combs, 2011).

Em suma, o terrorismo moderno assume-se em definitivo como um espetáculo mediático e corrobora a natureza simbiótica do relacionamento com os *media* (White, 2011). O aumento da cobertura mediática não raro resulta na intensificação de atentados terroristas e na sensacionalização das imagens de terror com vista a influenciar as audiências. A sua vulgarização, contudo, pode redundar em fenómenos de fadiga das audiências e de crescente insensibilidade relativamente a eventos terroristas. Esse eventual cenário de saturação mediática relativamente à violência, drama e tragédia, pode ser catalisador de uma realidade ainda mais paradoxal: para assegurar a noticiabilidade os atentados terroristas socorrem-se de ações ainda mais espetaculares e imagens visualmente cativantes e, se necessário, resultando numa escala de destruição cada vez maior (Tuman, 2003).

Internet: Arma Ciberterrorista ou Complemento e Alternativa aos *Media* no Terrorismo?

O terrorismo atual é caracterizado pelo seu caráter global, pelas táticas sofisticadas que emprega e pela dependência das modernas tecnologias, transformando-se num conflito de todos contra todos – numa espécie de terrorismo apocalíptico (Crelinsten, 1988; Macmillan, 2000; Weigert, 2003). De alguma forma o campo de batalha do terrorismo atual expandiu-se para o ciberespaço e para a internet, em particular, mesmo que seja utilizada como instrumento para atingir objetivos e alvos tradicionais (Cronin, 2006).

Apesar do potencial que encerra para eventuais utilizações em atentados terroristas, essa capacidade ainda não se manifestou (Conway, 2011).[4] Aliás, ainda que não totalmente impossível e apesar de surgir ocasionalmente nos media como estando iminente, a possibilidade da ocorrência de um atentado ciberterrorista é tida como sendo pouco provável que ocorra (Conway, 2011; Denning, 2000). A improbabilidade é sustentada, entre outros fatores, no desfasamento entre custos e risco envolvidos *versus* o objetivo atingido e o impacto mediático possível de obter,

4 Será mais apropriado falar em ameaça infundada ou inflacionada em virtude da ausência de atentados ciberterroristas. Com a exceção dos acontecimentos ocorridos na Estónia em 2007 e com *Stuxnet* no Irão três anos depois, a maioria dos ciberataques ou não foram perpetrados por grupos terroristas ou não envolveram os danos que qualificaria como ciberterrorismo (Conway, 2011). Trata-se isso sim de uma onda de alarmismo pós 11/9 fomentada por vários quadrantes (Conway, 2011; Denning, 2000) e que encontraram eco na cobertura mediática.

dado tratarem-se de ações pouco apelativas para os *media* (Conway, 2011).Dado que em grande medida os sucessos e insucessos do terrorismo e ciberterrorismo ainda dependem da publicidade que obtém para os seus atos, os *media* continuam a desempenhar um papel fundamental na disseminação e amplificação da audiência dos atentados terroristas. O uso da internet veio reforçar a possibilidade da promoção da propaganda, e nalguns casos contrariar e circum-navegar os *media* convencionais.

À semelhança do que sucedia com o terrorismo, a principal função e medida de eficiência dos recursos digitais no ciberterrorismo continua a ser a da comunicação. Tratando-se de uma plataforma multimédia, a internet permite uma rápida divulgação de informação complexa a custos controlados, garantindo anonimato e proporcionando a possibilidade de interação. A internet acentuou igualmente a globalização das comunicações, algo que proporcionou a ubiquidade aos terroristas e um poderoso meio de recrutamento. Conforme reconhece Cronin (2006), "*it is enabling the recruiting, training, convincing, and motivating of individuals who are driven to engage not primarily in the high-tech cyber-attacks that many US policy makers are focused upon, but in old fashioned violence in the physical world*". Assim sendo, a internet assume-se como meio mais eficaz de persuasão, potenciando a captação de prospetivos membros.

Mas a internet serve para outras finalidades, desde a monitorização das atividades militares e obtenção de informações sobre alguns potenciais alvos, até à angariação de fundos quer pela via de donativos voluntários quer com recurso a expedientes criminosos como as fraudes de cartões de crédito e tráfico. Por fim, outra das possibilidades da internet prende-se com o planeamento e coordenação de operações e atentados, assumindo-se paulatinamente como um poderoso mecanismo de comando e controlo de células geograficamente dispersas, reduzindo custos de transmissão e operacionais. Não será de todo estranho que a internet venha a assumir-se a breve trecho como a principal potencialidade *online* (Thomas, 2003).

Portanto, se é incontestável que a internet oferece aos grupos terroristas um enorme potencial de obter visibilidade para a luta política através de uma nova plataforma, não é menos verdade que o novo cenário dos *media* digitais providencia igualmente o acesso instantâneo a mensagens e interpretações alternativas de contestação. Consequentemente, a mediação do terrorismo poderá ser multiperspetivada e mais complexa no futuro (Der Derian, 2009).

Conclusão

Cientes do poder dos *media* e da predisposição para atos dramáticos de relevância para as respetivas audiências, os terroristas procuram desde há algum tempo a esta parte manter-se sob o radar mediático. Os *media* converteram-se numa arma para os terroristas no sentido em que lhes permitiram beneficiar, entre outras vantagens, do efeito de amplificação do impacto dos atentados terroristas envolvendo atos simbólicos que possam condicionar ou alterar o comportamento político por meios extranormais. Beneficiando da credibilidade e do impacto nos consumidores de notícias dos *media*, os terroristas tentam manipulá-los no sentido de difundirem mensagens que lhes permitem alcançar audiências maiores do que aquelas afetadas pelo atentado terrorista, e obter publicidade gratuita para as suas causas (preferencialmente numa luz positiva) ao mesmo que tempo que logram aterrorizar as populações.

De facto, apesar de nem todas as formas de terrorismo serem veiculadas pelos *media*, os principais atos e atentados terroristas são altamente mediatizados. Muito mais do que atores externos ou canal privilegiado das ações terroristas que se limitam a noticiar tais incidentes para audiências globais, os *media* fazem parte integrante da própria definição de terrorismo. Tal realidade é verificável conforme se depreende das recentes referências a 'terrorismo mediatizado' (Cottle, 2006), 'orientado para os *media*' (Surette *et al.*, 2009) e 'dos *media* de massas' (Nacos, 2007).

Adicionalmente, a confluência de interesses entre os terroristas e os *media* resulta numa relação de reciprocidade e interdependência mútua. Isto é, os terroristas fornecem matéria-prima dramática e sensacionalista que satisfaz a procura e necessidade mediática. Aliás, mais do que isso, argumenta-se que a necessidade de satisfazer o apetite mediático, de alguma forma justifica o recrudescimento das atividades terroristas (Scott, 2001). Um outro efeito secundário daí resultante prende-se com a probabilidade do afã e saturação mediáticos contribuírem para a necessidade dos grupos terroristas protagonizarem ações crescentemente espetaculares. Isto é algo que, para além de reforçar o argumento em torno da possível cumplicidade entre os *media* e o terrorismo, suscita a questão da causalidade dos primeiros relativamente aos últimos.

Independentemente das nuances da relação simbiótica entre os *media* e o terrorismo, é inquestionável que a comunicação reveste um caráter fundamental no sentido de obter a atenção e assegurar a perpetuação dos grupos terroristas. Incontroversa é também a constatação de que as ações terroristas visam ainda atrair a atenção e obter publicidade de assuntos ausentes das agendas mediática, pública ou governamental. Mesmo após o advento da internet, a comunicação continua a ser o veículo condutor dos motivos terroristas.

Ao invés de uma temível arma empregue em atentados ciberterroristas, a internet serviu de facilitador e instrumento do terrorismo moderno no sentido de alcançar audiências globais com uma mensagem de medo e terror. Na verdade, a internet operou a desterritorialização das operações mundanas terroristas para o ambiente *online* constituindo-se como uma ferramenta privilegiada para a angariação de fundos e o recrutamento de novos membros. Acima de tudo, as potencialidades do ciberespaço possibilitaram que a internet se assumisse como uma poderosa arma do terrorismo moderno e do ciberterrorismo, na exata medida em que permite organizar ou coordenar as redes emergentes de seguidores, bem como, possibilita o ciber-planeamento e a execução de atentados.

Referências

Barnhurst, Kevin (1991). "The Literature of Terrorism: Implications for Visual Communications" in A. Odasuo Alali e Kevin K. Eke (Eds.), *Media Coverage of Terrorism*. Newbury Park: Sage, pp. 112-137.

Bowen, Shannon A. (2008). "Frames of Terrorism Provided by the News Media and Potential Communication Responses" in Dan O'Hair, Robert Heath, Kevin Ayotte e Gerald R. Ledlow (Eds.), *Terrorism: Communication and Rhetorical Perspectives*. Cresskill, NJ: Hampton Press, pp. 337-358.

Boyns, David e Ballard, James David (2004). "Developing a Sociological Theory for the Empirical Understanding of Terrorism". *The American Sociologist* nr. 2, pp. 5-25.

Bruck, P. A. (1992). "Crisis as Specular: Tabloid News and the Politics of Outrage" in Marc Raboy e Bernard Dagenais (Eds.), *Media, Crisis, and Democracy: Mass Communication and the Disruption of Social Order*. Newbury Park: Sage.

Callaghan, K. e Schnell, F. (2001). "Assessing the Democratic Debate: How the News Media Frame Elite Policy Discourse". *Political Communication* nr. 18, pp. 183–212.

Castels, M. (2009). *Communication Power*. Oxford: Oxford University Press.

Chalfont, Lord (1980). "Political Violence and the Role of the Media: Some Perspectives – The Climate of Opinion". *Political Communication and Persuasion: An International Journal* nr. 1, pp. 79-81.

Combs, C. (2011). *Terrorism in the Twenty-first Century*. London: Longman.

Cottle, S. (2006). *Mediated Conflict: Developments in Media and Conflict Studies*. Maidenhead: Open University Press.

Crelinsten, Ronald D. (1988). "Images of Terrorism in the Media: 1966-1985". *Terrorism* nr. 12, pp. 167-198.

Cronin, Audrey Kurth (2006). "Cyber-Mobilization: The New Levée en Masse". *Parameters* Vol. XXXVI, disponível em http://ccw.modhist.ox.ac.uk/publications/cronin_parameters.pdf, acedido em 17 agosto 2010, pp. 77-87.

DeBord, Guy (1995). *The Society of the Spectacle*. Cambridge: Zone Books.

Der Derian, J. (2009). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. New York: Routledge

Der Darian, J. (2005). "Imaging Terror: Logos, Pathos and Ethos". *Third World Quarterly* nr. 1, pp. 23-37.

Freedman, D. e Thussu, D. K. (2012). *Media and Terrorism: Global Perspectives*. London: Sage.

Ganor, Boaz (2002). "Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?". *Police Practice and Research* no. 4, pp. 287-304.

Hoffman, B. (2006). *Inside Terrorism*. New York: Columbia University Press.

Hoskins, A. e Loughlin, B. (2007). *Television and Terror: Conflicting Times and the Crisis of News Discourse*. Basingstoke: Palgrave Macmillan.

Jenkins, Brian (1983). "Research in Terrorism: Areas of Consensus, Areas of Ignorance" in Burr Eichelman, David A. Soskis e William H. Reid (Eds.), *Terrorism: Interdisciplinary Perspectives*. Washington, D.C.: American Psychiatric Association, pp. 153-177.

Jenkins, Brian M. (2000). "Terrorism" in Edgar F. Borgotta (Ed.), *Encyclopedia of Sociology*. New York: Macmillan, pp. 3137-3141.

Kellner, D. (2002). "September 11, Social Theory and Democratic Politics". *Theory, Culture and Society* no. 4, pp. 147-159.

Kitzinger, J. (2000). "Media Templates: Patterns of Association and the (re)Construction of Meaning over Time". *Media, Culture and Society* no. 1: pp. 61-84.

Laqueur, W. (1977). *Terrorism*. London: Weidenfeld & Nicolson.

Laqueur, W. (1999). *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. London: Oxford University Press.

Lewis, J. (2012). "Terrorism and News Narratives" in Freedman, D. e Thussu, D. K. (Eds.), *Media and Terrorism: Global Perspectives*. London: Sage, pp. 257-270.

Lifton, Robert J. (2000). *Destroying the World to Save It: Aum Shinrikyo, Apocalyptic Violence, and the New Global Terrorism*. New York: Picador.

Low, E. (2003). "The War against Terrorism: a Public Relations Challenge for the Pentagon". *Gazette,* no. 3, pp. 211-230.

McNair, Brian (1999). *An Introduction to Political Communication*. London: Routledge.

Miller, Abraham H. (1982). *Terrorism, the Media and the Law*. New York: Transnational Publishers.

Nacos, B. (2007). *Mass Mediated Terrorism: the Central Role of the Media in Terrorism and Counterterrorism*. Lanham: Rowman & Littlefield.

Schmid, A. e Jongman, A. (2005). *Political Terror: a New guide to Actors, Authors, Concepts, Databases, Theories and Literature*. Piscataway, NJ: Transaction.

Schmid, Alex P., e de Graaf, Janny (1982). *Violence as Communication: Insurgent Terrorism and the Western News Media*. Beverly Hills: Sage.

Scott, John L. (2001). "Media Congestion Limits Media Terrorism". *Defence and Peace Economics* no. 3, pp. 215-227.

Simonson, Peter (2001). "Social Noise and Segmented Rhythms: News, Entertainment, and Celebrity in the Crusade for Animal Rights". *The Communication Review* no. 3, pp. 399-420.

Stepanova, E. (2008). *Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects*. SIPRI research Report no. 23. Oxford: Oxford University Press.

Surette, R., Hansen, K., e Noble, G. (2009). "Measuring Media Oriented Terrorism". *Journal of Criminal Justice* no. 4, pp. 360-370.

Thomas, Timothy L. (2003). "Al Qaeda and the Internet: The Danger of "Cyberplanning" *Parameters* no. 1. Disponível em http://www.carlisle.army.mil/usawc/parameters/Articles /03spring/thomas.pdf, acedido em 4 de julho de 2011, pp. 112-123.

Thussu, Daya Kishan (2008). *News as Entertainment: The Rise of Global Infotainment*. Thousand Oaks: Sage.

Tuman, Joseph S. (2003). *Communicating Terror: The Rhetorical Dimensions of Terrorism*. Thousand Oaks, CA: Sage.

Wardlaw, Grant (1989). *Political Terrorism: Theory, Tactics and Counter-Measures*. Cambridge: Cambridge University Press.

Weigert, Andrew J. (2003). "Terrorism, Identity, and Public Order: A Perspective from Goffman". *Identity: An International Journal of Theory and Research* no. 2, pp. 93-113.

White, Jonathan R. (2011). *Terrorism & Homeland Security*. 7th Ed. Belmont, CA: Wadsworth.

Wieviorka, Michel (2004). *The Making of Terrorism*. Chicago: The University of Chicago Press.

Wilkinson, Paul (1997). "The Media and Terrorism: A Re-Assessment". *Terrorism and Political Violence* no. 2, pp. 51-64.

Yungher, Nathan I. (2008). *Terrorism: The Bottom Line*. Upper Saddle River, NJ: Pearson Education.

A Chave da Inteligência Competitiva

Francisco Jaime Quesado

Economista e MBA pela Universidade do Porto, tem exercido funções de sestão na área pública (gestor do POSC – Programa Operacional Sociedade do Conhecimento, administrador da AdI – Agência de Inovação) e privada (gestor no Grupo Amorim e AEP) associadas às temáticas da Inovação e Conhecimento. Docente na Universidade do Porto e Universidade Católica Portuguesa, é autor da obra "O Novo Capital".

Resumo

Estamos na Sociedade do Conhecimento e o paradigma do modo de funcionamento da sociedade mudou. É hoje importante disseminar tudo o que se sabe e importa que individualmente se coloque em prol da sociedade a criatividade e capacidade inovadora de cada um, fazendo o que se chama empreendedorismo. Estes são fatores críticos da mudança numa sociedade de vivência num modo participado. Com efeito, a grande alavancagem deste novo modo de estar resulta de se estar na rede, de usar as tecnologias de informação e comunicação.

O fator tecnológico é central na dinamização desta "Nova Agenda de Inteligência" em Portugal mas também apostar na excelência deve constituir um compromisso permanente na procura de criação de valor.

Há uma oportunidade de reinvenção de identidade nacional com base nas nossas capacidades através da implementação de um Modelo Estratégico de Desenvolvimento diferente e com outros resultados.

Abstract
The Key to Competitive Intelligence

We are in a "Society of Knowledge" and the paradigm of her inner workings has changed. Today it is important to disseminate everything we know and it matters that each individual can and should put his creativity and innovative capability at the service of the society, doing what it is commonly called as entrepreneurship. These are critical factors of change in a participated society. Actually the big support for this new way of living is associated to being in the net and using and exploring the information and communications technologies.

The technological factor is central to the boosting of a "New Agenda for Intelligence" in Portugal but also if we want to bet on excellence and assume a permanent commitment towards the value creation.

There is an opportunity of reinventing the national identity based in our capabilities and through the implementation of a different Model of Strategic Development and with other results.

Os Desafios da Sociedade do Conhecimento: do Mero Ciberespaço a uma Nova Revolução

O conhecimento, embora não sendo uma novidade, é talvez uma marca própria dos tempos de hoje, os da Sociedade da Informação e do Conhecimento. Sob articulação estratégica de atores relevantes do tecido socioeconómico regional como decisores políticos, empresas, universidades e centros de inovação, o conhecimento tem de ser estruturado e adaptado às novas dinâmicas da economia, nomeadamente a global, apoiado sobretudo nas Tecnologias de Informação e Comunicação (TIC) no pressuposto da criação e sustentação de valor.

A diferença estará na capacidade de combinar eficiência com inovação mas para isso impõe-se:

Dar aos atores dinâmicos da sociedade civil (empresas, universidades, centros de I&D, empreendedores) a possibilidade de participarem de forma ativa numa verdadeira rede integrada de inovação e informação;

Proceder a uma ligação prática entre empresas e centros de conhecimento (universidades, centros I&D), usando as TIC como instrumentos dinâmicos de aumento de produtividade e reforço de valor na cadeia produtiva;

Criar centros de excelência e competitividade em zonas do interior ou mais desfavorecidas e que contribuam para a correção de assimetrias no desenvolvimento;

Participação na criação de riqueza e valor por parte dos diferentes atores sociais é um ato aberto mas avaliado segundo as dinâmicas da economia do conhecimento.

O investimento em conhecimento implica uma nova leitura do território. É conduzir a sociedade civil a protagonizar uma nova atitude, para intervenção: entendimento da evolução do conhecimento, capacidade de empreender para mobilizar novos projetos e criar valor e fixar riqueza; pensar de forma estruturada e atuar de forma organizada.

É papel da sociedade do conhecimento organizar a articulação dos atores, conformar vontades estratégicas, focalizar apostas, fazer equilíbrio entre inovação/criatividade e racionalidade/eficiência. Para esses desafios é importante elevar a qualificação das pessoas, habilitando-os a ser um novo tipo de cidadãos, como protagonistas ativos dum projeto de mudança coletivo.

A sociedade do conhecimento é de todos e para todos. Para isso é preciso dar um sentido de mobilização global. A participação de cada um numa sociedade

aberta só tem sentido se corresponder a uma aposta sentida e vivida em ideias e valores em que se acredite convictamente.

O conhecimento é o novo capital. A inovação e a criatividade são a voz duma economia global.

A Inteligência Competitiva

Quando esteve em Portugal Thomas Malone, emérito professor da MIT *Sloan School of Management*, apresentou uma excelente visão sobre o papel que a "inteligência coletiva" tem nas organizações do futuro. Trata-se de uma nova plataforma de articulação entre os diferentes atores, destinada conhecer as "competências centrais" da sociedade e qualificá-las duma forma estruturante como vias únicas de criação de valor e consolidação da diferença. Para Portugal a oportunidade é única também. Impõe-se, de facto, um sentido de "inteligência competitiva" num tempo novo que se quer para o país.

Para Portugal a essência desta nova "inteligência competitiva" tem que se centrar num conjunto de novas "ideias de convergência", a partir das quais se ponham em contacto permanente todos os que têm uma agenda de renovação do futuro. Importa acelerar uma cultura empreendedora em Portugal. A matriz comportamental da "população socialmente ativa" do nosso país é avessa ao risco, à aposta na inovação e à partilha de uma cultura de dinâmica positiva. Importa por isso mobilizar as "Capacidades Positivas de Criação de Riqueza" e fazer do empreendedorismo a alavanca duma nova criação de valor que conte no mercado global dos produtos e serviços verdadeiramente transacionáveis.

Na sociedade da "inteligência competitiva", a falta de rigor e organização nos processos e nas decisões, sem respeito pelos fatores "tempo" e "qualidade" já não é tolerável nos novos tempos globais. Não se poderá mais, a pretexto de uma "lógica secular latina", admitir o não cumprimento dos horários, dos cronogramas e dos objetivos. Não cumprir este paradigma é sinónimo de ineficácia e de incapacidade estrutural de poder vir a ser melhor. Importa por isso uma cultura estruturada de dimensão organizacional aplicada de forma sistémica aos atores da sociedade civil. Há que fazer da "capacidade organizacional" o elemento qualificador da "capacidade mobilizadora".

Pretende-se também um Portugal de "inteligência competitiva" mais equilibrado do ponto de vista de coesão social e territorial. A crescente (e excessiva) metropolização do país torna o diagnóstico ainda mais grave. A desertificação do interior, a incapacidade das cidades médias de protagonizarem uma atitude de catalisação de mudança, de fixação de competências, de atração de investimento empresarial, são realidades marcantes que confirmam a ausência duma lógica es-

tratégica consistente. Não se pode conceber uma aposta na competitividade estratégica do país sem entender e atender à coesão territorial, sendo por isso decisivo o sentido das efetivas apostas de desenvolvimento regional de consolidação de "*clusters* de conhecimento" sustentados.

A sociedade civil portuguesa tem nesta matéria um papel central. A aposta na excelência, na sua diferença e no seu sucesso, é o resultado duma agenda estratégica que se pretende voltada para um futuro permanente. Apostar na excelência deve constituir um compromisso permanente na procura do valor, da inovação e da criatividade como fatores críticos da mudança. Os bons exemplos devem ser seguidos, as boas práticas devem ser percebidas, o caminho tem que ser o da distinção e da qualificação. Na sociedade da "inteligência competitiva" sobrevive quem consegue ter escala e participar, com valor, nas grandes redes de decisão.

Num país que se quer voltado para o futuro, as empresas, as universidades, os centros de competência políticos têm que protagonizar uma lógica de "cooperação positiva em competição" para evitar o desaparecimento. O desafio da "inteligência competitiva" tem que ser desenvolvido. Fazer de Portugal a "oportunidade possível" dum país onde o conhecimento e a criatividade sejam capazes de fazer o compromisso, nem sempre fácil, entre a memória dum passado que não se quer esquecer e um regresso a um futuro que não se quer perder.

O Fator Tecnológico

O fator tecnológico é central na dinamização desta "Nova Agenda de Inteligência Competitiva" em Portugal. Para tal, importa saber responder às seguintes questões:

(1) O modelo de criação de valor na maior parte dos setores económicos do país continua a enfermar da falta de "leitura" estratégica dos novos *drivers* do crescimento – a "mecânica" de Porter, e de outros discípulos da competitividade, ainda não está suficientemente internalizada na prática da maior parte das empresas que a montante (utilização de recursos) e a jusante (integração nos circuitos comerciais internacionais) patenteiam ainda falhas estruturais incompreensíveis;

(2) A dimensão social do paradigma nacional está esgotada. Novos desafios exigem soluções pragmáticas e claramente que a integração social e o fomento da empregabilidade, próprios duma sociedade justa e equilibrada, têm que assentar na sustentabilidade do mercado económico e não (apenas) em dinâmicas artificiais de política pública meramente conjunturais. A justiça social potenciada pelo emprego tem que assentar na capacidade dos

atores sociais criarem aquilo que recebem, para que o sistema funcione de forma sustentada;

(3) A aposta na inovação tecnológica tem que ser lida a partir do mercado e da fase final da cadeia de valor. Criar novos produtos e serviços, melhorar processos, qualificar a utilização dos circuitos internacionais, dando-lhes dimensão e escala, é o caminho exigido por quem procura. Continua a haver uma utilização inadequada de recursos e esforço em I&D a partir da oferta, quando o pragmatismo da economia global exige respostas claras, atempadas e marcadas pela criatividade.

(4) A relação dos cidadãos com o Estado tem que, duma vez por todas, ser clara, transparente e eficaz. Numa sociedade sem tempo, exigem-se respostas rápidas, simples e sobretudo potenciadoras do "valor" mais importante que é a noção da qualidade de vida no exercício do direito da cidadania. Por isso, importa qualificar e sustentar essa relação, cabendo ao Estado o papel central de criação das condições de salvaguarda dessa relação.

Num tempo global cada vez mais difícil, as pessoas e as empresas precisam de soluções. As "Agendas de Mudança" associadas ao fator tecnológico não se podem fazer por decreto. Impõem um "sentido de urgência" em que a vontade da participação de todos e a capacidade de apresentar alternativas com sentido tem que ser o "*enabler* da diferença". Mostrar a Portugal que há uma oportunidade de reinvenção de identidade que tem por base as capacidades dos portugueses na implementação de um "Modelo Estratégico de Desenvolvimento" diferente e com outros resultados.

Modernizar o Estado

A reinvenção estratégica do Estado, enquanto "plataforma de centralidade" onde convergem as dinâmicas de qualificação dos diferentes atores sociais, ganhou hoje um paradigma que não se pode cingir às especificações operativas de mecanismos mais ou menos necessários de "governo eletrónico" ou de ajustamentos organizacionais adequados a determinados posicionamentos conjunturais de orgânica interna. Se é importante, como Francis Fukuyama não pára de reiterar, a evidência da capacidade da sociedade civil protagonizar dinâmicas de liderança nos processos de mudança, não menos verdade é que compete ao Estado modelar a dimensão estratégica dessa mudança.

O Estado existe para servir os cidadãos e estes têm que se rever na capacidade positiva deste de legitimar uma relação de confiança essencial. Quando David Osborne nos fala da crescente oportunidade e necessidade de recolocar na agenda o *reinventing the government*, está claramente a colocar a tónica num dos elementos

centrais da modernidade competitiva das nações. Importa mais do que nunca reposicionar o Estado como *pivot* central da organização, monitorização e funcionamento adequado da nossa sociedade e fazer com que os cidadãos se sintam perfeitamente legitimados numa relação de confiança validada por um "novo Contrato Social".

Há que fazer por isso opções. Opções claras em termos operacionais no sentido de agilizar a máquina processual e através dos mecanismos da eficiência e produtividade garantir estabilidade e confiança em todos os que sustentam o tecido social. Opções claras em torno dum modelo objetivo de compromisso entre governação qualificada central, geradora de dimensão estabilizadora e indução de riqueza territorial através da participação inovadora dos atores sociais. Opções assumidas na capacidade de projetar no futuro uma lógica de intervenção do Estado que não se cinja ao papel clássico, *dejá-vu*, de correção *in extremis* das deficiências endémicas do sistema mas saiba com inteligência criativa fazer emergir, com articulação e cooperação, mecanismos autossustentados de correção dos desequilíbrios que vão surgindo.

Mais do que nunca se impõe neste tempo complexo um "novo Estado" capaz de projetar no país, uma dinâmica de procura permanente da criação de valor e aposta na criatividade. Num tempo de mudança, em que só sobrevive quem é capaz de antecipar as expectativas do mercado e de gerir em rede, numa lógica de competitividade aberta, o "novo Estado" não pode demorar. Tem que se assumir como ator "perturbador" do sistema, induzindo na sociedade e na economia um capital de exigência e de inovação que lhe conferirá um desejado estatuto de centralidade e sobretudo de inequívoca liderança no processo de mudança em curso.

Um "novo Estado" é um desafio à capacidade de mudança de Portugal porque é um percurso possível decisivo na nossa matriz social. O sucesso com que conseguir assumir este novo desafio que tem pela frente, será também em grande medida, o sucesso com que o país será capaz de enfrentar os exigentes compromissos da globalização e do conhecimento. O "novo Estado" tem que assumir dimensão global ao nível da geração de conhecimento, valor, mas também de imposição de padrões sociais e culturais. O "novo Estado" tem que ser o grande "ator da mudança" que se quer para Portugal.

A Inovação Aberta

Um dos pontos críticos para o sucesso desta "Estratégia de Inteligência Competitiva" é apostar na concertação entre todos os atores da cadeia de valor – ou seja, apostar na inovação aberta. Alguns investimentos recentes na área da inovação e informação, como a Embraer em Évora, vieram demonstrar que há uma capacida-

de muito concreta de Portugal e dos seus protagonistas, em conseguirem "agarrar" com sucesso a decisiva rota da inovação e desta forma alterar, duma vez por todas, o modelo de desenvolvimento económico para o futuro. Por isso, com esta aposta na inovação aberta fica claro para todos que só há um regresso possível – o do futuro e protagonizado por todos.

A economia portuguesa está claramente confrontada com um desafio de crescimento efetivo e sustentado no futuro. Os números dos últimos 20 anos não poderiam ser mais evidentes. A incapacidade de modernização do setor industrial e de nova abordagem, baseada na inovação e criatividade, de mercados globais, associada à manutenção do paradigma duma "economia interna" de serviços com um caráter reprodutivo limitado, criou a ilusão no final da década de 90 dum "crescimento artificial" baseado num consumo conjuntural manifestamente incapaz de se projetar no futuro. Por isso, as apostas têm que mudar e a escolha de Champalimaud é um sinal.

Portugal precisa efetivamente de alavancar esta aposta da "inteligência competitiva", com todas as consequências do ponto de vista de impacto na sua matriz económica e social. A política pública tem que ser clara – há que definir prioridades do ponto de investimento estrutural nos setores e nos territórios, sob pena de não se conseguirem resultados objetivos. Estamos no tempo dessa oportunidade: definição clara dos setores competitivos em que atuar; seleção, segundo critérios de racionalidade estratégica, das zonas territoriais onde se vai atuar e efetiva mobilização de "redes ativas" de comercialização das competências existentes para aposta em investimento de inovação.

A "inovação aberta" desempenha, no momento presente, um papel único de alavancagem da mudança. Portugal precisa de forma clara de conseguir entrar com sucesso no roteiro do investimento de inovação associado à captação de empresas e centros de I&D identificados com os setores mais dinâmicos da economia – tecnologias de informação e comunicação, biotecnologia, automóvel e aeronáutica, entre outros. Trata-se duma abordagem distinta, protagonizada por "redes ativas" de atuação nos mercados globais envolvendo os principais promotores setoriais (empresas líderes, universidades, centros I&D), cabendo às agências públicas um papel importante de contextualização das condições de sucesso de abordagem dos clientes.

Uma "nova economia", capaz de garantir uma economia nova sustentável, terá que se basear numa lógica de focalização em prioridades claras: assegurar que o "IDE[1] de inovação" é vital na atração de competências que induzam uma renovação ativa estrutural do tecido económico nacional; mobilizar de forma efetiva os

1 Investimento Direto Estrangeiro.

"Centros de Competência" para esta abordagem ativa no mercado global – mas fazê-lo tendo em atenção critérios de racionalidade estratégica definidos à partida, segundo opções globais de política pública, que tenham em devida atenção a necessidade de manter níveis coerentes de coesão social e territorial. A "Inteligência Competitiva" é a chave desta mudança. Num tempo global em que a aposta no valor e na competitividade devem ser uma motivação coletiva da sociedade portuguesa, aí está um exemplo a seguir.

A Educação Colaborativa

Na "Sociedade da Inteligência Competitiva" estudar é uma condição essencial para garantir a liberdade do exercício da cidadania. De facto, só com o domínio do conhecimento, o indivíduo pode assegurar a sua intervenção cívica numa sociedade coletiva complexa e global cada vez mais exigente. A questão é que a liberdade que Karl Popper defende implica uma mudança no paradigma da Educação. De facto, num tempo de crise e de falta de soluções, a escola tem que encontrar novas respostas. A "nova ambição para a escola" é também a nova ambição que queremos para uma sociedade bloqueada e que precisa de se reencontrar com o futuro. Precisamos por isso de apostar numa "Educação Colaborativa".

A "Educação Colaborativa" de que o país precisa, tem de ser capaz de dotar as "novas gerações" com os instrumentos de qualificação estratégica do futuro e aliar, ao domínio por excelência da tecnologia e das línguas, a capacidade de com criatividade e qualificação conseguir continuar a manter uma "linha comportamental de justiça social e ética moral" como bem expressou recentemente Ralph Darhendorf em Oxford. Tem que se ser capaz de, desde o início, incutir nos jovens uma capacidade endógena de "reação empreendedora" perante os desafios de mudança suscitados pela "sociedade em rede". Precisamos de um Portugal voltado para o futuro e apostado no papel das novas gerações.

A "cooperação estratégica" entre a escola, o meio social, as áreas de conhecimento, e os campos de tecnologia, não pode parar. Vivemos a Era da cooperação em competição e os alicerces da "vantagem competitiva" passam por este caminho, sob pena de se alienar o "capital intelectual" de construção social de valor, de que tanto nos fala Anthony Giddens neste tempo de (re)construção. Na economia global das nações, os "atores do conhecimento" têm que internalizar e desenvolver de forma efetiva práticas de articulação operativa permanente, sob pena de verem desagregada qualquer possibilidade concreta e efetiva de inserção nas redes onde se desenrolam os projetos de cariz estratégico estruturante.

Por isso, a oportunidade e a importância da "Educação Colaborativa", para além dos efeitos ao nível da revolução na utilização das TIC como um instrumento

de qualificação pedagógica, tem que ter a capacidade de elevar na escala produtiva as empresas portuguesas, aumentando as exportações, consolidando dinâmicas de inovação e reforçando o emprego. É isso que conta nos tempos difíceis que vivemos: assumir roturas estratégicas e implantar uma "agenda de modernidade" para construir um país realmente diferente. A educação assume-se, desta forma, como o *driver* efetivo da mudança e da construção duma identidade cultural mais forte.

O papel das novas gerações é decisivo. São cada vez mais necessários "atores do conhecimento" capazes de induzir dinâmicas de diferenciação qualitativa um pouco por todo o país, capazes de conciliar uma necessária boa coordenação das opções centrais com as capacidades de criatividade local, capazes de dar sentido à "vantagem competitiva" do país, numa sociedade que se pretende em rede. É assim que se garante a liberdade que Karl Popper defende e que todos nós queremos, cada vez mais, para um Portugal 2020 positivo.

Referências Bibliográficas

Faulkner, W. e J. Senker (1994). "Making Sense of Diversity: Public-Private Sector Research Linkage in Three Technologies". *Research Policy n.º* 23, pp. 673-695.

Felsenstein, D. (1994). "University – Related Science Parks – "Seedbeds" or "Enclaves" of Innovation?". *Technovation* n.º 2, pp. 93-110.

Freeman, Christopher e Luc Soete (2009). "Developing Science, Technology and Innovation Indicators: What We Can Learn from the Past". *Research Policy* n.º 38, pp. 583-589.

Porter, M. (1990). "The Competitive Advantage of Nations". *Harvard Business Review* n.º 2, pp. 155-195.

Porter, M. (1987). "From Competitive Advantage to Corporate Strategy". *Harvard Business Review* n.º 2, pp. 117-151.

Porter, M. (1985). "How Information Gives You Competitive Advantage". *Harvard Business Review* n.º 3, pp. 75-98.

Porter, M. (1979). "How Competitive Forces Shape Strategy". *Harvard Business Review* n.º 1.

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.

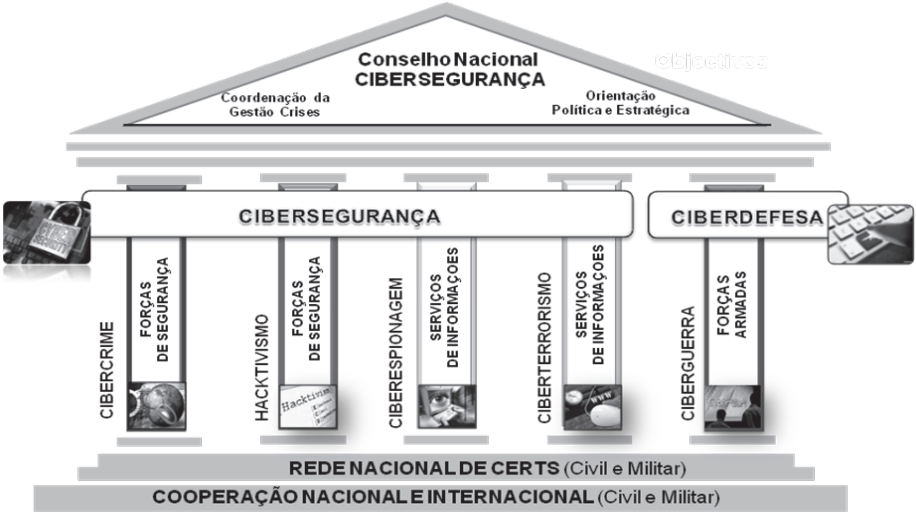
Reconhecendo-se a existência de um nível nacional e supranacional da cibersegurança (figura 1), constata-se que cada Estado terá que garantir não só a utilização segura do ciberespaço aos seus cidadãos mas também a salvaguarda da própria soberania.

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.

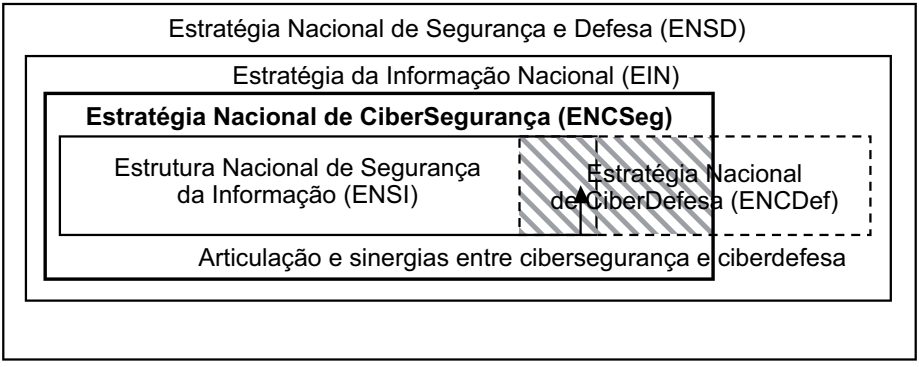
Atendendo ao princípio de que a cada forma de coação corresponde uma estratégia distinta (Couto, 1988: 227), a utilização da informação e do ciberespaço como forma de coação faz surgir uma nova estratégia, a Estratégia da Informação Nacional (EIN). Assim, como uma das componentes desta Estratégia e subordinada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

Protecting Critical Information Infrastructures

Eduardo Gelbstein

Ed Gelbstein has over 40 years experience in information systems and technology, both in the private and public sectors. His experience includes being Information Technology Strategy Manager for the British Railways and Director of the United Nations International Computing Centre. He was also an advisor to the United Nations Board of Auditors and the French Cour des Comptes. Ed is currently Adjunct Professor at Webster University Geneva and the author of several books and articles as well as a regular speaker at international conference on security, risk, audit and governance.

Resumo
Proteção de Infraestruturas Críticas de Informação

O recurso aos sistemas de informação na gestão e operação de infraestruturas críticas cresceu exponencialmente em todo mundo, sendo que atualmente não existem infraestruturas críticas que não dependam fortemente de software, computadores e redes informáticas.
Nenhuma tecnologia é perfeita e lidar com erros de sistemas faz parte das responsabilidades daqueles que fornecem e operam esta tecnologia. A ubiquidade das redes globais como a internet criou um desafio adicional: tentativas, por vezes bem-sucedidas, de aceder a estas tecnologias por parte de terceiros com a intenção de interromperem estas operações ao abrigo de justificações que vão desde o simples desafio individual, ao ativismo e, potencialmente, a operações de natureza militar ou terrorista.
Os desafios associados à proteção de infraestruturas de informação crítica da qual a sociedade depende para funcionar, são variadas e complexas e têm de lidar com componentes passíveis de gerarem erros: pessoas, processos e tecnologia.
Este artigo fornece uma visão sobre estes desafios e aponta sugestões e referências quanto às melhores práticas.

Abstract

The use of information systems in the management and operation of critical infrastructures has grown explosively around the world and, today, there are such infrastructures that do not have a strong dependency on software, computers and networks.
No technology is perfect and dealing with malfunctions is part of the responsibilities of all those who supply and operate such technology. The ubiquity of global networks such as the Internet has created an additional challenge: attempts, often successful, to access such technologies by external parties intent in disrupting their operations for any of a number of reasons, ranging from "because I can" to activism and, potentially, military and/or terrorist.
The challenges of protecting the critical information infrastructures, on which society depends to function, are many and complex as they have to deal with three imperfect components: people, processes and technology. This article provides an overview of these challenges and includes pointers and references to established standards and good practices.

Social and economic stability require the reliable operation of many Critical Infrastructures. While there are many definitions of what is a Critical Infrastructure, the one adopted by ENISA[1] states:

"Those interconnected systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy".

These include all utilities such electricity generation and distribution, water treatment, air traffic control, airport and airline operations, railroads and ports, telecommunications, logistics, law enforcement, refineries, banking, finance and many more.

All of these have, at one time or another, suffered disruptions that had significant economic and social costs. All such critical infrastructures have an irreversible dependency on computer systems and networks used to automate and support their operations and it is therefore appropriate to think of them as Critical Information Infrastructures (CII).

For the purpose of this article, the specific and essential characteristics of a CII are that:

- It operates seven days a week, 24 hours a day.
- Their operations require information systems and networks, sensors and other mechanisms for data acquisition.
- Many also operate physical devices ranging from cash dispensers (ATM) to motors (e.g. to switch a railroad track) and robotic systems (e.g. in manufacturing and other continuous processes).
- It is part of a supply chain – operational failure propagates to other entities that may also be CII.

When the objective of cyber-attackers is to – at the very least – cause disruption, CII are attractive targets.

The measures to protect CII described in these pages can be found everywhere and are based on a relatively small number of standards and good practices. However the way in which they are practiced are, like snowflakes, similar but different. The challenge is to demonstrate that they are "good enough" and this is hard enough.

1 European Network and Information Security Agency, www.enisa.europa.eu

Given the frequent, numerous and successful cyber-attacks on such systems and networks by largely unknown players, they should be considered to be potential targets of future cyber-attacks. This, in turn, creates a need for information security to be adequately implemented, managed and assessed.

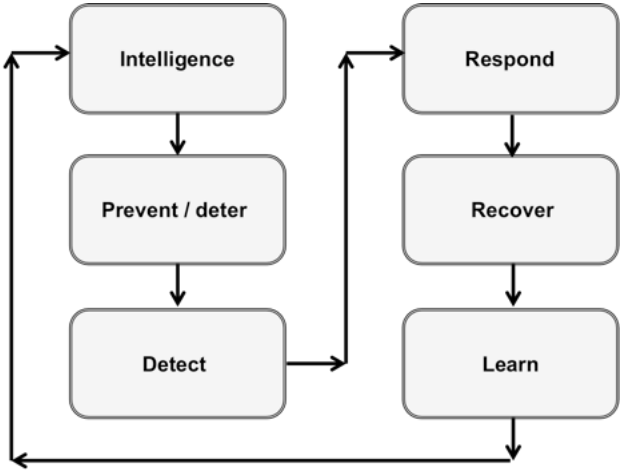
This article makes the assumption that CII operate within several constraints, notably financial, regardless of whether they are in the public or private sector, as well as cultural. The latter include risk aversion and resistance to change as well as difficulties to recruit and retain talented and experienced people.

The objective of information security is to provide adequate assurances of an organisation's information availability, confidentiality and integrity.[2]

The attackers' objectives are the precise opposite: to interfere with access to information, to steal and disclose sensitive or valuable information and to corrupt or destroy data.

The Lifecycle of Information Security

Sustainable security requires (at least) that the six tasks shown in the figure below to be performed adequately.



The main activities, which must be carried out proactively, are:

- Intelligence: this consists of several separate activities carried out by different people.

2 Appendix 1 provides definitions of the main information security terminology.

- Business Impact Analysis (BIA): usually associated with business continuity planning, a BIA identifies the most critical information components and processes of an organization.
- Risk Assessment: a detailed evaluation of the threat landscape of an organization's information covering physical events (such as earthquakes), accidental human intervention (errors, mistakes, ignorance and stupidity) and deliberate human intervention. The latter can be direct (such as fraud by an employee) or indirect (specifically, a cyber-attack). Risk assessment requires that specific attention be given to monitoring and tracking information security events around the world as attacks tactics and techniques change rapidly and, in reality, every organization should consider itself to be a potential target.
- Risk Management Plan: a portfolio of measures, technical and managerial, designed and tested to mitigate the impact of such events.
- Prevent and Deter: A key part of an information security strategy, this consists of protecting the information systems and data, regardless of where they are located, with appropriate tools and processes, ensuring these are up to date, building awareness of good security practices amongst the systems and data owners, those who use the systems and encouraging good behaviour. It must be recognised that a 100% ability to prevent and deter a cyber-attack is not achievable. The information security strategy should define what constitutes an acceptable level of security.
- Detect: the ability to detect an intrusion or attack is essential to take measures to contain and manage the attack. There are many tools (such as Intrusion Detection Systems) that can assist in this activity but none of them is perfect. Recent examples of intrusions that were undetected for a significant period of time were the subject of independent reports[3], and extensive media coverage. Obviously, detection is a pre-requisite to being able to respond.
- Respond: the collection of activities needed to manage an incident effectively, contain and repair any damage, collect information in such a manner that it can be used in evidence (digital forensics), involve law enforcement or other external parties, etc. The speed of response is fundamental to minimize damage and consequent losses.
- Recover: the steps needed to return to normal operations. Depending on the nature of the cyber attack, it may require communications to stakeholders, compensation for losses and reports to regulatory authorities.

3 Available at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf and http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

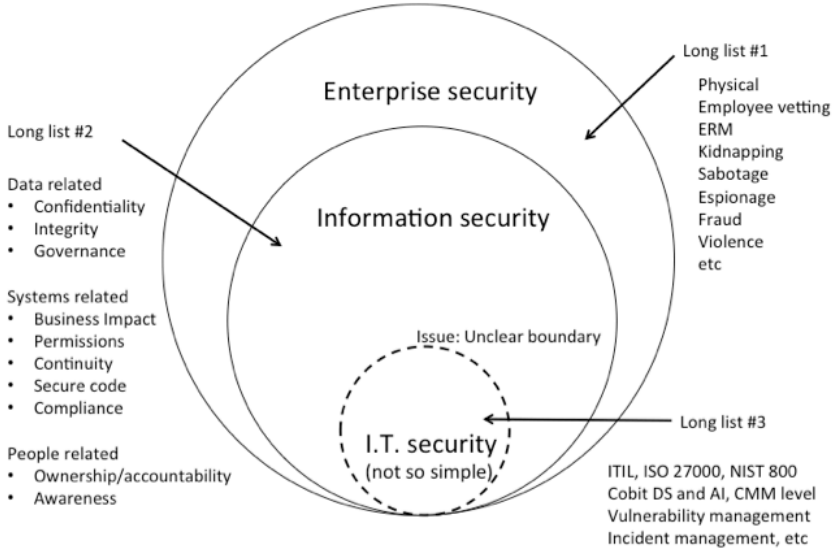
- Learn: every cyber attack represents an opportunity to learn about the effectiveness of information security arrangements, what could have been done better and what steps should be taken to strengthen security.

The converse of this is also true: every attack, regardless of whether it succeeds or fails, provides attackers with information about the security arrangements of the target. Unfortunately, this is an asymmetrical relationship: the defenders need to fight the battle every day while the attackers choose their time and have nothing to lose if they don't succeed.

The Architecture of Information Security

The statement "information security is everybody's responsibility" may appear to be a platitude, but is totally correct. The figure below shows a security architecture in which all the elements must be present and properly managed to deliver a sustainable information security.

It is easy to confuse Information Technology (IT) Security – a discipline in its own right – with Information Security and even then, not to fully appreciate how this interfaces with the overall Enterprise Security. The Figure below, presents a holistic view of how accountability for security is distributed in an organisation.



This discussion begins with the smallest (but visible and talked about) component: I.T. security. This is the technical component that is fully integrated in technical operations, regardless of whether these are provided within the company or by an external third party such as an outsourcing company.

Most people are familiar with words such as "firewall" and "anti-virus" but may not appreciate that these are merely some of the component parts. An appendix to this article gives definitions for the most commonly used terms in information security and the next section will discuss this topic in greater detail.

What the reader is invited to note are the things for which those providing for Information Technology Security are not accountable, amongst them:

- The classification of data and information into categories such as "public", "restricted to…", restricted until…", "confidential", "secret" and other as required to meet an organisation's needs;
- The assessment of the business impact of a security breach;
- The definition of access rights and privileges, i.e. who can be granted access to a network, system or database and, within that access what specifically they are authorized to do;
- Ensuring the quality of software (licensed from a third party or developed in-house). "Software" may include not only applications but also spreadsheets with complex formulae and web pages;

The parties accountable for these activities are those ensuring Information Security, the non-technical component. These parties include the functional managers who "own" computer systems such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and other corporate systems, usually licensed from a vendor and customised to meet the working practices of the organisation. The vulnerabilities of such systems tend to be identified and corrected by their vendors, as they tend to have substantial numbers of clients who would be quick to report them.

In addition, there are "Line of Business Systems", those specifically designed to meet the unique requirements of the core activities of an organisation. These may be highly complex as, for example, those for air traffic control or supply chain management. In addition to their operational criticality, these systems rely on support from a relatively small number of individuals with vital knowledge.

Changes to these systems to enhance their functionality or correct a defect are known to be a time of high risk of malfunction. Moreover, the vulnerabilities of such systems, particularly when they are "one of a kind" are likely to be unknown unknowns.

Critical Information Infrastructures frequently also need another family of computer systems and networks globally referred to as Systems Control and Data Acquisition (SCADA) which are physically distributed and not managed by the IT

function as many of them are embedded into the controls of physical devices and as such, designed and maintained by vendors. Most SCADA devices have been designed to be physically robust and reliable. Security features were, traditionally, not part of the design specification and it can be assumed that many such devices remain in use. The latest generation of SCADA is believed to be considerably more secure as their operational criticality has become clear to their designers.

Other parties with key roles to play in information security include the Procurement function (contracts need to be specific on liabilities should an event occur), the Human Resources function (to report on changes of function, disciplinary action or investigations that would require access rights to the individual to be suspended, etc.), Legal Counsel (on contracts, disciplinary action, the contents of security policies, etc.), and other players will depend on the nature of the organisation.

As information security is tightly linked to enterprise security, there are other components to consider: per-employment checks, the issuance (and control) of credentials to enter a buildings or specific zones of a building, services that allow non-employees access (for example cleaners and vendors' maintenance personnel), the keeping of access logs, investigations, etc. Finally there is the Governance role of executives and senior management. This will be discussed further in the sections that follow.

All of these activities can be undermined if those who use information networks, systems and data are inadequately aware of their responsibilities with regards to information security or, worse, are not sufficiently motivated or engaged with the activities of the organisation and, as a consequence, fail to behave in a manner that protects the information assets of an organisation. Examples of such behaviour include the disclosure of information to unauthorised parties or simply ignoring security policies that rely on their cooperation.

The Components of Information Security

It is well known that a chain is only as strong as its weakest link. This article suggests that the information security chain has five links:

- Governance;
- Technology;
- Processes;
- People;
- Standards and Best practices.

The last of these is probably the strongest while "people", in the author's experience as a practitioner and auditor, almost certainly the weakest. The short discussion that follows attempts to explain why this is the case.

Governance

The governance of information security is a subset of the governance of information systems and technology, which in turn, is a subset of enterprise governance. If and when senior management abdicates its responsibilities for such governance, practitioners are obliged to second guess the organisation's security needs and work on a "best effort" basis.

The three basic governance functions as defined in international standards[4] are to: Direct, Evaluate, and Monitor (ISO 38500, ISO 27014, and other).

Senior management and, ideally, the Board of Directors, should:

- Be informed about information security and its relevance to the organization;
- Set strategy and policy, including the management of non-compliance;
- Provide technical, human and financial resources for information security;
- Assign responsibilities to management and set priorities;
- Monitor the security performance of the organization and initiate corrective actions as required.

Management's role is to assume responsibility for all operational aspects of information systems governance and deal with them proactively:

- Assessing and analyzing the impact of information systems on the organization (BIA);
- Assessing, analyzing, and managing risks associated with information systems;
- Setting information security policy;
- Assigning responsibilities to staff;
- Defining the information security management framework for the organization;
- Implementing security awareness training of all staff,

Standards and best practices for information security governance are listed in Appendix 2.

Technology

The range of technologies in today's organisations is vast, ranging from the data centre components of servers, network devices, storage, power supplies, diagnostic systems, SCADA devices, etc. These are typically "invisible" to the rest of the organisation (except at budget time).

Each of these technical components is a potential source of insecurity in itself, for example by constituting a Single Point of Failure or by containing hidden flaws

4 ISO 38500 (information systems) and ISO 27014 (information security) amongst them.

that make them insecure by design as is usually the case with software. Vendors continually issue fixes (also called patches) to remedy such flaws as and when they are discovered. It's up to the information technology service provider to implement these fixes, some of which are themselves faulty and introduce new vulnerabilities.

There is however, much more technology that introduces security vulnerabilities. A recent concern has been the rapid spread of the "Bring Your Own Device" (BYOD) concept as increasingly IT literate staff no longer wishes to be constrained by corporate technical choices and "insist" on making their own choices, initially for using their home computers and networks and more recently with smart phones and tablets.

Processes

Security practitioners have adopted three fundamental information security principles and turned them into processes – activities that are structured to be consistently repeatable and reviewed and refined to remove all (or as many as possible) systematic errors. These are:

- Need to know: information is classified and access to it is provided to enable a person to perform their tasks, but no more. The technical solutions to achieve these are globally referred to as Role Based Access Control.
- Least privilege: also related to the role of the person accessing systems, this principle defines the actions allowed, ranging from "read only, no printing or downloading allowed" to "create new record".
- Separation of duties: The limiting of individual authorities to ensure that sensitive transactions are reviewed and approved by another person (or more than one). Originally introduced to prevent fraud, this principle has found its way into other domains, such as managing technical changes and monitoring testing.

This is just the beginning of a long list of processes that support information security. The scope of this article does not allow a detailed discussion of all of them. Two key processes that management should be aware of (and control appropriately) are those of:

- Information (and data) classification: briefly mentioned earlier in this article.
- Identity and access management: the steps needed for a person to be given the credentials needed to access corporate networks and systems and their subsequent lifecycle. At the technical level (and mostly hidden from view) is a whole portfolio of processes that include such things as "change management", "configuration management", "promotion from test to produc-

tion", etc. Thick books[5] and many websites describe them in various levels of detail.

- Encryption: a method to render data unreadable to unauthorised parties.

People

Responsibility for information security, although not likely to be mentioned in any job description (other than that of the Chief Information Security Officer) rests with virtually everybody.

Board Members, Executives and Senior Managers have a primary role in Governance.

Functional Managers in Finance, Human Resources, Procurement, etc. are the custodians (some refer to them as "owners") of information assets – applications software and, more importantly, data and information.

The users of such systems and data should have contractually defined accountabilities for protecting such data from disclosure, theft, corruption and deletion. This accountability may have already spread beyond the boundaries of the organisation as information sharing with partner organisations and/or other members of a supply chain demanded it, thus creating an additional challenge for the management of Identity and Access rights.

The same users have, in recent years, challenged corporate technology choices and demand the right of using technologies of their own choice for home computing, smart phone and tablets under the concept of BYOD.

Unless the organisation takes preventive measures to avoid architectural anarchy and place controls on such devices, the risk of malware attacks and theft of intellectual property is increased.

The urge to be "permanently connected" also encourages owners of such devices to use public unencrypted networks, typically the free of charge wireless networks in hotels and coffee bars to access sensitive corporate systems while being unaware how easy it is to intercept such exchanges and also acquire login information such as user names and passwords.

Another people-related challenge relates to the explosive popularity of social networks (there are hundreds of them) and web based discussion sites and blogs which, in the absence of clear policies and controls could constitute a further information security risk.

Last but not least, are the people providing information technology services. They may be members of the organisation, an external service provider or a mix of

5 The Information Technology Infrastructure Library (ITIL), the Data Management Body of Knowledge (DMBOK), the Control Objectives for Information Technology (COBIT) are well established examples.

both. In the latter two situations terms of contract and relationship management become critical activities.

Standards and Best Practices

Information security has been recognised as an important topic for many years and this is reflected in the large volume of standards and best practices currently available. A summary list of the most widely recognised is included as Appendix 2.

The adoption of standards and best practices is essentially optional. It is a fact that these are the result of work and discussions by professional bodies and practitioners over a period of many years. Adopting them recognises that they represent their collective knowledge and experience. On the other hand, not adopting them represents one of two things:

- The organisation that chooses not to adopt such standards and best practices is more advanced in the practice of information security than their latest edition (and no doubt some are);
- The culture of the non-adopters is one of learning from experience (known as being the best teacher and also the most expensive).

Adopting such standards and best practices requires considerable effort and changes to the way security-related activities are conducted. In the first instance, the documents listed in Appendix 2 represent a large amount of information – thousands of pages to read study and understand.

Having got to this point, the next stage consists of conducting a gap analysis to identify the areas where meeting the requirements of the standard or best practice requires activities and/or changes and then carrying them out.

This requires motivation and, most important of all, time. This happens to be the resource of which we all have the least.

The Challenges of Information Security

The previous sections could be regarded as textbook stuff and now is the time to explore why, in practice, all the things mentioned before have not solved that information security "problem".

Governance

A recently published paper[6] discusses the challenges of information security governance (ISG) in some detail. This section summarises its main points as situations that practitioners and auditors encounter regularly.

It is widely advocated that Board Members, Executive and Senior Management play an active role. In practice, this is difficult to achieve because of the numerous and diverse demands on their time. In addition, practitioners are often tempted to use technical, rather than business, language creating a communications barrier and possibly losing credibility in the process.

Another driver for the failure of ISG has to do with the inevitable and human Office Politics that result in a silo mentality of "it's not in my job description" and an unwillingness to share information or collaborate towards a common objective.

Another aspect of weak ISG concerns security policies (and compliance thereto). It's easy and tempting to engage consultants to prepare such policies, which they do using templates. There is absolutely nothing wrong with such templates given that they are based on international standards and best practices.

The issue is a lack of ownership within the organisation that leads to the policies taking a long time to be issued (need to be consulted with Human Resources, Staff Representatives, Legal counsel and others) and then risk being forgotten about, i.e. not updated, not tracked to determine who has read them, if there has been a formal agreement to accept and follow such policies. Unless the policies can be enforced automatically by computer systems, there is a risk they will be ignored.

Technology

Management rely on their technical staff (or that of their service providers) for advice on technologies appropriate to meet their requirements. Technical staff relies on vendors and product reviews by independent industry observers. The truly independent observers are reputable companies that charge for their services, and therefore, not everybody subscribes, relying instead of "free" publications many of which carry advertisements for the same vendors they report on.

Many vendors have long histories and excellent track records for seriousness and quality. This does not stop their marketing departments from being perhaps too optimistic about their products, which invariably claim to be the "ultimate" answer to whatever they specialise in. In the field of information security vendors

6 Gelbstein, Eduardo, 2012. "Strengthening Information Security Governance". ISACA Journal n.º 2.

come and go. The expression *caveat emptor* is just as valid as it was when first stated.

The life cycles of technology are short and the I.T. industry is highly innovative. This means that investment cycles are short and the need to procure new products is constant. Many products can introduce major disruption to an organisation – this was the case with the personal computer, local area networks, graphical user interfaces, the Internet, mobile everything and the potential loss of control of the organisation's technical architecture. This has security implications which need to be balanced against the potential benefits of these innovations.

Processes

The challenge of implementing processes is that of making sure that the right things are done the right way and well enough.

In practice, this easier said than done. In the first instance, consensus (or clear direction) on what are "the right things" is essential, as these are not necessarily the same for all organisations at a given time. What these things are depends on the status of information security management at a given time.

For example, for an organisation that has not reviewed its information security policies for the last six years, the "right thing" may be to do so immediately. Another example could involve a situation where the Chief Information Security Manager is an individual that has no backup in the organisation. Should the situation arise that this person leaves the organisation or is unavailable to work for an extended period of time, identifying a second person to take over would also be the "right thing" to do.

Doing things "the right way" relates to the organisation's willingness to adopt a specific set of standards and/or best practices and implement them, and then ensure that appropriate training is part of the implementation project.

The third part, "well enough" is again an individual assessment driven by the nature of the organisation and its security needs. This is explore further later in this section under Assurance.

Some standards and best practices support a certification of compliance process, notably ISO 27001 "Information Security Management System (ISMS)". There is debate about the value of such certification for three reasons:

- It is possible to obtain it for a limited part of an organisation's information security arrangement.
- That it is only valid for a limited period of time, requiring regular audits and re-certification.
- That it may give management a false sense of security given the changing nature of attacks.

People

The challenges relating to people are enough to fill a book. For the purpose of this article, only two are included:

- Certifications: information security professionals can acquire, in addition to degrees and experience, formal certifications from independent organisation, notably:
  - The Information Systems Audit and Control Association[7] (ISACA) – the Certified Information Security Manager (CISM) and the Certified Information Security Auditor (CISA).
  - The International Information Systems Security Certification Consortium[8] (ISC2). This body can accredit an individual as a Certified Information Systems Security Professional (CISSP) and several others.

Requiring information security professionals in the organisation to have or acquire such certifications is a governance and human resource management question the answer to which has implications in terms of availability and conditions of employment (compensation package).

Another possible certification, internal to an organisation, would be a license to access sensitive computer systems and data, requiring the completion of a number of training modules and a test, the informational equivalent to a driving license.

- Engagement: studies published in the recent past indicate that in many organisations, particularly large one, employee engagement (or lack of it) may be an issue. Disengaged staff have limited commitment to the organisation, seen mainly as a source of income, and are apt to disregard policies and best practices. This makes disengaged staff a security risk.
- Standards and best practices: the challenges here are not simple to resolve: should the organisation adopt standards and best practices? Which ones would be the most appropriate?

While it's tempting to answer the first question in the affirmative, the effort and time involved in doing so are significant if this is to be done well enough. Management and staff commitment are essential to succeed and this cannot be done without adequate resources and determination as doing so is likely to require many changes: cultural, procedural and technical.

The second question is even harder as there are several options ranging from fairly general and non-prescriptive international standards, such as the ISO 27000 series, to national standards in the public domain such as the U.S.'s NIST SP 800 series and others that integrate the perspectives of governance,

7 www.isaca.org.

8 www.isc2.org.

audit and management such as the recently published COBIT5 for Information Security. There is, in the author's opinion, such a thing as "best".

Assurance

The remaining challenge to explore here is that of knowing how good an organisation's information security actually is. There are five complementary approaches to consider, each of them having plus and minus points:

- Information security metrics: it is often said that "you cannot manage what you do not measure" and collecting meaningful information on information security is hard to do. Many publications have long lists of things that *can* be measured. Some metrics can be very useful such as availability, number of dormant credentials (i.e. issued but not used), failed attempts to login, but collecting such data requires resources and judgement needs to be exercised in defining what is worth collecting and analysing. The significant point about metrics is that they are lagging indicators and therefore not useful to predict future performance. The fact remains that attack methodologies and tools continue to evolve and are, therefore, unpredictable.
- Information risk, vulnerability and security self-assessments: a good practice, particularly to identify vulnerabilities and in fact, those accountable for security performance are the best qualified to do this. The minus point is that optimistic bias can find its way into the assessments as not everyone is willing to admit to shortcomings of one's work or organisation.
- Independent certifications: these have been mentioned in the previous section.
- Audits: valuable when carried out by experienced and qualified auditors following formal guidelines. Useless when done by inexperienced people ticking boxes in a form without seeking evidence to support any claims made by the audited. Furthermore, audits are disruptive to day-to-day work and there is rarely a "good time" to be audited.
- Penetration tests: these will really tell an organisation how good their defences are – on condition that the ethical hackers employed are a) very capable and b) independent. A good way to conduct a penetration test would not give prior warning to those responsible for information security. However this may not be a good way to maintain their goodwill and commitment, so it's a delicate decision. It should be noted that the ethical hackers will, as a result of their tests know more about internal security arrangements than the professionals providing this service. Legally binding confidentiality agreements and a large measure of trust are essential.

Conclusions

- Every organisation should consider itself a target of a cyber attack. Many are unprepared.
- 100% information security is not achievable. Technology alone cannot provide security – it needs to be complemented by governance, processes and people.
- Everyone, from senior management to the uniformed (and possibly outsourced) security guard has a role to play to ensure an organisation's information security.
- People are the weakest link in the security chain. The practices that support information security are not self-evident and must be clearly communicated and supported.
- How much insecurity is "acceptable" will vary from one organisation to another.
- Security assurance through metrics, self-assessments, certification, audits and penetration tests needs to be used regularly if information security is critical to the role of the organisation.

Appendix 1
Basic information security definitions and terminology

The objective of **Availability** is to ensure that information can be accessed by those authorised to do so.

The objective of **Confidentiality** is the prevention of unauthorized disclosure of information.

Integrity has the objective of protecting information from unauthorised modification or deletion.

Hacker a person (in fact various types of person) who circumvents the security measures of a computer system. They intent on disruption or other malicious activity are often referred to as "Black Hat Hackers" or "Crackers". Those who use their skills to identify vulnerabilities, with or without the consent of the systems owners are called "White Hat Hackers" or "Ethical Hackers". There are, of course, those who are morally ambiguous, referred to as "Grey Hat Hackers".

Malware is an abbreviation of Malicious Software. This is designed with a multiplicity of purposes, including hostile, intrusive and annoying and used to disrupt computer operations, access private and/or sensitive information and/or take over a user's computer (without their knowledge). Malware can take many forms and evolves continuously. Its various forms include Virus, Worm, Trojan

Horse, Rootkit, Macro, Logical Bomb, and more.

SPAM is (other than the commercial product) unsolicited electronic messaging. While most common in electronic mail it has spread to other activities such as text messages on mobile phones, blogs and other forms of exchanges.

Botnet is a collection of computers connected through the Internet that are under the control of a "bot-herder" or "bot-master", who may have criminal intent – disseminating spam through the target computers – or disruptive intent – launching a Denial of Service Attack on a target organisation. Individual computers are compromised by malware and integrated into the botnet.

Denial of Service (and Distributed Denial of Service) a form of attack intended to temporarily (or indefinitely) interrupt the ability of a computer (such as a server) connected to the Internet to operate. Botnets are often used to achieve this objective.

Firewall is a device (hardware and/or software) designed to control the flow of information in and out of computing devices and, using a set of predefined rules, decide whether or not to allow the data to cross the device.

DMZ, an abbreviation of Demilitarised Zone, is an intermediate network that buffers an organisation's internal and presumed secure network from the Internet, presumed insecure.

SIEM, abbreviation of Security Information and Event Management – such systems provide real-time monitoring, correlate events and provide notifications to operational staff. It also provides storage, analysis and reporting of log data to provide information on trends and potential compliance issues.

Appendix 2
A short (and not comprehensive) list of standards and best practices for information security

International Standard ISO/IEC 38500-2008, "Corporate governance of information technology".

International Standard ISO/IEC DIS 27014-2012, "Information technology – Security techniques – Governance of information security".

International Standard ISO 31000-2009: "Risk Management, Principles and Guidelines".

International Standard ISO 31010-2009: "Risk Management, Risk Assessment Techniques".

"Control Objectives for Information Technology" (COBIT), Version 5, 2012, Information Technology Governance Institute.

"COBIT 5 for Information Security", 2012, Information Technology Governance Institute.

"Information Security Guidance for Boards of Directors and Executive Management", 2nd Edition, 2006, Information Technology Governance Institute.

"Information Security Guidance for Information Security Managers, 2008, Information Technology Governance Institute.

The Risk IT Framework and its Practitioner Guide, 2009, Information Systems Audit and Control Association.

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) issued by the Software Engineering Institute at Carnegie Mellon University (USA).

"The Standard of Good Practice for Information Security", 2011, Information Security Forum.

"Information Security Handbook: A guide for Managers" (SP800-100), 2007.

The Data Management Body of Knowledge (DMBOK) published in 2009 by the Data Management Association.

International Standard ISO/IEC 20000-2011 "Information Technology Service Management" (parts 1 to 5).

"The Information Technology Infrastructure Library" (ITIL) Version 4, issued in 2011 consists of five volumes (ISO 20000 is fully compatible with the ITIL framework.

British Standard BS 25999 "Business Continuity Management" (parts 1 and 2) issued in 2006 and 2007.

The "Business Continuity Management Body of Knowledge" is available online and is continuously evolving through contributions from practitioners.

International Standard ISO/IEC 27000 series (from 27001 to 27014 at the time of writing) "Information Technology Security Techniques), latest versions published in 2011.

"The Standard of Good Practice for Information Security", 2011, Information Security Forum.

The USA government series SP-800 (over 100 publications).

International Standard ISO/IEC 27007-2011 "Information technology – Security techniques – Guidelines for information security management systems auditing".

International Standard ISO/IEC 27008-2011 "Information technology – Security techniques – Guidelines for auditors on information security management systems controls".

USA publication NIST SP 800 -53: Recommended Security Controls for Federal Information Systems and Organizations.

The Global Technology Audit Guides (GTAG) issued by the Institute of Internal Auditors which includes GTAG 15 "Information Security Governance" and GTAG 11 "Developing the Audit Plan". The whole collection constitutes a valuable source of guidance for both auditors and practitioners.

The Control Objectives for Information Technology (COBIT) issued by the Information Technology Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). Version 5 was issued in April 2012.

ISACA Auditing Guideline G40: Review of Security Management Practices (2002).

The Role of Security Breach Notifications in Improving Cyber Security

Steve Purser

Attended the universities of Bristol and East Anglia where he obtained a BSc. in Chemistry and a PhD in Chemical Physics respectively. He started work in 1985 in the area of software development, subsequently progressing to project management and consultancy roles. From 1993 to 2008, he occupied the role of Information Security Manager for a number of companies in the financial sector. He joined ENISA in December 2008 as Head of the Technical Department and is currently responsible for all operational activities of ENISA. Steve is co-founder of the 'Club de Securité des Systèmes Informatiques au Luxembourg' (CLUSSIL) and is currently the ENISA representative on the ISO SC 27 working group. He frequently publishes articles in the specialised press and is the author of 'A Practical Guide to Managing Information Security' (Artech House, 2004).

Resumo

O Papel das Notificações de Violação de Segurança na Melhoria da Cibersegurança

Neste artigo analisa-se como os procedimentos de Security Breach Notification (SBN) podem ser utilizados na melhoria da cibersegurança numa envolvente transfronteiriça. A ideia central assenta no pressuposto de que dados quantitativos são necessários para melhor se compreender as ameaças envolventes, ainda que se reconheça existirem fortes condicionantes que requerem a implementação de uma recolha estruturada de dados e uma análise cautelosa de tendências.

É feita uma distinção entre SBN e Data Breach Notification (DBN). Ambos os conceitos serão relevantes para os futuros desenvolvimentos de uma política de cibersegurança da União Europeia, sendo a sua implementação requererá a adoção de requisitos específicos e economicamente viáveis em ambos os processos. Por fim, serão descritas questões relacionadas com a implementação de tais processos num contexto transfronteiriço e transcomunitário.

Abstract

This article examines how Security Breach Notification (SBN) procedures can be used to improve cyber security in a cross-border environment. The central idea is that quantitative data is necessary in order to better understand the evolving threat environment, although there are some strong limitations on this statement and it is extremely important to implement the data collection in a structured way and to analyse any trends cautiously.

A distinction is made between SBN schemes and Data Breach Notification (DBN) schemes. Both schemes are likely to play a role in future EU policy developments relating to cyber security and implementations will need to take account of the specific requirements on both processes whilst remaining economically viable. Finally, issues related to implementing such schemes in a cross-border and cross-community environment will be presented.

Introduction

Breach notification schemes provide a mechanism for institutions and enterprises to notify the competent authorities and/or the individuals affected in case of a serious security-related incident. In this article, the distinction will be made between "Security Breach Notification schemes (SBN)" and "Data Breach Notification schemes (DBN)". An example of the former scheme would be Article 13a of the EU Telecommunications Framework Directive of 2009,[1] whereas Article 4 of the ePrivacy Directive[2] provides a good example of the latter.

In the past, companies have shown themselves to be reticent in publishing data about security incidents that they have experienced. This is largely due to the fear that such publication could result in reputational damage and have a consequent impact on the success of the enterprise or organisation. For this reason, actual data characterising security incidents within the European Union (EU) has been fragmented making it more difficult to identify certain underlying trends.

The main benefit of a wide reaching breach notification scheme in the EU would be the creation of a pool of data that could be used to predict such trends across borders and across communities. Other benefits include increased opportunities to learn from mistakes and more input into improving protection mechanisms, both of which should result from the increased transparency that breach notification procedures bring about.

The possibility of introducing such a scheme across the EU Member States is an opportunity for the EU. Seizing this opportunity would enable the creation of a new source of security data, managed by a neutral third party, which could considerably increase our understanding of the nature and impact of security events throughout the union.

The Importance and Limitations of Quantitative Data

The use of past data as a tool for predicting what will happen in the future is the cornerstone of the scientific method. Such a method is however based on the

1 Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive).

2 Directive 2002/58/EC on privacy and electronic communications.

assumption that the data that is being collected is subject to some form of governing law or principle that can be captured and then used to predict how similar data will look in the future. Whilst experience has shown that such modelling techniques can usefully be applied to issues that are well-understood (such as proliferation of malicious code), they are in general not helpful in predicting the so-called "low-probability, high-impact events" (also called 'Black Swan events'). Unfortunately, such events tend to be extremely significant where information security is concerned.[3]

Another issue associated with the use of quantitative data is the degree of precision to which the data describes the event of interest. A virus infection could result on the one hand in nothing more serious than a ball bouncing across the screen, which is annoying but not critical, to the (stealthy) gradual destruction of data over a long period of time, which would often be catastrophic as it would infiltrate backup tapes and result in an unrecoverable situation. If the data being captured takes no account of the impact, this does not necessarily provide a lot of information on the nature of the breach.

Despite these limitations, it is clear that better data on security incidents would increase our understanding of what has happened to date and offer some degree of predictive power over how things are likely to evolve in the near future. Such data is also useful in understanding how well traditional response mechanisms coped with particular types of incidents and where such mechanisms broke down when an attack was successful. The key to getting the most out of security breach data is to understand the limitations in its predictive power and to concentrate on those trends that can be quantified and predicted.

Key Elements of Breach Notification Schemes

In the opinion of the author, breach notification schemes should provide clear descriptions of all the following points:

- Objectives and outcomes.
- Trigger conditions.
- Definition of content and data formatting rules.
- Roles and responsibilities for all actors.
- Documented procedural steps with associated timing constraints.
- Rules for handling sensitive data (including private data)

3 An example might be *stuxnet*, which was significant because of the change of target (and hence possible impact) and represented an important change in the way in which malware was being used.

- Data lifecycle management rules.
- Adequate awareness training requirements.

Defining clear objectives and outcomes is the most fundamental requirement of a breach notification scheme, as it is these which provide the justification for defining a scheme in the first place. Furthermore, breach notification schemes should be evaluated on their ability to meet the defined objectives.

Conditions according to which breach notification procedures are triggered should be simple and unambiguous. Unfortunately, the more heterogeneous the environment to which the requirement applies, the more difficult it will be to achieve this in practice. For instance, different communities are likely to have different ideas on thresholds and how to define different severity levels.

The definition of content and suitable formatting rules is essential to ensure that the correct information is collected and that it is comparable across the contributing communities.

The need for clear roles and responsibilities, well defined procedures and timing constraints is not of course particular to breach notification, but the absence of any of these elements could result in procedures that are sub-optimal or (in extreme cases) ineffective.

Any breach notification scheme should clearly define how sensitive data (and notably private data) is to be handled. In particular, every effort should be made to ensure that the breach notification scheme cannot be itself the origin of a further breach. This kind of consideration is likely to be important where the data is provided at different levels of granularity to different audiences.

Data lifecycle management rules should clearly state under what conditions data is stored and processed, how long it is retained and when and how it will be destroyed. Backup and archiving procedures are also important in this area.

Finally, it is critical that all actors understand their role (and that of other actors) in the overall process. This will certainly require training on a regular basis and it would be prudent to include an outline o0f the requirements in this area in the definition of the scheme itself.

European Union Policy Developments

At the time of writing, European Network and Information Security Agency (ENISA) is assisting the Commission and the Member States in the implementation of two breach notification schemes.

The EU Telecommunications Framework Directive of 2009 included the addition of Article 13a, regarding security and integrity of public electronic communication networks and services. This Article states the following:

- Providers of public communication networks and services should take measures to guarantee security and integrity (i.e. availability) of their networks.
- Providers must report to competent national authorities about significant security breaches.
- National authorities should inform ENISA and authorities abroad when necessary, for example in case of incidents with impact across borders.
- National authorities should report to ENISA and the EC about the incident reports annually.

The Commission, ENISA, and the National Regulatory Authorities (NRA) have jointly proposed a single set of security measures for the European electronic communications sector and a modality for reporting security breaches in the electronic communications sector to authorities abroad, to ENISA and the EC. In May 2012 ENISA received the first set of annual reports from Member States, covering incidents that occurred in 2011. These reports covered 51 large incidents and describe services affected, number of users affected, duration, root causes, actions taken and lessons learnt.

Article 4 of the e-Privacy Directive addresses data protection and privacy related to the provision of public electronic communication networks or services. This is a Data Breach Notification article that requires providers to notify personal data breaches to the competent authority and subscribers or individuals concerned, without undue delay. The obligations for providers are:

- To take appropriate technical and organisational measures to ensure security of services;
- To notify personal data breaches to the competent national authority;
- To notify data breaches to the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy, and;
- To keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

Throughout 2011 and 2012, ENISA has been working with expert groups, national data protection authorities, industry, and the EDPS, to draft recommendations for the technical implementation of Article 4.

In general, it is likely that the EU will continue to promote breach notification schemes and it is highly likely that such schemes will be designed to be not only cross-border but cross-sector in their scope.

One of the more interesting challenges in this area is to ensure that breach notification schemes are implemented in an economically efficient manner. Thus, although SBN and DBN have different goals and are covered by different legislative instruments, it is clear that the procedures for implementing these schemes in real operational environments will have a lot in common. Implementation

schemes should therefore concentrate on achieving synergies and avoid duplication of effort.

Implementation Issues

In its capacity as a centre of competence in the area of Network and Information Security (NIS), the ENISA is particularly well placed to assist the Commission and the EU Member States in the implementation of policy and legislation in this area. In particular, as any widespread breach notification scheme is likely to involve both public and private sector organisations, the implementation of such a scheme will require aligning objectives and procedures across the two communities in addition to ensuring a coherent approach in a cross-border environment. This is entirely compatible with ENISA's role of creating effective stakeholder communities to improve the level of information security across the EU.

There are however many challenges in implementing breach notification schemes in such a cross-border, cross-community environment. These include, but are not limited to:

- Difficulties in collecting and comparing data from different sources.
- Cross-border and cross community effects.
- Agreeing suitable thresholds.
- Preventing the identification of individual entities through data aggregation and anonymisation – inference techniques.
- Data protection and privacy issues.
- Problem of scalability in security – orders of magnitude.

The issue of collecting and comparing data is easy to understand – if incident data is to be collected from a variety of different environments, it is likely that the syntax and semantics will be different from environment to environment It is therefore essential to define and implement standards that allow data to from different sources to be compared.

Whereas the issue of structure is easy to understand, other cross-border and cross-community effects may be much more difficult to pin down and might manifest themselves in factors such as interpretation or significance of the data. Whilst agreeing on suitable thresholds could provide an answer to some of these concerns, it is unlikely to resolve all such issues.

If only aggregated data is to be published to a wider public, there may be a risk of employing techniques based on inference in order to link particular incidents to particular enterprises or organisations for some of the smaller Member States. Such Member States may well require more advanced data handling techniques in order to hide such relationships.

The issue of data protection and privacy is common to all Member States of course and is at the very core of the Data Breach Notification schemes. In this context, the challenge will be to define procedures for handling breach notifications that do not in themselves put personal data at risk.

Last but not least, it is clear that breach notification schemes will need to be inherently scalable if they are to stand the test of time. This is most easily illustrated by considering mergers and acquisitions, where the number of incidents that occur may grow drastically in a very short period of time.

Towards Multi-national Capability Development in Cyber Defence

Frederic Jordan

Started his career in 1996 with an Aerospace Engineer degree and a Master's degree in Computer Science. He then worked as an Information Security Engineer in the French Ministry of Defence before he joined the NATO C3 Agency in 2005. Since then his responsibilities have progressively evolved from scientific and technical activities to project and team management. He is now the Project Manager for most of the NCI Agency Cyber Defence scientific and technical projects. He is also the Project Manager for the Bi-SC AIS IDS acquisition project which provides the NATO Military Command sub-structure with Host based Intrusion Detection capability.

Geir Hallingstad

Received his B.Sc. and M.Sc. in computer engineering from Iowa State University in 1996 and 1997, respectively. He has over 10 years of experience working with information security in military systems and is currently working as a principal scientist at the NCI Agency. His work area includes networked systems that provide both secure and flexible communications in support of an network enabled capability (NEC) operational environment, and the establishment of cyber defence and its various components as a fundamental capability in providing cyber security and information assurance.

Agata Szydelko

Received Master's degree in Management and Marketing at Wroclaw University of Economics. As Principal Business Manager she is responsible for the strategic planning, cooperation development and business assurance of Multinational cooperation with the Nations and Organizations in the area of C4ISR. Her professional experience as NCIA Senior Contracting Officer includes the execution of high-volume NATO C4ISR acquisitions, also in support of NATO operations in Afghanistan and the Balkans. Moreover, as International Business Manager for national industry she was in charge of the supply of IT systems to commercial and military customers.

Resumo

Para o Desenvolvimento de uma Capacidade Multinacional de Ciberdefesa

Este artigo apresenta uma abordagem de desenvolvimento de uma capacidade multinacional de ciberdefesa que tem sido discutida entre vários países da NATO e a NATO Communications and Information Agency, inserida no contexto da NATO Smart Defence. Existem ganhos potenciais se se alavancarem requisitos e recursos comuns, quando as capacidades existentes entre os vários países são variáveis e o financiamento destinado os desenvolvimento das mesmas é escasso, sendo que se apontam alguns dos fundamentos justificativos para esta cooperação multinacional.

Abstract

This article presents a multi-national cyber defence capability development approach discussed between several NATO Nations and the NATO Communications and Information Agency in the context of NATO Smart Defence. There is potential gain from leveraging common requirements and resources when the levels of nation capabilities in this area vary and funding to develop the capabilities is scarce. The article will address some of the fundamentals for multi-national cooperation.

Introduction[1]

NATO and NATO Nations are heavily dependent on communication and information systems (CIS), which, to varying degrees, are vulnerable to threats from different adversaries through their network connections and also from access by authorized and/or unauthorized insiders. A disruption or an intrusion into a CIS could seriously harm the functions of the Alliance, especially if it affects NATO or the NATO Nations' classified networks. Even if unauthorized access to the secure networks is successfully denied, cyber-attacks on critical infrastructure could degrade the functioning of national security, law and order, and lead to disturbances and losses in economic systems.

Cyber defence is the application of security measures to protect against, and react to cyber-attacks against communications and command systems infrastructure. It requires capabilities to prepare for, prevent, detect, respond to, recover from, and learn lessons from attacks that could affect the confidentiality, integrity and availability of information as well as supporting system services and resources.

However, establishing an effective cyber defence capability is a new and major endeavour. Many nations have just started to consider cyber defence as a significant defence capability. Building a cyber defence capability also represents a high level of technical complexity, many procedural challenges, as well as an urgent requirement which makes the implementation even more challenging.

This article presents a multi-national cyber defence capability development approach currently being discussed between an open group of NATO Nations and the NATO Communications and Information Agency (NCI Agency). The potential gain from leveraging common requirements and resources is high, as NATO and the NATO Nations have varying levels of capabilities in this area and limited funding to develop the capabilities. The article will address some of the fundamentals for multi-national cooperation, as well as some of the cyber defence topics with high probability for immediate success.

1 This article is an update of the one published in the special issue of the *Information & Security* journal on C4ISR support to the Comprehensive Approach. Frederic Jordan and Geir Hallingstad (2011). "Towards Multi-National Capability Development in Cyber Defence". *Information & Security* n. º 27, pp. 81-90. Available at http://www.procon.bg/node/2469.

Background

The analysis and recommendations of the group of experts on a new strategic concept for NATO (Albright, 2010) highlighted that "NATO must accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence." The new strategic concept (NATO, 2010), approved by the heads of state at the Lisbon summit in November 2010, highlights the new threats and emerging security challenges as one of the key aspects to address in order to keep the Alliance effective. The further development of the cyber defence capability is listed as necessary to ensure the safety and security of the population. Furthermore, it is stated that cyber defence shall be included in the NATO defence planning process to enhance and coordinate NATO and national cyber defence capabilities. Another section of the strategic concept recognizes the need to "develop and operate capabilities jointly for reasons of cost effectiveness and as a manifestation of solidarity", pointing to the need for multi-national cooperation.

Following this direction, the Defence Ministers adopted in June 2011 the revised NATO Policy on Cyber Defence which sets out a clear vision on NATO's efforts in cyber defence throughout the Alliance and also establishes the principles for NATO's cyber defence cooperation with partner countries, international organizations, the private sector, and academia. Allies are also encouraged to work more closely with their national defence industrial leaders to pursue collaborative and multinational projects wherever possible, and to seek out opportunities for consolidations and mergers to develop cyber defence capabilities.

A major element of the NATO Cyber Defence is the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC) project, which will provide not only a technology refresh of the existing NCIRC IOC capability but will also introduce new technologies to improve cyber defence situational awareness and enhance NATO's ability to respond to evolving cyber-threats.

Once the NATO CIRC FOC capability is in place the NCI Agency will establish the appropriate mechanisms to enable the nations to acquire the associated tools and services for national use.

The NATO Secretary General's original call for Smart Defence in February 2011 (Rasmussen, 2011) at the Munich Security Conference has been repeatedly reiterated in numerous addressees and forums. The Chicago Summit declaration of 20 May 2012 – "Toward NATO Forces 2020" (NATO, 2012) – clearly confirmed that Smart Defence is at the heart of the new approach towards NATO retaining and developing the capabilities necessary to perform its essential core tasks of collective defence, crisis management, and cooperative security. The political direction

is clear both with respect to the significance of establishing a solid, comprehensive cyber defence capability, and to the importance of cooperation between nations to be cost-effective and efficient in order to be able to quickly share information about cyber incidents, to rapidly react to cyber threats and attacks against Alliance CIS.

Establishing Multi-national Capability Development

The objective of a multinational cyber defence capability development (MNCD2) programme is to facilitate the development of cyber defence capabilities in the nations and NATO through a collaborative effort. It provides a vehicle for the nations to focus their efforts in areas of their choice, and within any monetary constraints, while maintaining an overall approach and achieving a well-balanced cyber defence capability.

This programme is established with a management structure executing the primary coordination and interface activities required to align the various national and NATO efforts. This includes coordination of all facets of capability development including research, design and engineering, testing and experimentation, verification, procurement preparation, and procurement. In addition, the programme ensures interoperability through validation and/or certification of the capabilities and in particular the interoperability interfaces.

NATO already facilitates coordinated research through the Science and Technology Organisation (S&TO), which covers a wide spectrum of activities. Each nation usually participates in technical activities based on own funding in already established national projects. This structure, therefore, primarily helps to coordinate on-going projects. This is sometimes problematic as nations may have different objectives, and when participating in activities over time, the individual national objectives may change and make cooperation and coordination more difficult. Furthermore, the S&TO activities are limited to research and do not include any other components of capability development.

Within NATO, there is currently no programme for nations to establish a viable cyber defence capability. The defence planning process is there to help establish the capability requirements across the nations and the S&TO can facilitate research coordination. However, there is no multi-national approach in NATO that will ensure pull-through from requirements analysis, over prioritization and research, to acquisition and final implementation.

To reap full benefit of the common interests in achieving cyber defence capabilities, a greater effort is required to align national activities in addition to coordination. This requires a dedicated structure to continually monitor national requirements and efforts and to coordinate and strategize on the way forward so as

to ensure that there is no dispersion of efforts and that the tempo of research and development activities is in line with the assessment of the risks against NATO and national CIS. Establishing this structure and facilitating the coordinated development of cyber defence capabilities is the purpose of the MNCD2 programme.

However, joint plans are often difficult to establish due to the lack of a common reference framework and terminology that one can use as a foundation for coordinated capability development. Likewise, there are no metrics defined so as to assess how much of a given specific cyber defence capability is needed within NATO (or nationally), which could potentially lead to inefficient use of scarce resources.

Advantages of Multinational Effort

There are several benefits from a multi-national effort in developing cyber defence capabilities. First, there is a potential for cost-savings through joint research, development, and specification of a given capability. In addition to cost savings, the quality of the result will likely be better since the effort has more diverse exposure. Furthermore, there is potential cost savings in joint procurement due to economies of scale, and even with individual procurement in a nation, the cost is reduced due to the ability to use the common procurement requirements. Finally, a capability developed in this way is, by default, "born interoperable" and potentially saving significant investments in the long term, rather than the often used ad-hoc and most of the time costly solutions that provide limited functionality.

Collaboration Climate

While the advantages argued for any multinational efforts remain nearly the same for any multinational project – interoperability, economies of scale, optimized collaboration and more efficient use of the resources it is remarkable that in an area considered to be of great sensitivity and with significant security concerns the nations are willing to open up and work together, seeing more pros than cons for joining up the collaborative environment. Economic crisis? Maybe, although if this was the case the multinational collaboration projects would have been flourishing all over the place, which does not seem to be the case. What then? The most likely explanation is that the overwhelming pressure coming from around the globe and the cross-borders nature of computer networks pushed the nations to reconsider the limits of their own sovereignty for the benefit of enhancing the collaborative security, probably marking a new era in multinational collaboration and once again in human history pushing the limits of sharing.

Framework for Cyber Defence Capabilities

In order to aid in cyber defence capability development, Allied Command Transformation (ACT) and the NCI Agency have initiated the development of a cyber defence capability framework (Hallingstad and Dandurand, n.d). This document aims to clarify the scope of cyber defence, establish a common taxonomy, provide a foundation for multi-national capability development, and identify interoperability interfaces for cyber defence to enable federated cyber defence.

The capability framework contains a hierarchical breakdown of the cyber defence capability, meaning that each capability is broken down into manageable components and gives a structured way to determine what NATO and the nations are working on, and which capabilities need to be addressed further. The first level cyber defence capabilities identified in the capability framework are:

- Malicious activity detection;
- Attack termination/prevention/mitigation;
- Dynamic risk, damage and attack assessment;
- Cyber-attack recovery;
- Timely decision making;
- Situational awareness visualization;
- Cyber defence information management.

While many of the capabilities listed above have been a subject of research over the last few decades, others are immature. In order to efficiently progress towards these capabilities, the various NATO and national efforts must be coordinated. The capability breakdown is central in this effort with its terminology and structured breakdown.

The framework currently consists of capability definitions only. However, one can achieve a capability in several different ways, and the same capability can vary in its efficiency and ability. Therefore, a natural extension to the capability definition would be a maturity model that would describe levels of a capability. For example, the ability to detect a malicious cyber attack can take days or seconds while still being the same capability. However, the ability to detect in real-time is clearly a more mature capability and needs to be expressed.

A natural accompaniment to a maturity model is measurements and metrics to evaluate the capability. This is important to define in order to evaluate the overall capability, both to establish that the desired effect is being achieved, and to establish the maturity level of the capability for the purpose of defence planning and interoperability in multi-national scenarios.

Topics for MNCD2

Through an analysis of existing capabilities and needs, the following three areas have been identified as initial targets for a multinational capability development initiative: (1) cyber defence information sharing; (2) cyber situational awareness; and (3) a distributed multi-sensor collection and correlation capability.

Cyber Defence Information Sharing Capability

The first topic, the development of a *cyber defence information sharing* capability, will enable efficient exchange of cyber defence information such as incident information, attack signatures, and threat assessments, between national Computer Emergency Response Teams (CERTs) including the NCIRC.

The activities needed to put this capability in place include a determination of the type and format of the information to be exchanged, completing an interface specification, design of the infrastructure for sharing, writing procurement requirements, the actual procurement, and a test and validation of the delivered equipment. In addition, there may be a need for training and education of staff in the use of the system, and there will likely be a need to translate some formats from the existing CERTs' systems to meet the interface specification and allow interoperability with the other CERTs.

The determination of the requirements for information to be exchanged and the data format will leverage the lessons learned from the annual NATO Cyber Coalition exercise as well as the Coalition Network Defence Common Operational Picture work conducted in an S&TO working group (IST-081-RTG-039).

For the infrastructure design, the communication infrastructure requirements will be thoroughly assessed so as to determine the elements required at the National CERTs, the elements required at the NCIRC as well the available transport networks, for, at least, each of the three main NATO security domains (NATO Unclassified, NATO Restricted and NATO Secret).

Procurement could be done individually in a nation, jointly, or any combination of the two. In the case of multiple procurements in different nations, there would be a clear need for a testing and validation effort since different systems will need to interoperate.

Once this initial Cyber Defence information sharing capability is in place, other issues of importance could be addressed. For example, there is currently no standard approach for the direct integration of data into Cyber Defence applications. As well, there is no agreed framework or standard to facilitate collaboration between Nations and NATO on the dynamic generation, refine-

ment and vetting of cyber security data. For these reasons, the NCI Agency has started investigating under the ACT cyber defence research and development programme (R&D POW) the concept and requirements for a Cyber Defence Collaboration and Exchange Infrastructure (CDXI). The CDXI addresses syntactic and semantic interoperability between different communities of interest that nevertheless wish to exchange Cyber Defence data, while avoiding the pitfall of supporting only a single ontology. In particular, it uses pure enumerations and independent topic ontologies as a mean to provide an agile and decentralized data model.

To understand the CDXI, it is best to see it primarily as a software library to be used in the development of Cyber Defence applications. While it will have its own set of user interfaces, these will be intended primarily for the management of the core infrastructure and its data. The exchange of information in operational scenarios and the automation of Cyber Defence will be through various applications developed by industry and organisations that use the "CDXI software library" to manipulate the required Cyber Defence data for those purposes. Whether or not these applications will expose the full range of services offered by the CDXI through their own user interfaces will depend on each application's purpose, their intended user community and the products' specific goals.

Cyber Situational Awareness

The second topic under consideration is the development of a capability to improve *cyber situational awareness*. For most NATO Nations, operational cyber defence is performed using a variety of tools and products including Intrusion Detection System (IDS) and other sensors, Security Incident and Event Managers (SIEM), vulnerability databases, and network monitoring software. These tools typically operate individually and there is no overall view. Cyber defence situational awareness is, therefore, achieved by experts manually consulting and consolidating a variety of feeds. Significant competency and a lot of manual effort are required.

Due to the complexity and the vastness of information provided by these feeds, an efficient and accurate visualization capability is required to provide relevant and clear situation perception that supports a timely decision making process. It is necessary to generate specialized views for humans to be able to understand what is happening and derive knowledge from all this information.

From a capability definition perspective, visualization represents activities in the CIS, as well as the CIS components, the objectives and their priorities, the threats, discovered vulnerabilities and reference security information from vari-

ous sources. In addition, the visualization needs to show projected actions based on the events and context and present these to the users with the potential impact. The visualization should address the needs of different user roles at different command or management levels, including the ability to alert, highlight, filter, and drill-down for additional detail as necessary, in a customizable fashion.

The joint development of this capability would simplify and enable quick decision making in the cyber domain, especially in a coalition environment, by providing a flexible set of visual interfaces (*e.g.* dashboards, dynamic views, and reporting features). It would leverage work conducted under the ACT R&D POW on the Consolidated Information Assurance Picture (CIAP) which provides a set of specifications of various flexible views using information contained in the NATO Consolidated Security Information Repository (CSIR) and to be implemented by the NCIRC Full Operational Capability (FOC).

Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI)

Attacks on CIS infrastructures are increasingly sophisticated and increasingly successful. In particular the Advanced Persistent Threats (APT) has grown in importance and can no longer be dismissed as marginal events. This has led to efforts to fundamentally rethink the defensive strategy. For example, DARPA has started several projects under its CRASH program (Clean-slate design of Resilient Adaptive Secure Hosts) that aim to fundamentally redesign CIS systems with security as a main requirement. The main aim of the Distributed Multi-source Collection and Correlation Infrastructure (DMCCI) investigated under the ACT R&D POW is to define an open architecture that overcomes the limitations of the current protection and detection mechanisms in order to increase network situational awareness and facilitate the detection of advanced and stealth attacks.

At its core the DMCCI capability provides the means to coherently collect and correlate data from multiple sensors in an efficient and distributed manner so as to enable flexible management of sensor data storage and run a variety of correlation algorithms against the collected data.

In effect, DMCCI enables the rapid, seamless and continuous introduction of complex, multi-source detection algorithms that can correlate data from various sources not only newly arriving data but also on previously stored data, including events, network flows and metadata. It also supports and streamlines the post intrusion analysis and damage assessment processes while addressing constraints imposed by the geographic distribution of the components of a CIS as well as the bandwidth limitations of its communications links.

One use case of how DMCCI could facilitate post intrusion analysis and damage assessment is when malicious software and malicious network traffic is detected in an organization's CIS. The organization then usually generates or exploits a security bulletin which contains the signatures or traces of the attack. The signatures are then deployed through-out NATO networks allowing anti-virus software to detect *new* compromises using this malware. However, attackers are likely to remove these traces on machines that have already been compromised. An analysis of different APT attacks shows that attackers often use the initial malicious software only to exploit a software vulnerability on a host and then install a different piece of malicious software to remotely control the machine. So the question is now, which hosts in the organization's network have *in the past* received any of the signatures associated to the attack. Anti-virus software cannot answer this question as it did not previously have the signatures of the newly discovered files. All these hosts need to be analysed for signs of compromise. And the follow up question is, with which hosts have these potentially compromised hosts communicated, as the attackers may have used the compromised hosts as a pivoting point (stepping stone) to move laterally to other parts of the organization's networks.

DMCCI would allow an analyst to answer these questions by running queries over correlated data from collected from network, DNS servers and proxy servers, without the need of a manual investigation of each of these systems. The analyst can then focus the manual effort on forensic investigation of affected hosts. In addition, DMCCI will allow the analyst to use findings from his investigations to write advanced algorithms that will detect similar attacks and shorten the delay between the time of attack and time of detection. The goal is to be able to apply new rule sets and detection algorithms not only upon new flows and events but also upon past flows and events. DMCCI could also be used to address many of the capabilities related to situational awareness within the cyber defence capability framework.

Cyber Defence Experimentation and Validation Capability

A key element of joint capability development is an experimentation and validation infrastructure that would ensure that new cyber defence capabilities are validated and interoperable as required. For this reason, the NATO cyber defence capability framework has to be complemented by a structure that would allow NATO and NATO Nations to experiment new technologies, technical/operational concepts and procedures and to test cyber defence standards against a reference.

From experience gained in other technical areas, the vision would be to establish a federated and shared experimentation and validation infrastructure which would possibly borrow concepts from other federated capabilities like the Distributed Networked Battle Labs (DNBL) Framework.

By defining the necessary trust and technical environment allowing the federation of existing efforts, this capability would have the potential to contribute to a better and accelerated development of cyber defence and cyber security capabilities in a cost effective manner

NATO C&I Agency Role in Multinational Development

The NCI Agency is part of the NATO Communications and Information Organisation (NCIO), along with the Agency Supervisory Board and supports the mission of the NCIO through unbiased and independent advice in the C4ISR area. The NCI Agency consists primarily of NATO employed personnel in order to be independent of industry and national bias, including among others scientists as well as procurements specialists. The NCI Agency is authorized by its Charter to provide technical advice and support to customers who are either NATO bodies or Nations.

The legal framework to be used for the establishment of the MN CD2 is a multilateral Memorandum of Understanding (MOU). The primary focus of the MN CD2 MOU is to establish the multinational project governance and management framework as well as to facilitate the execution of the multi-year programme of work across the three proposed Work Packages. The MOU will be supplemented by Task Orders detailing the exact scope and execution of the respective Work Packages. One of the advanced features of this MOU is the opportunity for inclusions of Contributions in Kind offered by any of the participating nations in the execution of the project. Currently the MN CD2 is open for participation to all the NATO nations.

Under the MN CD2 legal umbrella the NCI Agency will act as a multi-national executive coordination agent in support of capability development in cyber defence, from running project office to any area covered under the technical framework. The support will span from research contributions and correlation to procedure design and engineering and procurement. In this role, the NCI Agency will also facilitate the discussion with the cyber defence operational community about the definition and establishment of maturity levels for the technical elements under investigation so as to provide prioritization and guidance for implementation.

MN CD2 and Smart Defence

A big step forward in the establishment of the MN CD2 project was the decision by Canada in June 2012 to take on the Lead Nation role for this project as well as its inclusion in the NATO Smart Defence Multinational Projects database. This further reconfirms the nations' will for the project establishment and provides greater project visibility and alignment with the NATO Defence Planning Process.

Conclusion

The political guidance regarding cyber defence is to continue to develop the capability, and that the overall alliance cyber defence capability needs to be considered through the NATO defence planning process. In addition, technical capabilities should be developed jointly in order to be as efficient as possible.

Securing cyberspace is a complicated issue and, in particular, implementing effective interoperable cyber defence capabilities is a major endeavour with many technical, procedural and political challenges. NATO and NATO Nations are currently at various stages of implementation for such capabilities and are now challenged to develop the tools and mechanisms that will allow them to optimize their resources and exploit all possible synergies. A multi-national cyber defence capability development programme will help NATO and NATO Nations and deliver benefits to all participants by providing support, coordination, and coherency in the area of cyber defence capability development.

The NCI Agency is well positioned to support this effort through its charter and its mix of unbiased personnel including scientists and procurement specialists. In addition, the existing legal agreements between the NCI Agency and a number of nations can be used to accelerate and ease the setup of such an initiative.

A multi-national cyber defence capability development will meet the political guidance as agreed in the new strategic concept and the subsequent cyber defence concept and policy. More importantly, it will contribute to a significant improvement in defence against the continually increasing threat of cyber attacks across the alliance and therefore contribute to the overall security of the alliance. Finally, it's coming right on time for the nations to take advantage of collaborative rather than individual efforts in one of the most crucial areas for the stability and prosperity of our world.

References

Albright, Madeleine K. (2010). *NATO 2020: Assured Security, Dynamic Engagement – Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*. Brussels, 17 May.

Hallingstad, Geir, Luc Dandurand (n.d.). Cyber Defence Capability Framework – Revision 3"(NATO C3 Agency Reference Document RD-3060). The Hague.

Jordan, Frederic, Geir Hallingstad (2011). "Towards Multi-National Capability Development in Cyber Defence", *Information & Security* n.º 27, pp. 81-90. http://www.procon.bg/node/2469

NATO (North Atlantic Council) (2010). "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation". Lisbon, November.

NATO (2012). "Chicago Summit Declaration on Defence Capabilities: Toward NATO Forces 2020". 20 May. Available at http://www.nato.int/cps/en/SID-EE03881B-D6E19CED/natolive/official_texts_87594.htm

Rasmussen, Anders Fogh (2011). "Building Security in an Age of Austerity". Keynote speech by NATO Secretary General Anders Fogh Rasmussen at the 2011 Munich Security Conference. Available at http://www.nato.int/cps/en/natolive/opinions_70400.htm.

Preservação Digital

Francisco Barbedo

Licenciado em História (arte e arqueologia), pós graduado em ciências documentais (opção arquivo), e mestre em gestão de informação. Foi subdiretor da Direção Geral de Arquivos entre 2007 e 2012. É presentemente diretor de serviços na área de inovação e administração eletrónica, na Direção Geral do Livro, dos Arquivos e das Bibliotecas.

Sílvia Saraiva Carvalho Martins

Mestre em Engenharia Eletrónica e Telecomunicações pela Universidade de Aveiro, Especialista de Informática no Instituto de Segurança Social desde 1999, tendo desempenhado cargos de chefia e direção desde 2005. Auditora do Curso de Defesa Nacional 2009.

Resumo

As sociedades atuais estão completamente suportadas e dependentes das Tecnologias de Informação, documentos e conteúdos digitais. Tudo aparentemente à distância de um simples clique, porém, para que se tenha acesso à informação digital é sempre necessário utilizar um interlocutor (hardware e software), que fruto da sua evolução exponencial rapidamente se torna obsoleto. Acontece, que quando se fala em objetos e documentos digitais só se preservarão os que se conservarem, tudo o resto se perderá. São aliás conhecidos casos de formatos, suporte e software que foram descontinuados, sem que hoje seja possível recuperar essa informação.

As instituições sejam do setor público ou privado, parecem ainda não ter acordado para esta realidade que pode por em causa o seu normal e bom funcionamento. É pois pertinente que se salvaguarde informação crítica para as organizações, pessoas e sociedade em geral e, esteja disponível, autêntica, fidedigna, utilizável e com caráter evidencial durante o período de tempo que dela se necessite. É importante que a nível nacional se tome consciência desta problemática sob pena de se perder irrecuperavelmente informação, ciando uma política de preservação digital.

Abstract
Digital Preservation

Currently our society fully relies on ITC and digital content. However digital information is also dependent of an intermediary system, which is basically the software and hardware used to produce the information in the first place. The dynamism of the information technology industry quickly turns this intermediary system obsolete, creating dramatic problems to the retrieval and preservation of information on the medium and long terms. If no preservation actions are considered, digital information will become unreadable and therefore will be lost.

Institutions, both public and private, seem to have problems grasping this reality that can indeed jeopardize their regular activities. In order to achieve it several measures are necessary: one of them consist on the development of digital preservation plans that may help organizations to identify their digital information assets and prescribe the best strategies to preserve them. Is of utmost importance to acquire conscience of this problem and what exactly is at stake in order to develop a national level policy for information that includes its preservation

A crescente dependência das tecnologias de informação, atualmente o principal suporte para a produção e armazenamento de informação, a par da rápida taxa de obsolescência tecnológica característica da indústria informática, levantam às organizações problemas críticos de preservação de informação digital. Esta tem de ser mantida durante o tempo que for operacionalmente necessária, ou seja, enquanto a organização necessitar de dispor dessa informação por razões de execução da sua missão e para o exercício das suas atividades.

O tempo durante o qual é necessário guardar a informação é variável pois depende, ou deveria depender, de critérios estabelecidos com o máximo possível de objetividade, relacionados com necessidades de caráter administrativo e operacional e também com razões de caráter histórico e social.

Nem toda a informação é idêntica, ou tem propósitos funcionais similares. Assim o período de conservação dessa informação irá mudar em função de variáveis que têm de ser analisadas, tendo como objetivos:

- Guardar de forma autêntica e acessível a informação durante os períodos de tempo que a organização estime como necessários;
- Eliminar a informação assim que ela deixa de ser necessária à organização (pois a sua preservação implica elevados custos);
- Assegurar que a informação com interesse histórico e social é identificada e preservada;
- Otimizar os custos necessários para manter uma infraestrutura capaz de assegurar a preservação e utilização da informação digital.

De entre as várias razões acima indicadas para a realização desta análise discriminativa, chama-se a atenção para o elevado e permanente custo exigido para preservar informação digital de forma autêntica, e acessível ao longo do tempo.

Informação Digital

A era digital trouxe consigo a produção exponencial de informação. Há quem afirme que se produziu mais informação nos últimos anos do que em toda a história conhecida da humanidade. Saliente-se que a informação digital tem como principais vantagens a sua fácil criação, manipulação, acesso, partilha, disseminação, duplicação e transmissão e como principal desvantagem a sua volatilidade inerente à sua dependência da tecnologia, que rapidamente se torna obsoleta.

Importa também referir neste contexto, o conceito de objeto digital que se define como "todo e qualquer objeto de informação que possa ser representado através de uma sequência de dígitos binários" (Ferreira, 2006). São exemplos de objetos digitais: texto, som, vídeo, radiografias, fotografias, bases de dados, aplicações de *software*, páginas *Web*, modelos de realidade virtual, etc.. Um único objeto digital pode ser constituído por vários tipos de informação, contendo capacidades dinâmicas e interativas.

A distinção entre formato e suporte torna-se evidente, o mesmo documento pode ser representado ou reproduzido em suportes diferentes. Assim como, o mesmo objeto digital pode ser representado em formatos diferentes.

Preservação Digital

Atualmente, a informação toma um valor singular, aparentemente sempre disponível e fácil de aceder, à distância de um clique, sem que o seu utilizador final tenha consciência da sua localização ou da necessidade da sua disponibilidade ao longo do tempo. A forma fácil e confortável como toda a informação de que se depende no quotidiano tem sido rapidamente transferida para *bits* e *bytes* é espantosa e assustadora, assim como é espantosa a forma como as infraestruturas críticas estão assentes e dependentes desta tecnologia.

Acontece que este mundo espantoso tem a particularidade de a informação só estar acessível e poder ser lida através de um interlocutor tecnológico com características específicas, leia-se *software* e *hardware*. As Tecnologias da Informação e Comunicação (TIC), como são denominadas, evoluem exponencialmente ficando rapidamente obsoletas, não sendo invulgar alguma informação crítica ficar refém de formatos e suportes que entretanto foram descontinuados.

A obsolescência é portanto o fator crítico e determinante na preservação, autenticação e arquivo digital, tanto mais que o ciclo de vida de um formato/suporte digital está estimado de 5 a 7 anos, e a informação a preservar será a de conservação de médio prazo (10 anos) e longo prazo (mais de 10 anos), classificada como de preservação permanente.

É importante que se salvaguarde informação crítica para as organizações, pessoas e sociedade em geral e, esteja disponível, autêntica, fidedigna, utilizável e com caráter evidencial durante o período de tempo que dela se necessite.

O objetivo da preservação digital é garantir a acessibilidade sustentada e fiável à informação. Como definição, "a preservação digital consiste na capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação." (Ferreira, 2006).

Estratégias de Preservação Digital

Acompanhando a evolução tecnológica foram desenvolvidos dois tipos de estratégias de preservação digital: as de preservação tecnológica, centradas no objeto físico/lógico e as de preservação de informação centrada no objeto conceptual. O primeiro preserva a informação nos seus formatos físicos e/ou lógicos originais, utilizando a tecnologia inicialmente associada aos objetos digitais, garantindo-lhes assim o acesso. O segundo tipo está focado na preservação das características essenciais dos objetos digitais, sendo independente do *software* ou *hardware* utilizado (Ferreira, 2008).

As estratégias de preservação digital são a emulação, a migração e o encapsulamento. A emulação consiste na utilização de um *software* capaz de reproduzir o comportamento de uma determinada plataforma de *hardware* e/ou *software* numa outra que, à partida, seria incompatível. Este *software* tem o nome de emulador (Ferreira, 2006). É uma estratégia utilizada em objetos digitais com características dinâmicas e/ou interativas como aplicações de *software*, animações *flash*, por exemplo o antigo Windows, ou jogos do antigo Spectrum. A sua vantagem é a capacidade de preservar com grande fidelidade as características e funcionalidades originais do objeto. A grande desvantagem é o facto dos próprios emuladores se tornarem obsoletos.

A migração converte objetos digitais de determinado formato *hardware* e/ou *software* para outro mais recente. É uma estratégia utilizada em objetos digitais com características não dinâmicas como documentos de texto, imagens e base de dados que se divide em vários tipos: retro-compatibilidade, interoperabilidade, conversão para *standard* e a migração para suportes analógicos.

A retro-compatibilidade (ou atualização da versão do formato) é definida como a possibilidade de interpretar e reproduzir um ficheiro que foi criado numa versão antiga de uma determinada aplicação informática, numa nova versão da aplicação. Por exemplo, é possível criar, ler e gravar ficheiros Excel 97 na versão Excel 2010. Esta possibilidade tem como desvantagens permitir um número limitado de compatibilidade de formatos, normalmente dois ou três; o fato dos registos permanecerem dependentes do fornecedor que é proprietário do *software* e muitas vezes o objeto conceptual ser alterado ligeiramente, o que pode afetar a autenticidade e a integridade de registos digitais (Verdegem e Slats, 2004). Este tipo de migração é mais indicado para o curto prazo, pois com as sucessivas migrações corre o risco de acumular pequenos erros ou mutações.

A interoperabilidade é entendida, neste contexto, como a possibilidade de um ficheiro poder ser transferido de uma plataforma ou aplicação para outra diferente mantendo a possibilidade de reprodução na mesma aplicação ou outra similar. Por exemplo, um ficheiro Excel pode ser lido em Lotus 1-2-3 e pode ser gravado/

transformado num ficheiro Lotus. Neste tipo de migração corre-se o risco de se perderem características essenciais dos registos digitais, em particular se se tratar de um *layout* complexo ou conteúdo multimédia (Verdegem e Slats, 2004).

A conversão para *standards* é a migração de um formato proprietário (fechado) para um formato *standard* publicado (público ou proprietário). A vantagem desta migração é o facto dos registos digitais deixarem de depender do *hardware* e *software* original, que os poderiam levar à obsolescência (Verdegem e Slats, 2004).

A migração para suportes analógicos consiste na conversão de objetos digitais para suportes analógicos (não digitais) de longa duração, como por exemplo, a reprodução de um objeto em papel ou microfilme, cuja finalidade é aumentar a longevidade do objeto digital. Tem como principal desvantagem, o facto de só poder ser adotada para objetos digitais que tenham características passíveis de serem representadas em suportes analógicos, como texto ou imagem, não se aplicando a objetos digitais interativos e/ou dinâmicos (Ferreira, 2006).

O encapsulamento preserva juntamente o objeto digital e toda a informação necessária e suficiente para no futuro permitir o desenvolvimento de emuladores, conversores e visualizadores e tem como objetivo a conservação do formato original. Foram desenvolvidos alguns formatos que são independentes da aplicação informática a utilizar, ou dos suportes físicos onde os objetos digitais são criados ou armazenados.

Quando se fala em preservação digital é ainda importante realçar os conceitos de refrescamento e meta-dados. O primeiro consiste na transferência periódica de suporte físico de armazenamento para um mais recente antes que o anterior se torne obsoleto ou se deteriore. O segundo é definido, de forma simplista, como a informação sobre a informação, ou, informação estruturada para descrever dados digitais utilizando *standards* específicos, ou de outra forma, é a descrição exaustiva e estruturada da informação digital. Embora não constituam estratégias de preservação em si mesmas contribuem para o seu sucesso.

Afinal qual a melhor estratégia de preservação a seguir? A resposta é simples. É a que melhor se adequa ao contexto específico da instituição preservadora e às características do objeto digital a preservar. Ao escolher a estratégia de preservação deve ter-se em consideração além do já referido, o interesse em fazer o arquivo e sua comunidade de interesse, o tipo de material, o custo da manutenção e implementação.

O mercado oferece várias soluções informáticas, vocacionadas essencialmente para a gestão de documentos eletrónicos, que permitem gerir de forma eficaz a produção, circulação e armazenamento de documentos, mas não a conservação digital, não comportando funcionalidades de preservação dos documentos por períodos de tempo prolongados. Esta lacuna implica que as organizações tenham muitas vezes que desenvolver o seu próprio *software*.

A preservação digital deve ser planeada desde o momento da criação da informação digital, pois dada a sua complexidade e pertinência não se pode correr o risco de se perder informação crítica para as instituições ou para os cidadãos. É determinante que seja equacionada logo na fase de requisitos e implementação das aplicações informáticas, o que raramente acontece.

Plano de Preservação Digital

Objetivos Genéricos

O projeto de elaboração de um Plano de Preservação Digital (PPD) pretende produzir um documento estratégico que:

- Identifique e caraterize a informação digital produzida pelo organismo, categorizando-a de acordo com necessidades operacionais e consequentemente, atribuindo prazos de conservação das classes de informação identificadas;
- Determine quais os procedimentos a realizar para evitar obsolescência tecnológica e a consequente probabilidade de perder informação, indicando os procedimentos que devem ser empreendidos para cada classe de informação identificada;
- Indique e clarifique responsabilidades dentro da organização relativamente à execução desses mesmos procedimentos.

Complementarmente, a elaboração de um plano de preservação digital pretende dotar o organismo de ferramentas conceptuais e operacionais que permitam a gestão da sua informação digital de forma a mantê-la utilizável, garantindo os seus propósitos administrativos e eventualmente patrimoniais pelo tempo considerado necessário.

Objetivos Específicos

Para conseguir os propósitos enunciados, a elaboração de um PPD segue uma metodologia que pretende essencialmente recolher de forma pertinente, sistemática e direcionada, a informação necessária para a formulação de procedimentos práticos.

Esta informação incide sobre diversas entidades e objetos que podem ser assim categorizados:

- Sistemas. São recolhidos dados identificativos sobre os sistemas onde a informação digital é produzida e/ou guardada. Com este primeiro nível de informação ficar-se-á a saber que sistemas existem, onde existem (física e

logicamente), quais os atores que agem sobre esses sistemas e em que papel o fazem. Cada sistema será identificado de forma unívoca dentro da organização através da atribuição de um identificador de projeto.

- Avaliação. É recolhida informação específica sobre o conteúdo funcional de cada sistema identificado (e da informação nele contida), a relação informacional e funcional que cada sistema tem em relação aos outros; será feita uma estimativa de prazo de conservação dessa informação (sistema) e do seu destino final. Sempre que possível procurar-se-á sustentar esta análise com diplomas jurídicos ou normativos.
- Plataforma tecnológica. Neste nível é recolhida informação técnica sobre a plataforma tecnológica subjacente a cada um dos sistemas identificados. Esta plataforma integra o sistema intermediário (*software*) do *hardware*, as estruturas de armazenamento, de *backup*. Pretende-se ainda localizar procedimentos de *software* conducentes a aumentar a segurança do sistema (existência de criptografia, rotinas de auditoria e respetivos registos, etc.). Ainda nesta etapa serão identificados os formatos em que se encontra registada a informação.

Todos estes dados serão necessários para propor procedimentos e plataformas alternativas para assegurar a preservação da informação digital.

Após a análise desta informação, a qual deverá ser recolhida da forma mais completa, precisa e sistemática possível, é realizado um quadro síntese que inclui as estratégias de preservação bem como os procedimentos específicos para a informação contida em cada sistema identificado.

A concretização do Plano de Preservação Digital implica uma atitude organizacional compaginável com a gestão da mudança. A atribuição de novas responsabilidades para a concretização do plano bem como as responsabilidades imputadas aos serviços e pessoas implica a assimilação dessas novas tarefas e esquemas interpretativos associados, numa lógica de atividade corrente e continuada da organização.

Benefícios

Evitar a obsolescência tecnológica terá como consequência a diminuição da probabilidade de perder informação. Atuando antes da informação digital se tornar obsoleta e consequentemente inutilizável estar-se-á em melhor situação para gastar significativamente menos recursos e conseguir melhores resultados na gestão de informação.

Pretende-se que os organismos sejam capazes de gerir a sua informação digital de forma a mantê-la utilizável garantindo os seus propósitos operacionais.

Se o Plano for corretamente elaborado, executado e monitorizado as vantagens serão:

- A utilização racional e continuada da informação digital mantendo a operacionalidade da organização;
- O conhecimento exato dos sistemas existentes, a sua relação com o contexto funcional e organizacional, bem como a clarificação dos agentes que sobre eles atuam;
- A criação de conhecimento e infraestruturas apropriadas para a preservação digital;
- A redução de custos de armazenamento e gestão provocadas pela eliminação de volumes de informação desnecessária;
- A aquisição do conhecimento e das informações necessárias para a implementação de outros projetos como a segurança informática (*e.g.* COBIT).

A Preservação Digital em Portugal

Em Portugal temos vindo a acompanhar a tendência de desmaterialização de processos e crescente intermediação tecnológica. O *Simplex* e a modernização administrativa são exemplo paradigmático dessa tendência. No entanto, nenhum dos projetos desenvolvidos neste âmbito contempla qualquer ação de planeamento ou implementação relativa a preservação digital, ou seja, são orientados para o resultado imediato sem levar em linha de conta as necessidades decorrentes da manutenção dos produtos obtidos a médio e longo prazo. Os próprios sistemas desenvolvidos subjacentes a interfaces virados para o utilizador cliente, não consideram fatores destinados a acautelar a usabilidade da informação produzida e armazenada a médio ou longo prazo. Esta situação tem implicações graves que nos parecem óbvias.

Sem o desenvolvimento de medidas de proteção e salvaguarda da informação que lhe permita resistir mantendo a sua autenticidade e usabilidade ao longo do tempo, o resultado provável é essa informação tornar-se obsoleta acompanhando assim a tendência natural de desatualização dos sistemas de informação e das tecnologias informáticas. Não se questiona a existência de ações de atualização de *software* e que estas tenham sido planeadas. No entanto, estas medidas não incidem ou podem não incidir sobre informação proveniente de transações passadas e que não têm utilidade administrativa operacional mas mantêm ainda valor informativo e probatório.

Nota-se uma atitude de desvalorização desta componente em favor de outros fatores considerados prioritários, como a rapidez de desenvolvimento e disponibilização ao cliente de um determinado serviço. A nosso ver esta atitude compor-

tamental e metodológica apresenta graves riscos no que respeita à preservação do património arquivístico digital.

Constata-se a existência de falta de consciência relativamente ao risco da memória social digital se perder. De uma forma geral as pessoas encontram-se ainda mentalmente enquadradas, no que respeita a preservação e memória, ao ambiente tradicional de suporte papel. A perenidade e estabilidade que são qualidades intrínsecas deste suporte levam a pensar que o mesmo se passa no que respeita a informação digital. Considerações sobre quem preserva, como se preserva não são óbvias nas ações e planeamento dos agentes organizacionais e sociais. E se em papel esta atitude era similar, as suas consequências transportadas para o contexto volátil das TIC, resulta provavelmente no desaparecimento da memória.

Existem casos constatados de perda de registos em determinados sistemas de informação desenvolvidos no contexto do plano tecnológico, sistemas esses que são críticos do ponto de vista social e probatório, justificativos de conservação permanente. É, por exemplo, o caso do sistema SIRIC (Sistema de Informação do Registo Civil) que guarda os registos vitais dos portugueses – nascimentos, casamentos, óbitos, divórcios –, ou o CITIUS o atual sistema de suporte à atividade judicial. Estas perdas podem ainda não ser consideradas críticas, na medida em que, sendo o sistema recente, as pessoas sobre as quais os registos dizem respeito ainda são presumivelmente vivas pelo que é possível refazer esses registos, mas não há garantia que no futuro o mesmo não possa voltar a ocorrer. Não existe inclusivamente qualquer estudo publicamente divulgado que nos permita saber a dimensão da perda nem tão pouco o impacto que essa perda pode vir a ter tanto sob o ponto de vista de prova como de memória nacional.

A preservação digital não se inicia, tal como acontece com documentos em papel, na sua fase terminal de vida operacional. Um documento eletrónico torna-se potencialmente ilegível e portanto inutilizável ao fim de um período de tempo variável mas que pode ser tão curto como apenas sete anos. Nestas circunstâncias, a preservação digital é necessária mesmo dentro da organização produtora para que a informação produzida possa manter a sua usabilidade e utilidade probatória e operacional.

Considerações Finais

O facto de o papel ter uma durabilidade de mais de cem anos, leva o ser humano a não ter urgência na sua preservação. Aliás, a preocupação é o expurgo por questões de segurança e espaço. Mas, o paradigma mudou, e agora à medida que as aplicações, formatos e tecnologia vão sendo descontinuados, se tornam obsoletos ou irrecuperáveis, tudo se perderá à exceção do que se preservar.

As instituições não estão sensibilizadas para a pertinência dos planos de preservação digital. Embora as instituições possam ter em alguns casos um plano de preservação documental para suportes analógicos, não sentem necessidade de desenvolver o mesmo tipo de estratégia para a informação do universo digital. Muitas instituições já só dispõem de determinados documentos em formato digital sem que tenham a mínima sensibilidade para a sua preservação de longo prazo. Este facto pode implicar que esta informação se perca com as óbvias consequências ao nível de desempenho operacional traduzido em todas as vertentes da atividade organizacional (económica, salvaguarda de direitos, bem social). Muitos dos sistemas implementados estão já em fim de vida sem que as organizações e os seus gestores estejam sensibilizados para este tema, correndo sérios riscos de se perder informação crítica que será irrecuperável.

As infraestruturas de informação críticas para a segurança nacional deveriam obrigatoriamente ter planos para garantir a continuidade operacional da informação. E não nos referimos apenas à informação residente em sistemas ativos mas aquela que tendo ultrapassado um determinado prazo de vigência operacional ainda possui importância estratégica sob o ponto de vista de conhecimento, ou seja, a informação residente em *backups* não monitorizados e sistemas em vias de isolamento tecnológico.

A identificação da informação digital categorizada como crítica, independentemente da sua área funcional – saúde, obras públicas, etc. –, incluindo a sua evolução temporal associada ao respetivo grau de criticidade bem como a definição de medidas que assegurem continuadamente o acesso e exploração dessa informação, deveria ser uma prioridade na definição de uma política de informação nacional.

O desenvolvimento da sociedade está de certa forma relacionado com a memória de que essa mesma sociedade dispõe. A coesão social apenas é possível se a memória de um país e das suas estruturas individuais e coletivas for mantida viva, dinâmica e acessível atuando então como referencial identitário do país. No entanto, a memória radica na informação e se esta desaparecer, as consequências serão dificilmente mensuráveis, mas facilmente percetíveis como graves.

Afinal de contas de que serve a segurança nacional se não houver Nação?

Referências Bibliográficas

Ferreira, M. (2006). *Introdução à Preservação Digital: Conceitos, Estratégias e Atuais Consensos*. Guimarães: Escola de Engenharia da Universidade do Minho.

Ferreira, M. (2008). *Preservação Digital: Um Problema Multidimensional*. Paper apresentado no Seminário de Preservação Digital. Disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/8431/1/SMD-0.2.pdf

Verdegem, R. e J. Slats (2004). "Practical Experiences of the Dutch Digital Preservation Test-bad". *The Journal of Information and Knowledge Management System* n.º 34.

Ciber(in)segurança da Infraestrutura de Transportes Públicos

Nelson Nobre Escravana

Engenheiro informático pelo IST com especialização em Gestão pelo ISEG. Tem efetuado no INOV INESC Inovação (Instituto de Novas Tecnologias) atividades associadas à criação e desenvolvimento de software para sistemas embebidos, de aplicações para operadores de telecomunicações móveis, consultadoria em segurança informática, análise de risco e auditorias de segurança com ênfase em testes de penetração. Atualmente coordena a área de Comunicações do INOV onde se inclui a área de investigação e desenvolvimento em cibersegurança.

João Lima

Aluno finalista de Engenharia Informática e Computadores do IST e investigador de segurança informática no INOV INESC Inovação.

Carlos Ribeiro

Licenciado em Engenharia Electrotécnica, mestre e doutor em Engenharia Informática e docente neste departamento do Instituto Superior Técnico. Tem duas obras publicadas sobre arquitetura de computadores e sistemas operativos. De 1995 a 1998 foi consultor de segurança do Gabinete Nacional de Segurança. Entre 2008 e 2011 foi vice-presidente do conselho diretivo do centro de informática do Instituto Superior Técnico. É, desde Janeiro de 2012, pró-reitor da universidade técnica de Lisboa para a área das tecnologias de informação.

Resumo

A insegurança informática tem estado principalmente associada a ataques a computadores pessoais, ao furto de cartões de crédito ou aos ataques de negação de serviço aos sítios de internet de organizações de alta visibilidade. No entanto com a recente proliferação de ataques informáticos de elevada complexidade e eficácia, tem crescido entre os operadores de transportes públicos a necessidade de aumentar a resiliência da sua infraestrutura informática contra este tipo de ataques.
Não obstante já existir um conjunto considerável de ferramentas construídas com o objetivo de prevenir e detetar ataques informáticos, estas não estão devidamente adaptadas às necessidades específicas de proteção de infraestruturas críticas. A nossa proposta consiste numa ferramenta de deteção de intrusões especialmente construída para ambientes com um elevado nível de automação e cujos processos podem ser facilmente descritos. O sistema desenvolvido pode ser uma forma especialmente eficaz de detetar ataques nas infraestruturas de transportes públicos e, por extensão, ser utilizada na proteção de infraestruturas críticas em geral.

Abstract
Cyber-(in)security in Public Transportation Infrastructure

Cyber-(in)security has been mainly associated with attacks to personal computers, credit card theft or denial-of-service attacks to high-visibility organization's websites. However, with the recent proliferation of cyber-attacks aimed at critical infrastructures, have been growing among public transport operators the need to increase the resilience of their technological infrastructure against this type of attacks.
Despite the significant amount of tools developed in order to prevent and detect cyber-attacks, these tools were not adequately adapted to the specific needs of critical infrastructure protection. Our proposal consists of an intrusion detection tool specifically developed to be used in environments with a considerable level of automation, whose processes may be easily described. These processes may be an especially effective way to detect attacks not only in public transport infrastructures but also in critical infrastructures in general, thus increasing their protection.

Introdução

Ao longo do tempo as organizações têm vindo a adotar um número significativo de sistemas e tecnologias de informação e comunicação (TIC) como forma de automatizar e melhorar os seus processos, ao mesmo tempo que reduzem a dependência do trabalho manual. O uso desses sistemas teve origem em pequenas aplicações cujos objetivos diferem entre melhorar e acelerar a comunicação entre colaboradores, clientes e fornecedores, substituir processos manuais e mecânicos por processos automatizados praticamente sem intervenção humana e melhorar a segurança face a acidentes (*safety*), tendo crescido para aplicações críticas que controlam quase todos os processos e operações de uma organização.

Esta automatização, resultante da introdução das TIC, é comum a praticamente todos os setores da sociedade, incluindo aqueles que são atualmente considerados pela Comissão Europeia (The Council of the European Union, 2008; The Council of the European Union, 2007) como infraestruturas críticas nacionais (ICN) abrangendo setores como a energia (eletricidade, petróleo e gás), águas e transportes (terrestres, marítimos e aéreos) e muitos outros, desde o setor financeiro até à generalidade do tecido empresarial.

Os centros urbanos cresceram significativamente, quer em tamanho, quer em população, nas últimas décadas e consequentemente as infraestruturas de transportes sofreram alterações como forma de suportar as necessidades de mobilidade de pessoas e bens. Com o crescimento das redes de transportes, a tarefa de manualmente gerir e operar cada linha dos vários sistemas de transportes tornou-se complexa. Como forma de lidar com este problema, os Operadores de Transportes Públicos (OTP) criaram um conjunto de sistemas de informação de forma a automatizar as suas operações, tornando-as ao mesmo tempo mais seguras, reduzindo a dependência do controlo humano, muitas vezes sujeito a falhas.

Ataques terroristas à infraestrutura de transportes públicos como aqueles observados em 20 de março de 1995 em Tóquio, 11 de março de 2004 em Madrid, e posteriormente em 7 de julho de 2005 em Londres mostraram a criticidade do papel que estas têm na sociedade, e ao mesmo tempo quão vulneráveis são.

O advento das Tecnologias de Informação, aliado a más práticas de codificação, instalação e administração de sistemas, trouxe também um conjunto de problemas de segurança. Aliado à questão tecnológica, encontra-se o facto do desenho dos processos de negócio dos operadores de transportes públicos, tal como de várias outras

ICN, não ser na sua maioria pensado de raiz com as preocupações de segurança face a ataques maliciosos (*security*), nomeadamente de ciber-segurança, mas antes com preocupações de segurança face a acidentes e ações não intencionais (*safety*). Tal resulta fundamentalmente destes sistemas terem sido desenhados para ambientes controlados onde escasseavam "predadores", mas também da ausência de soluções de segurança específicas para sistemas tão especializados como os sistemas dos OTP.

Genericamente, os sistemas informáticos são diariamente sujeitos a um grande número de ataques com o objetivo de interromper o seu funcionamento, ganhar acesso a estes, ou retirar-lhes informação valiosa. Os sistemas de informação e gestão da rede dos OTP não são exceção.

Que seja do nosso conhecimento, nenhum ciberataque de larga escala às redes de transportes públicos foi reportado, no entanto a sua criticidade aliada às vulnerabilidades usualmente existentes em sistemas informáticos levantam preocupações quanto à sua proteção.

Tome-se como exemplo um ataque conduzido por um estudante polaco de 14 anos que, usando apenas um comando de TV modificado, foi capaz de tomar o controlo de uma rede de elétricos, mudando as agulhas da linha à sua vontade. As únicas consequências deste ataque foram alguns comboios descarrilados, e algumas pessoas com ferimentos ligeiros. No entanto, a facilidade e reduzido esforço necessário para o conduzir, mostra quão vulneráveis estes tipos de infraestruturas estão.

Apesar das ameaças de segurança das TIC serem tão antigas como as mesmas (devemos recordar episódios como a interferência em transmissões morse no início do século XX, ou a guerra de grupos de *hackers* na década de 80) foi recentemente após episódios como o ataque ao Pentágono em 2008, o ataque à rede Sony, o ataque à Lockheed Martin, e culminando no *Stuxnet* (Falliere *et al*, 2011), dirigido aos sistemas de supervisão, controlo, automação e aquisição de dados (SCADA) de uma central nuclear iraniana em 2010, que emergiu o facto de que os tradicionais *script kiddies* e *hackers* individuais ou em pequenos grupos estão a ser substituídos por grupos altamente organizados e com capacidade para desferir poderosos ataques. Sendo as infraestruturas críticas um alvo apetecível para ciberataques de larga escala que apenas começaram a ser explorados, urge identificar mecanismos para a sua proteção.

Os sistemas de deteção de intrusões (IDS) apresentam-se como uma das soluções para aumentar o nível de proteção de qualquer infraestrutura informática, e por consequência as infraestruturas informáticas de suporte de infraestruturas críticas. No entanto, historicamente estes sistemas sofrem de um conjunto de problemas de eficácia, dado o número elevado de falsos alarmes gerados (Axelsson, 2000) que fazem com que os responsáveis de segurança das organizações estejam muitas vezes demasiado ocupados a distinguir os verdadeiros alarmes de entre os alarmes gerados, limitando assim a sua capacidade de resposta. Este número elevado de falsos alarmes não resulta tanto da ineficiência dos sistemas de deteção

de intrusos, que apresentam taxas de eficácia da ordem dos 99%, mas sim da elevada quantidade de informação a tratar o que é usualmente designada por *base-rate fallacy* (Axelsson, 2000).

Como solução para alguns dos problemas identificados acima, o INOV desenvolveu um sistema de deteção de intrusões híbrido (patente pendente), que combina técnicas de deteção de assinaturas (*misuse detection*), com técnicas de deteção baseadas em especificações (*specification-based*) de processos de negócio. As primeiras com o objetivo de detetar eficientemente ciberataques já conhecidos e as segundas como forma de detetar desvios da execução dos sistemas face ao especificado.

A grande vantagem desta solução é, não só, a capacidade de detetar ataques que explorem vulnerabilidades não conhecidas mas também ataques que resultem de comportamento malicioso, sem, no entanto, sofrer dos problemas do elevado número de falsos positivos que os sistemas de deteção de intrusos baseados na deteção de anomalias têm (Debar *et al*., 1999).

Tecnologias de Informação nas Redes de Transportes Públicos

O uso de tecnologias de informação tem crescido ao longo do tempo como forma de apoiar os operadores de transportes públicos a prestar um serviço melhor e mais seguro aos seus clientes.

Apesar da sua relevância não são conhecidas descrições detalhadas ou mesmo superficiais das tecnologias de informação utilizadas nas redes de transportes públicos o que dificulta a avaliação das vulnerabilidades do sistema e o desenho de tecnologias de proteção contra ciberataques. É pois particularmente pertinente a realização de uma avaliação, ainda que breve, sobre os sistemas em causa. Dado que a par da aviação, a rede metropolitana de comboio (de agora em diante Metro) é o tipo de redes de transporte em massa cuja infraestrutura tecnológica é mais complexa, foi esta a escolhida para uma breve análise. Desta resultaram cinco grupos de sistemas que serão descritos de seguida.

Sistemas de Bordo

Os sistemas de bordo são os utilizados para gerir tudo aquilo que acontece dentro dos veículos, ou está relacionado com o seu movimento. O conjunto de funcionalidades que estes sistemas oferecem é diverso, passando pelo controlo físico do veículo, até à disponibilização de informação aos passageiros:

- O Sistema de Informação aos Passageiros (SIP) é não só responsável por informar os passageiros acerca do tempo estimado até à chegada à próxima

paragem, mas também acerca das condições atuais de circulação, conexões com outros meios de transporte, e até, em alguns casos, oferecer acesso a internet sem fios;
- Por outro lado, o Sistema de Bilhética é usado para receber dos passageiros o pagamento pelas viagens que estão a realizar, bem como validar os seus títulos de transporte;
- Finalmente, e talvez mais importante, o Sistema de Controlo e Seguimento do Veículo é usado para controlar, monitorizar e operar todos os componentes eletromecânicos do veículo. De entre estes componentes estão incluídos os subsistemas de propulsão, travagem, e deteção de obstáculos, sendo estes componentes vitais para o correto funcionamento do veículo.

Em alguns casos, a operação dos veículos é inteiramente assegurada por este sistema. Nesses casos, este grupo de sistemas assume um caráter ainda mais crítico, dado que este é responsável pela operação do veículo, quer seja em condições normais ou numa emergência. É também responsabilidade deste sistema o cálculo da posição atual do veículo, para que os sistemas auxiliares possam determinar a zona até onde este pode avançar em segurança.

Sistemas de Linha

Neste grupo de sistemas constam todos os sistemas instalados ao longo das linhas, e que gerem a interação dos veículos com os sistemas de controlo centrais. Uma linha é usualmente dividida em várias zonas, sendo que cada zona contém uma instância dos sistemas abaixo:

O Sistema Automático de Gestão de Velocidade é o sistema de terra responsável por interagir com o Sistema de Controlo do Veículo. A sua principal função é calcular o ponto que pode ser atingido com segurança por cada um dos veículos sem que se corra o risco destes colidirem ou se aproximarem demasiado;

Por sua vez, o Sistema de Controlo de Zona interliga os diversos sensores e controladores existentes numa zona da linha tais como as agulhas, passagens de nível, energia e equipamento de sinalização, e gere o seu estado de acordo com os veículos em circulação nessa zona.

Sistemas de Estação

As estações, como agregadores de pessoas por excelência, estão equipadas com um conjunto de sistemas desenhados com o objetivo de assistir os passageiros a alcançar os transportes desejados de forma rápida, fácil e confortável:

- Nas estações, o Sistema de Informação a Passageiros (SIP) tem um papel central. A sua principal função é ajudar os passageiros a movimentar-se dentro das estações, dado que tem o conhecimento das plataformas a que os veículos esperados pelos passageiros irão chegar. Da mesma maneira, em caso de emergência, este sistema é usado para encaminhar os passageiros para uma localização segura;
- O Sistema de Controlo de Estação gere, controla e monitoriza os diversos componentes eletrónicos e eletromecânicos existentes numa estação, tal como as portas das plataformas, elevadores, escadas rolantes, sistemas de deteção e supressão de incêndios, etc.;
- O Sistema de Bilhética é utilizado não só para vender títulos de transporte aos passageiros, mas também para os validar, e consequentemente permitir o acesso dos passageiros às diversas plataformas existentes na estação.

Sistemas de Centro de Controlo de Operações

Como forma de centralizar a gestão e operação das diversas linhas à responsabilidade de cada operador, estes criaram centros de controlo de operações que assumem esta função que, por consequência, contam com um conjunto significativo de sistemas de apoio:

- A gestão e operação de uma linha em que circulam um número considerável de veículos ao mesmo tempo seria muito difícil sem a existência de um Sistema de Controlo de Tráfego. O objetivo deste sistema é capturar, em alto nível, o estado da rede de forma a manter os operadores informados, e ao mesmo tempo permitir comparar este estado com o estado esperado dos veículos;
- O objetivo do Sistema de Controlo de Energia é monitorizar e controlar o estado da rede elétrica usada para mover os veículos. Este trabalha em colaboração com o Sistema de Controlo de Tráfego, de forma a saber os troços de linha que devem ter a energia ativada a cada momento;
- O Sistema de Videovigilância é usado para guardar e monitorizar as imagens de videovigilância das várias entidades na rede (veículos, estações, postos de transformação elétricos, etc.). Em algumas situações, estes sistemas usam capacidade inteligentes de processamento de vídeo, de forma a detetarem imagens às quais deve ser dada especial atenção pelos operadores;
- O Sistema de Gestão da Informação de Passageiros é responsável pela preparação, configuração e distribuição da informação a ser apresentada nos vários pontos, nomeadamente naqueles em que existem Sistemas de Informação de Passageiros em uso.

Tecnologias de Comunicação

A comunicação entre as várias entidades envolvidas numa rede de transportes é de extrema importância. Para além disto, os próprios sistemas usados nestas redes necessitam de comunicar de forma expedita e contínua, de forma a coordenarem a sua operação. Três tipos principais de redes de comunicação são tipicamente utilizados:

- Redes móveis profissionais, como o TETRA e o GSM-R são usadas não só para comunicação de voz entre os operadores e o pessoal de terra, mas também para executar pequenas aplicações de assistência à operação dos veículos. No futuro, é esperado que a rede GSM-R seja utilizada para possibilitar a interoperabilidade entre as redes de transportes de cada país;
- Redes sem fios, como o Wi-Fi, são usadas com dois propósitos: por um lado, são usadas por aplicações utilizadas nos veículos com necessidades de grande largura de banda, como seja a transferência de imagens de bordo para o centro de controlo de operações, e por outro lado para suportar a comunicação de aplicações críticas como a localização de veículos e cálculo de posição máxima permitida. No segundo caso é utilizada normalmente uma frequência especial;
- Finalmente, as redes cabladas são utilizadas para interligar as várias subredes existentes numa rede de transportes.

Iniciativas Europeias

Com os ataques terroristas de Tóquio, Madrid e Londres, a União Europeia aumentou a preocupação na procura de soluções de forma a aumentar a proteção das infraestruturas de transportes públicos.

Neste contexto, foram criados vários projetos de investigação e desenvolvimento, suportados pelos Programas Quadro da Comissão Europeia. Dois desses projetos, cuja relevância é maior relativamente a este trabalho são o COUNTERACT e o DEMASST.

COUNTERACT

O projeto COUNTERACT (*Cluster of User Networks in Transport and Energy Relating to Antiterrorist Activities*) é composto por um alargado consórcio industrial, e teve como principal objetivo aumentar a segurança contra ataques terroristas dirigidos a redes de transporte de passageiros e mercadorias, bem como infraestruturas de produção e distribuição de energia.

Este projeto foi conduzido a um alto-nível de abstração, apesar do seu foco na ameaça terrorista, de forma a identificar genericamente as vulnerabilidades nos domínios estudados.

No contexto deste projeto, foi realizada uma análise das ameaças a que estão sujeitos os domínios em estudo, tendo sido apontados os ataques por bombistas suicidas, a detonação remota de dispositivos explosivos improvisados (IED), os ataques incendiários, a vandalização da infraestrutura e as armas químicas, biológicas, radiológicas e nucleares (CBRN) como as principais ameaças (COUNTERACT Consortium, 2010).

A ciberameaça é apenas superficialmente endereçada, sendo no entanto referido que esta é considerada relevante, dadas as consequências que poderia ter quer no funcionamento da rede, quer em termos de vidas humanas.

DEMASST

O projeto DEMASST (*Demo for Mass Transportation Security: Roadmapping Study*), ao contrário do projeto COUNTERACT, teve como objetivo estabelecer o estado da arte da segurança nas redes de transportes, identificando pontos de melhoria e apontando uma estratégia para implementar as soluções propostas.

No estudo realizado acerca do estado da arte da segurança nas redes de transportes (DEMASST consortium 2009), e naquilo que à ciberproteção diz respeito, é referido que o esforço empregue pela maioria dos operadores para melhorar a sua proteção é baixo, limitando-se ao uso de mecanismos de proteção já oferecidos pelas tecnologias utilizadas.

Cibersegurança nas Redes de Transportes Públicos

Não obstante já terem sido realizados diversos projetos com foco na segurança em redes de transportes, a cibersegurança tem sido subvalorizada, e por vezes totalmente ignorada. Nos projetos descritos anteriormente, o fraco desenvolvimento desta área é associado ao facto de os operadores de transportes não possuírem o conhecimento suficiente para abordar o problema.

No entanto, a ciberameaça é unanimemente considerada como de elevado risco, cujas consequências caso fosse explorada seriam significativas. Michael *et al.* (2003) apresenta uma comparação entre um ataque cinético e um ciberataque usando uma análise quantificada de Schmitt, provando que os ciberataques têm consequências similares, se não superiores, aos ataques cinéticos.

Baseado no nosso estudo da infraestrutura TI das redes de transportes públi-

cos, foram identificados três cenários de ataque de alto nível, cuja realização teria consequências relevantes no normal funcionamento destas:

- Sequestro de veículo – um atacante que consiga ganhar acesso aos sistemas de controlo automático dos veículos pode dirigi-los para onde quiser, podendo fazer dois veículos colidirem em hora de ponta por exemplo;
- Disrupção da circulação numa linha – se um atacante for capaz de ganhar acesso a qualquer um dos sistemas de controlo de linha, ele consegue parar essa linha, e assim gerar o pânico e a confusão entre os passageiros;
- Manipulação da informação aos passageiros – os passageiros apoiam-se consideravelmente nos SIP para se movimentarem nas estações. Se um atacante for capaz de manipular a informação apresentada por esses sistemas, por exemplo gerando um false alarme de incêndio, este conseguiria gerar o pânico numa estação e assim pôr em causa a integridade física dos passageiros. Se esta ação for complementada com outras como por exemplo colocar as escadas rolantes e torniquetes em posição de entrada, as consequências podem ser dramáticas.

Sistemas de Deteção de Intrusão

Os Sistemas de Deteção de Intrusão (IDS) têm sido utilizados ao longo do tempo como forma de aumentar a proteção dos sistemas e infraestruturas de TI contra ataques. Um IDS pode ser definido como um sistema que monitoriza a atividade de um sistema, grupos de sistemas ou rede, de forma a detetar qualquer atividade ilícita executada neste, reportando as ilicitudes detetadas de forma estruturada e facilmente percetível pelos responsáveis de segurança.

Os IDS são usualmente classificados em três grandes eixos (Axelsson, 1999): (1) método de captura de dados, (2) arquitetura de sistema e (3) estratégia de processamento.

O primeiro diz respeito ao local onde são capturados os dados que servem de base à deteção, se na memória (persistente ou volátil) das máquinas que suportam as TI, se na rede que interliga as TI. O segundo está intimamente ligado à dimensão do sistema de deteção de intrusos e ao facto dele poder ser: uma instância única que colige e analisa os dados; um sistema centralizado com vários sensores que capturam dados e os enviam para uma unidade central de processamento; ou um sistema distribuído que captura e analisa os dados de forma distribuída. É, no entanto, o terceiro eixo de classificação que se afigura o mais importante para o problema a resolver.

Estratégia de Processamento

De forma a ser capaz de detetar intrusões, o IDS tem de ser capaz de processar os dados capturados, de forma a descobrir algo relacionado com alguma tentativa de intrusão, quer esta já tenha sido bem-sucedida ou não. Quanto à estratégia de processamento, consideramos a existência de três alternativas:

- Deteção de Assinaturas – de molde a detetar intrusões, estes sistemas utilizam assinaturas de ataques, que são criadas cada vez que um novo tipo de ataque é descoberto. Posto isto, estes sistemas têm como limitação o facto de apenas conseguirem detetar ataques para os quais uma assinatura já tenha sido produzida. O Snort (Roesch, 1999) é um exemplo de um sistema que utiliza assinaturas de ataques;
- Deteção de Anomalias – alguns sistemas baseiam a sua deteção em modelos de comportamento dos sistemas monitorizados, gerando alarmes quando são observados desvios a estes modelos. Estes sistemas têm uma fase inicial, chamada de aprendizagem, em que os modelos de comportamento dos sistemas a serem monitorizados são criados. No entanto, esta fase é considerada um dos pontos fracos deste tipo de sistemas (Gates e Taylor, 2006). O sistema IDES (Denning, 1987), e posteriormente o sistema PAYL (Wang e Stolfo, 2004) foram propostos usando técnicas de deteção de anomalias;
- Deteção Baseada em Especificações – este tipo de sistemas foi criado como forma de resolver alguns dos problemas identificados nas duas estratégias de processamento anteriormente descritas. O seu processamento é baseado na comparação entre o comportamento dos sistemas monitorizados, e uma especificação do comportamento esperado. Estas especificações são normalmente modelos definidos por humanos, quer sejam os responsáveis pela segurança da organização ou qualquer outra entidade externa, e que devem refletir, da forma mais aproximada possível da realidade, o comportamento dos sistemas. Por aproximarem a deteção de intrusões ao comportamento esperado pelos sistemas monitorizados, estes sistemas são conhecidos por produzirem um baixo número de falsos alarmes;
- Um dos primeiros sistemas propostos a utilizar esta estratégia de processamento foi apresentado por Ko *et al.* (1997), e o seu funcionamento baseava-se na monitorização da execução de aplicações com privilégios elevados em sistemas UNIX.

Problemas

Apesar do reconhecido valor dos IDS na proteção de redes e sistemas contra ataques, é também apontado um conjunto de problemas que impedem o seu uso de forma mais abrangente. O aspeto à volta do qual tem existido mais discussão, e também sobre o qual os resultados práticos têm sido mais contraditórios, é a estratégia de processamento.

Os sistemas de deteção de assinaturas são conhecidos por produzirem um elevado número de falsos negativos, que se caracteriza por não gerarem um alarme quando um ataque realmente aconteceu. Estes erros acontecem neste tipo de sistemas dado a sua deteção ser baseada em assinaturas especificadas previamente, não sendo portanto capazes de detetar ataques para os quais ainda não tenham uma assinatura especificada.

Por outro lado, os sistemas de deteção de anomalias, são conhecidos por produzirem um elevado número de falsos positivos, que se caracterizam por gerar um alarme quando nenhuma intrusão aconteceu. Neste caso, estes erros acontecem dado que algumas vezes um desvio do padrão "aprendido" não se traduz efetivamente num ataque. Para além disto, é também possível que estes sistemas gerem falsos negativos, uma vez que é muito difícil de garantir que os dados de treino não tivessem qualquer ataque.

Por fim, os sistemas baseados em especificações são conhecidos como sendo mais balanceados do que as outras propostas. No entanto a sua utilização tem sido limitada, e quando usados, esta utilização é restrita aos níveis mais baixos do sistema, como sejam as chamadas de sistema e os protocolos de rede de baixo nível. A sua adaptação e utilização em camadas semânticas mais elevadas é ainda um desafio em aberto.

Uma das grandes vantagens dos sistemas baseados em especificações face aos sistemas clássicos de deteção de anomalias é a possibilidade de existir um aperfeiçoamento constante da especificação ao longo da vida do sistema. Nestes sistemas quando um falso positivo é detetado é possível analisar a especificação e perceber o que estava errado e que levou ao falso positivo. Já nos sistemas clássicos de deteção de anomalias é necessário voltar a treinar o sistema com novos dados, sendo que não há garantia que esses novos dados não tenham eles próprios ataques não detetados.

Por outro lado, os sistemas de deteção baseados em especificações são bem mais difíceis de colocar em produção que os sistemas clássicos de deteção de anomalias, isto porque é necessário efetuar uma especificação completa e detalhada do sistema, razão pela qual só podem ser aplicados a sistemas com processos algo repetitivos e de dimensão limitada, como são muitos dos sistemas que controlam as redes de transportes públicos.

Sistema Desenvolvido

Tal como já foi referido na introdução, o sistema desenvolvido consiste num sistema de deteção de intrusões híbrido, que combina técnicas de deteção de assinaturas com técnicas de deteção baseadas em especificações. A componente baseada em assinaturas tem como objetivo a deteção de ataques já conhecidos que podem ser utilizados para um atacante se estabelecer no interior de uma dada rede/sistema e a partir daí lançar ataques mais complexos, enquanto a componente baseada em especificações é utilizada para detetar ataques relacionados com a lógica de negócio dos sistemas monitorizados.

Este sistema oferece também a hipótese de utilizar sensores baseados na máquina e/ou sensores baseados na rede, como forma de adaptar a deteção ao tipo e especificidades dos sistemas monitorizados.

Modelo de Deteção Baseado em Especificações

Os sistemas de deteção de intrusão baseados em especificações têm sido apenas pontualmente utilizados, de fato, até em iniciativas puramente académicas as propostas na área são raras.

No sistema desenvolvido, a componente de deteção baseada em especificações é utilizada a um nível semântico mais elevado, a camada de negócio. Na camada de negócio, a deteção de atividades ilícitas é baseada quer na verificação da correta execução de processos de negócio, quer na verificação de conformidade das regras de negócio.

Um processo de negócio pode ser definido como sendo a forma como um conjunto de atividades numa determinada organização está estruturado e relacionado, de maneira a produzir um determinado resultado ou atingir um determinado objetivo, e assim criar valor. Estas atividades tanto podem ser executadas automaticamente pelos sistemas monitorizados, bem como podem requerer intervenção humana. A verificação dos processos de negócio é baseada na captura de padrões previamente estabelecidos, sejam estes observados em eventos de rede ou em registos aplicacionais ou de sistema operativo, que são utilizados como indícios da ocorrência de uma determinada atividade. Estes padrões capturados são posteriormente analisados, de forma a verificar que a execução real da atividades ocorreu de acordo com aquilo que foi especificado no processo de negócio.

Por outro lado, as regras de negócio definem ou delimitam uma certa propriedade do negócio, de forma a validar se determinada atividade está a ser conduzida de acordo com as políticas e orientações da organização. A verificação das regras de negócio está centrada na informação de negócio da organização, comummen-

te denominada de entidades informacionais, manipulada e/ou modificada pelos processos de negócio. Quando é verificada alguma alteração numa entidade informacional ligada a uma determinada regra de negócio, esta regra de negócio é reavaliada de forma a determinar a sua conformidade.

Quando existe uma violação da especificação de um processo/regra de negócio (como sejam um conjunto de ações executadas fora da ordem pela qual o deveriam ser, ou uma regra de negócio que é avaliada como não conforme), esta violação é analisada de acordo com um conjunto de critérios previamente estabelecidos, de modo a determinar o nível de alarme de intrusão a ser emitido.

Arquitetura de Sistema

O sistema desenvolvido está organizado segundo uma arquitetura centralizada. Utiliza, para detetar as atividades que ocorrem nos diversos sistemas e redes monitorizados, diversos sensores remotos, quer sejam estes sistemas de deteção de intrusão, sistemas de deteção de incidentes ou sistemas de monitorização e geração de alarmes. De maneira a interagir com estas soluções, que podem ser instaladas para serem usadas com este sistema ou já existirem nos sistemas a monitorizar, é disponibilizada uma camada fina de integração para que seja possível suportar qualquer tipo de sensor remoto.

Não obstante a deteção dos eventos ser realizada de forma distribuída, a gestão dos sensores e verificação dos eventos detetados é efetuada centralmente, num sistema propositadamente desenvolvido para esse efeito. Por um lado, este sistema central interage com os sensores de deteção para configurar as atividades que estes devem detetar. Por outro lado, recebe dos diversos sensores instalados os indícios da execução das atividades.

Este sistema central aplica um algoritmo especificamente desenvolvido para esse efeito de modo a verificar a correção das atividades detetadas. Este algoritmo é responsável por, após ter recebido um indício da execução de uma determinada atividade, selecionar de entre os processos de negócio em verificação aquele a que a atividade recebida pertence, e verificar a sua correção e ordem no respetivo processo. Caso alguma anomalia se verifique, este sistema reporta o processo (ou regra) onde esta anomalia aconteceu, bem como o fluxo de ações, quer no geral, quer no que diz respeito ao processo em análise, que antecederam a anomalia.

Avaliação

De forma a validar o sistema desenvolvido, foram conduzidos um conjunto de testes baseados em capturas de um conjunto de simuladores de uma rede de metro. A utilização deste simulador permitiu testar a ocorrência de situações anormais na circulação de uma rede de transportes sem que para tal fosse necessário recorrer a uma infraestrutura real, que em muito limitaria o âmbito dos testes[1].

O simulador em questão estava configurado para simular a circulação de 14 veículos numa linha, existindo 10 estações ao longo dessa linha. Em cada estação, existiam duas plataformas, às quais se dirigiam os veículos em função da direção em que se deslocavam na linha.

Deste ambiente de simulação foram sintetizados três processos de negócio que correspondem respetivamente à gestão de emergências numa plataforma, à gestão da informação de passageiros numa plataforma, e por fim à gestão da movimentação dos veículos na linha. Para além disto foi estabelecida uma regra de negócio que especificava a distância mínima que deveria ser mantida entre veículos.

Baseado neste ambiente de simulação e nos processos de negócio extraídos, foram realizados dois tipos de teste:

Teste de funcionamento normal – nestes testes foi simulado o funcionamento normal da rede de metro, de forma a avaliar a capacidade do sistema desenvolvido em verificar a execução dos processos e regras de negócio especificados sem que falsos alarmes fossem produzidos;

Teste com injeção de atividades anormais – por outro lado, neste conjunto de testes era pretendido avaliar se o sistema desenvolvido era capaz de detetar violações à especificação dos processos/regras discriminados.

Tendo em conta os veículos a circular na linha, o número de plataformas, e os processos de negócio sintetizados, é possível determinar que em cada teste existiam simultaneamente em verificação no mínimo 34 instâncias de entre os três processos de negócio.

Resultados Práticos

No primeiro conjunto de testes, verificou-se o sistema num contexto de normal funcionamento do ambiente simulado. Neste caso, e na primeira iteração, foi produzido apenas um alarme. Após uma análise detalhada do alarme produzido, foi possível verificar que se tratava de um falso alarme, que se devia a uma falha

1 O acesso ao simulador foi disponibilizado pela Thales Portugal, à qual agradecemos.

de perceção do funcionamento global do sistema que conduziu a uma falha na especificação de um dos processos de negócio. Esta falha foi corrigida, tendo sido seguida de uma nova iteração de testes, sendo que neste caso já não foi produzido qualquer alarme durante a totalidade do período de simulação.

De seguida procedeu-se ao teste num ambiente em que foram injetadas atividades externas. As atividades externas que correspondiam a atividades não especificadas foram assinaladas pelo sistema como atividades anormais; note-se porém que as atividades injetadas permitidas pelo sistema foram consideradas normais. Cada alarme gerado foi manualmente verificado, de forma a garantir não corresponder a um falso positivo, facto de nunca se verificou. De igual modo, foi verificada a relação entre o número de atividades anormais injetadas e, considerando os instantes de tempo em específico em que as mesmas chegaram ao sistema, verificou-se que nenhuma anomalia escapou à verificação da conformidade do processo.

Discussão

Analisando os resultados dos testes realizados na simulação da rede de metro, é possível discutir o potencial da solução desenvolvida.

Em primeiro lugar, demonstra-se que este tipo de abordagem é capaz de detetar intrusões com um reduzido número de falsos alarmes. Na primeira iteração de testes de funcionamento normal, foi verificada a existência de um falso alarme, devido a uma falha na especificação do processo de negócio. Resolvida que foi esta situação, este falso positivo não se verificou mais durante a totalidade dos testes.

Por outro lado, demonstra-se também que o sistema desenvolvido, naquilo a que ao ambiente de simulação diz respeito, não produziu qualquer falso negativo, tendo sido capaz de detetar todas as atividades que constituíam um desvio à correta execução do processo.

Por fim, todos os alarmes emitidos, possuíam um atraso que, caso se tratasse de uma rede real, poderia ter permitido ao responsável de segurança tomar medidas de contingência de forma a contornar a anomalia, possivelmente evitando que danos significativos fossem infligidos na infraestrutura e nos passageiros.

As principais limitações identificadas na aplicabilidade da solução desenvolvida consistem:

Na obrigatoriedade de proceder à completa definição dos processos de negócio a monitorizar. Tal facto limita o âmbito de aplicação da solução a cenários onde os processos de negócio conseguem ser definidos com elevada precisão;

A utilização de sensores (de rede ou de sistema) com o objetivo de obter indícios suficientes para inferir a execução dos processos de negócio, requer um

profundo conhecimento dos sistemas e protocolos envolvidos. No entanto após o desenvolvimento de regras para um dado sistema ou protocolo de comunicação, as mesmas regras podem ser facilmente reutilizáveis em outras instalações dos mesmos equipamentos.

Conclusão

As redes de transportes públicos, como infraestrutura crítica que são, têm-se tornado um alvo cada vez mais apetecível, incluindo através de um ciberataque aos seus sistemas informáticos. Algum trabalho foi já desenvolvido no sentido de aumentar a proteção destas infraestruturas contra este tipo de ataques, no entanto estas iniciativas são consideradas insuficientes.

Os sistemas de deteção de intrusão, sendo uma solução viável para aumentar a proteção destas infraestruturas, são ainda de utilidade limitada, dado o conjunto de problemas normalmente associados às suas técnicas de deteção e às elevadas necessidades de configuração. No entanto, com o sistema desenvolvido, demonstrámos que é possível resolver alguns dos problemas identificados.

A deteção de intrusões através da identificação de discrepâncias entre os indícios revelados pelos sistemas de informação e comunicação e a especificação dos processos de negócio vai bastante além da segurança dos sistemas envolvidos, pois contempla o negócio como um todo. Desta forma é possível não só detetar ataques aos sistemas, mas também tipos de ataque aos processos de negócio que tem historicamente sido consideravelmente difíceis de detetar e prevenir, tal como é o caso de ataques recorrendo à engenheira social.

Para além disto, a correlação dos alarmes da componente baseada em deteção de especificações com a componente de deteção baseada em assinaturas, que está prevista para uma futura versão deste sistema, permitirá obter a sequência de atividades maliciosas executadas por um atacante, e assim permitir aos responsáveis de segurança reconfigurar os seus sistemas de modo a colmatar essas vulnerabilidades.

Com esta nova tecnologia desenvolvida em Portugal no INOV, enquadrada no projeto SECUR-ED (cofinanciado pelo FP7[2] da Comissão Europeia) e que será demonstrada em redes de transportes terrestres europeias, é possível alargar a sua aplicação, para outros domínios onde seja relativamente fácil definir, com considerável precisão, os processos de negócio envolvidos. É possível prever a sua aplicabilidade em setores tais como o da energia, na distribuição de água potável e em muitos ramos da indústria.

2 Sétimo Programa Quadro de Investigação e Desenvolvimento.

Bibliografia

Axelsson, S. (1999). *Research in Intrusion Detection Systems: a Survey*. Disponível em ftp://ftp.cis.upenn.edu/pub/htdocs/verinet/references/Axelsson99.pdf.

Axelsson, S. (2000). "The base-rate fallacy and the difficulty of intrusion detection". *ACM Transactions on Information and System Security* n.º 3, pp.186–205. Disponível em http://portal.acm.org/citation.cfm?doid=357830.357849.

COUNTERACT Consortium (2010). *Deliverable 2 – Security in Transport and Energy: Overview of the Current Situation*. Disponível em http://www.transport-research.info/Upload/Documents/201207/20120719_144510_49401_Report%20_Deliverable%202.pdf.

DEMASST Consortium (2009). *Deliverable D3.1 - Current Status of Security in Mass Transport*. Disponível em http://www.bmbf.de/pubRD/WS_MT_Eriksson.pdf.

Debar, H., Dacier, M. e Wespi, A. (1999). "Towards a Taxonomy of Intrusion-Detection Systems". *Computer Networks* n.º 8, pp. 805–822.

Denning, D.E. (1987). "An intrusion detection model". *IEEE Transactions on Software Engineering*, n.º 2, pp. 222–232. Disponível em http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1702202.

Falliere, N., Murchu, L.O. e Chien, E. (2011). *Symantec W32.Stuxnet dossier*. Disponível em http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/falliere.pdf.

Gates, C. e Taylor, C. (2006). "Challenging the anomaly detection paradigm: a provocative discussion" in *New Security Paradigms Workshop (NSPW) '06*. Schloss Dagstuhl: ACM Press, pp. 21–29. Disponível em http://dl.acm.org/citation.cfm?id=1278940.1278945 .

Ko, C., Ruschitzka, M. e Levitt, K. (1997). "Execution monitoring of security-critical programs in distributed systems: a specification-based approach" in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*. IEEE Comput. Soc. Press, pp. 175–187. Disponível em http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=601332.

Michael, J.B., Wingfield, T.C. e Wijesekera, D. (2003). "Measured responses to cyber-attacks using Schmitt analysis: a case study of attack scenarios for a software-intensive system" in *Proceedings 27th Annual International Computer Software and Applications Conference, COMPAC 2003*, pp. 622–626. Disponível em http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1245406.

Roesch, M. (1999). "Snort – Lightweight intrusion detection for networks" in *Proceedings of LISA '99: 13th Systems Administration Conference*. Seattle: USENIX, pp. 1-11. Disponível em http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.105.6212.

The Council of the European Union (2007). "Communication from the Commission to the European Parliament and the Council on Stepping up the fight against terrorism". pp. 1–9. Disponível em http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,pt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=459135:cs&page=

The Council of the European Union (2008). "*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*". Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT

Wang, K. e Stolfo, S. J. (2004). "Anomalous payload-based network intrusion detection" in *Recent Advances in Intrusion Detection* (RAID), pp. 203-22.

Como Manter um Segredo... Secreto

Bernardo Patrão

Engenheiro Sénior da Critical Software. É licenciado em Engenharia Informática, pela Universidade de Coimbra. Iniciou a sua colaboração com a Critical Software aquando do seu estágio no verão de 2002, focando-se em sistemas confiáveis e sistemas operativos de tempo real, mudando-se posteriormente para a área de Segurança da empresa. Participou em vários projetos de desenvolvimento de software e auditoria na área de Segurança de Informação, sendo certificado em ISO 27001. É atualmente Gestor Técnico da solução csSECURE.

Resumo

A fuga de informação é um problema acidental? A necessidade de proteção da informação nas organizações está presente na mente de qualquer profissional de segurança. Acontecimentos recentes (WikiLeaks, fugas de dados pessoais de clientes, etc.) mostram-nos que a informação confidencial não está segura na sua forma tradicional, e o acesso à informação não é, de todo, controlado.

As ferramentas de segurança mais usadas atualmente são sobretudo centradas na rede e/ou no computador, protegendo a informação de ataques externos (hacks, vírus, cavalos de Tróia), mas não protegem as organizações contra fugas de informação. As técnicas mais promissoras para controlar as fugas de informação são o ERM (Enterprise Rights Management) e o DLP (Data Loss Prevention).

Os inconvenientes das soluções de ERM (dependência do utilizador, falta de classificação automática e a complexidade de administração) são colmatados com os pontos fortes dos produtos DLP, resultando numa abordagem inovadora no campo da segurança da informação.

Há soluções que combinam o ERM e o DLP, baseadas no conceito de segurança multinível que efetivamente protege as organizações contra fugas de informação, mantendo o controlo sobre os dados corporativos e monitorizando as ações dos utilizadores sobre a informação produzida.

Abstract
How to Keep a Secret… Secret

Is information leakage an accidental problem? The need for information protection within organisations, is present in the mind of every security professional. Recent history (WikiLeaks, information leakage of personal client data, etc.) teaches us that confidential information is not secure in its traditional form and access to information is not controlled at all.

Common security tools in place are typically network and/or computer centric, protecting information from external attacks (hacking, virus, trojans, etc.) but fail to secure companies against information leakage. The most promising techniques for controlling information leakage are ERM (Enterprise Rights Management) and DLP (Data Loss Prevention).

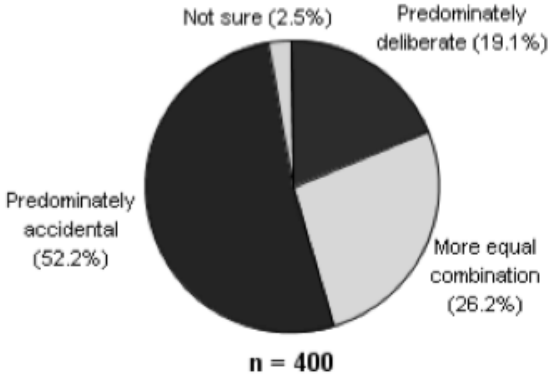
The drawbacks of the ERM solutions (user dependency, lack of automatic classification and administration complexity) and the strengths of DLP products combined, would reap the benefits of ERM and DLP, resulting in an innovative approach within the information security field.

There are solutions that combine ERM and DLP solution, based on the Multilevel security concept that effectively protects your organization against information leakage, while maintaining control over corporate data.

As fugas de informação são um problema real e cada vez mais comum. Quase todos os meses, notícias sobre fugas de informação numa organização tornam-se públicas. No entanto, estes são os casos conhecidos do público em geral e que têm um impacto mais visível nas organizações. Milhares de fugas de informação de organizações acontecem todos os dias, e maioritariamente por acidente, displicência ou mesmo com intenção!

De acordo com estudos recentes, a vasta maioria das fugas de informação têm uma natureza acidental: "O IDC[1] acredita que a maior parte das fugas de informação vão continuar a ser acidentais, mas esperamos um número crescente de ataques cuidadosamente planeados por sofisticadas organizações criminosas. Também acreditamos que os impactos financeiros dos incidentes deliberados de perdas de informação são normalmente muito maiores que os acidentais." (IDC, 2010).

Figura 1 – Distribuição de incidentes relacionados com segurança de informação



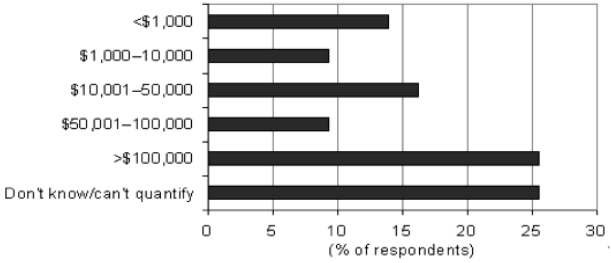
Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

Isto significa que as fugas de informação não são apenas o resultado de atos intencionais, mas também de ações sem intenção que os colaboradores da organização podem executar. As fugas de informação acidentais são talvez as mais perigosas, pois o utilizador não está consciente (pelo menos no imediato), nada fazendo para que tal não ocorra.

1 International Data Corporation.

Além de serem um problema real, as perdas de informação podem representar um custo muito elevado para as organizações. De acordo com o estudo Information Protection and Control (IDC, 2010), 26% das empresas refere que eventos de perdas de informação tiveram um custo superior a $100.000!

Figura 2 – Custo de perdas de informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

A perda de informação tem um custo direto (Kolodgy, 2011): a propriedade intelectual ou a informação industrial perdida na fuga, assim como a gestão das consequências desta. Tem também um conjunto de custos indiretos[2], como: perda de credibilidade no mercado, perda de propriedade intelectual que pode levar à erosão de vantagens competitivas, e a falha de cumprimento com determinada legislação.

Definição do Problema

Hoje em dia pouca ou nenhuma informação em papel está envolvida nos processos centrais das organizações. A informação crítica de negócio está cada vez mais no formato digital. Estudos recentes mostram que a tendência de crescimento da informação em formato digital é exponencial e vai atingir os 35 Zettabytes[3] em 2020.

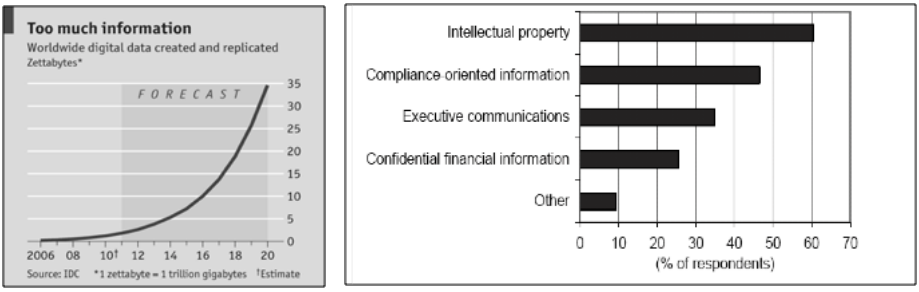
A crescente consciencialização dos riscos das fugas de informação foi despoletada por uma série de escândalos em que informações confidenciais foram divulgadas. Tal como a maioria desses casos demonstra, essas fugas são, muitas vezes, não o resultado de ações mal intencionadas, mas antes de ações de colaboradores que, sem o saberem, põem as suas organizações em risco. Isto pode acontecer quando colaboradores enviam para o exterior *e-mails* que contêm ficheiros ou documentos sem estarem cientes de que estes contêm informação confidencial. Outros exemplos são os

2 csSECURE, uma ferramenta da autoria da Critical Software.

3 1 Zettabyte = 1 Bilião de Gigabytes

colaboradores carregarem ficheiros com informação confidencial para as suas contas de *e-mail web-based*, ou copiarem ficheiros para dispositivos móveis e, assim, expô-los em ambientes que não são confiáveis. Tal como tem sido mostrado em estudos recentes, cerca de 60% das fugas de informação são relacionadas com Propriedade Intelectual, o que constitui para a maioria das organizações o seu bem mais valioso.

Figura 3 – Quantidade de informação e tipos de fugas de informação:
ICD Questionário de Proteção da Informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

A segurança da informação tem sido encarada como uma tarefa que envolve a proteção da informação sobretudo de ataques externos às infraestuturas e processos das organizações. Os *standards* de segurança e as melhores práticas (*e.g.* ISO/IEC 27002: 2005) são principalmente focados na proteção de um sistema de informação de eventos de origem externa, envolvendo a segurança de processos e da infraestrutura.

As situações que se referem a seguir dão conta da inconsciência (fugas de informação) de cooperadores ao lidarem com informação e tecnologias sensíveis para as organizações:

"Deutsche Bank Loses Hertz IPO Role Because of E-Mails
"Nov. 8 (Bloomberg) – Deutsche Bank AG, Germany's largest bank, lost its spot among the underwriters of Hertz Global Holdings Inc.'s initial public offering after an employee sent unauthorized e-mails to about 175 institutional accounts."
Carol Wolf and Christine Harper – November 8, 2006 14:51 EST
http://www.bloomberg.com

"MoD loses more laptops, USBs and 'secret files' (UK)
The Ministry of Defence has revealed that 658 laptops have been stolen over the past four years (…) The department also disclosed 121 of its USB memory sticks, some containing sensitive information, have been lost or stolen since 2004".
Siobhan Chapman | Published 17:06, 18 July 08
http://www.computerworlduk.com

> *"**Ponemon Institute Survey Finds 90 Percent of Businesses Fell Victim to Cyber Security Breach at Least Once in the Past 12 Months (…)***
> *A survey of US IT and IT Security professionals, conducted independently by Ponemon Institute and sponsored by Juniper Networks (NYSE: JNPR), found the threat from cyber attacks today is nearing statistical certainty and businesses of every type and size are vulnerable to attacks. (…) Overall, companies indicate that security breaches have cost them at least half a million dollars to address in terms of cash outlays, business disruption, revenue losses, internal labor, overhead and other expenses. Most respondents (59 percent) report that the most severe consequence of any breach was the theft of information assets, followed by business disruption (…) only 11 percent of respondents know the source of all network security breaches…"*
>
> NEW YORK, NY, Jun 22, 2011 (MARKETWIRE via COMTEX) – NExTWORK CONFERENCE – http://investor.juniper.net

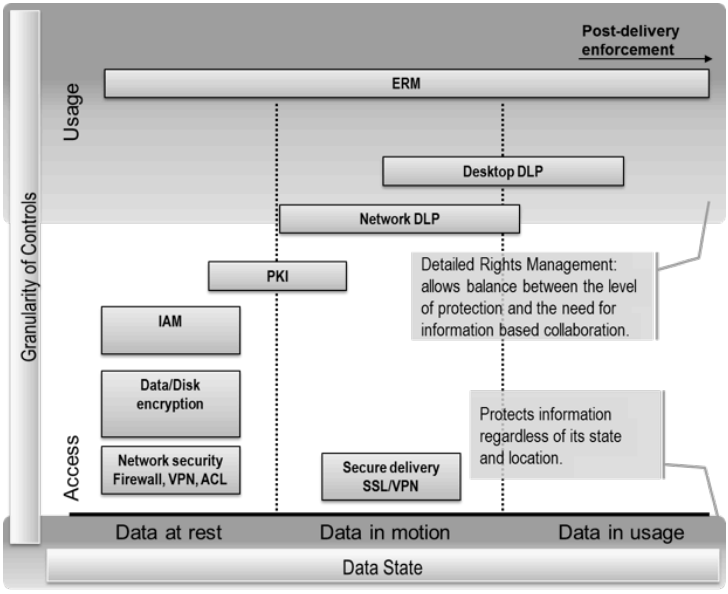
Afinal, proteger sistemas, infraestruturas e processos já não é, de todo, suficiente. As organizações devem proteger a informação em si mesma e assegurar que ela está bem protegida contra acesso não autorizado, independentemente do seu estado ou localização!

Solução de Alto Nível

A fim de evitar fugas de informação, esta deve estar protegida contra acessos não autorizados. A única forma de o assegurar é usar uma solução que aplique proteção persistente à informação e que viaja com ela, assegurando que os dados são protegidos independentemente do seu estado ou localização. Estas são soluções de segurança centradas nos dados.

Ao analizar a taxonomia das técnicas mais relevantes de segurança da informação (apresentadas na figura seguinte) é fácil perceber que a maioria das tecnologias foca-se na proteção dos dados num estado específico: em repouso – enquanto estão armazenados num computador ou disco rígido de rede; em movimento – quando estão a circular através da rede entre dois utilizadores ou máquinas; e em uso – quando estão a ser acedidos (a ser lidos, editados, imprimidos, etc.) pelos utilizadores.

Figura 5 – Taxonomia das tecnologias de segurança da informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

Pelo menos dois tipos de soluções de segurança têm uma maior visibilidade, tendo em conta a sua cobertura em termos de estados dos dados e funcionalidades: ERM e o DLP.

Enterprise Rights Management

Enterprise Rights Management – ERM – é uma tecnologia de segurança que aplica encriptação permanente aos dados, assegurando que a informação é protegida independentemente de estar em repouso, em movimento, ou em uso. Mesmo quando está a ser usada, a informação só é desencriptada na memória do computador e disponibilizada para a aplicação que a pretende usar. Enquanto a informação protegida por ERM está em uso, o ERM também aplica direitos detalhados sobre a sua utilização (bloquear certas ações como: imprimir, copiar para a área de transferência, exportar para outro formato, reencaminhar um *e-mail*, etc.).

Data Loss Prevention

As tecnologias de *Data Loss Prevention* – DLP – incluem uma ampla gama de soluções desenhadas para descobrir, monitorizar, proteger e controlar informação

sensível encontrada nos dados em repouso, dados em movimento, e dados em uso. Os sistemas são desenhados para detetar e prevenir o uso e a transmissão não autorizada de informação confidencial.

As soluções DLP baseadas na rede são normalmente instaladas no *gateway* corporativo. Estas soluções analizam o tráfego da rede como o *e-mail*, mensagens instantâneas, FTP, ferramentas *web-based* (HTTP ou HTTPS), e aplicações *peer-to-peer,* para detetar fugas de informação confidencial.

Soluções locais de DLP são normalmente instaladas em computadores de secretária, portáteis, dispositivos móveis, *pens* USB, servidores de armazenamento/ficheiros e outros tipos de repositórios de dados. Esta abordagem também inclui soluções que fornecem extração de dados e capacidades de classificação.

Soluções DLP de extração de dados são desenhadas para descobrir informações sensíveis em computadores de secretária, portáteis, servidores de ficheiros, bases de dados, gestores de documentos e registos, repositórios de *e-mail* e conteúdo e aplicações Web.

ERM *vs* DLP

Na tabela seguinte as vantagens e as desvantagens de cada tecnologia são apresentadas. Uma análise rápida revela que as desvantagens do DLP são exatamente as vantagens do ERM, e vice-versa.

Figura 6 – ERM vs DLP

	DLP	**ERM**
Sensibilização ao conteúdo	Descoberta de informação de conteúdo sensível e classificação	Não
Nível de imposição das políticas	Cumprimento ao nível do ficheiro, baseando-se em fatores tais como o tipo de dados; quando, onde e como podem ser acedidos; destinatários autorizados; tipo de informação	Persistente, proteção baseada na encriptação ao nível dos dados, independentemente de onde e por quem vão ser manuseados.
Nível de envolvimento do utilizador	Automático	Dependente do utilizador
Cobertura do ciclo de vida da informação	Aplicada apenas no acesso e utilização dos dados	Aplicada na criação dos dados e forçada através de todo o ciclo de vida da informação, incluindo proteção após transmissão da informação.

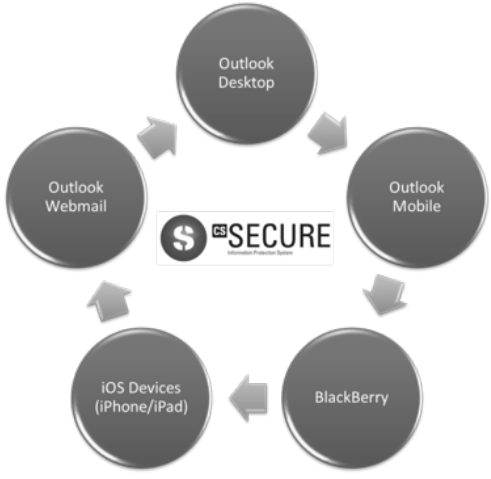
Há soluções que fornecem funcionalidades conjuntas de ERM e DLP, tirando partido dos pontos fortes de cada tecnologia de segurança. Entre empresas portuguesas que o fazem, são exemplo a *Critical Software* com o *software* csSSECURE.

Uma Solução de Segurança Centrada nos Dados

Entre outras soluções, seria interessante encontrar uma solução de proteção de informação integrada e transparente, que implemente o modelo de segurança multinível, permitindo que os utilizadores produzam informação usando as ferramentas de produtividade mais comuns (*office*, *e-mail*, dispositivos móveis, servidores de conteúdo, etc.).

Considera-se que a informação deve ser continuamente protegida. Ações como abrir, imprimir, editar, copiar, exportar, responder, reencaminhar devem ser ativadas ou desativadas de acordo com os direitos do utilizador sobre essa mesma informação. O *software* csSECURE conseguiu estes desideratos. Com ele a informação é protegida através de um algorítmo de encriptação permantente e os direitos que cada utilizador tem sobre a informação, são controlados durante o acesso.

Figura 7 – Plataformas de *e-mail* suportadas pelo csSECURE



Este *software* é baseado no modelo de segurança multinível que foi desenvolvido no mundo militar e assenta nas seguintes premissas:

- Toda a informação produzida numa organização é classificada de acordo com o seu nível de confidencialidade (e.g. interno, reservado, confidencial, secreto, …);

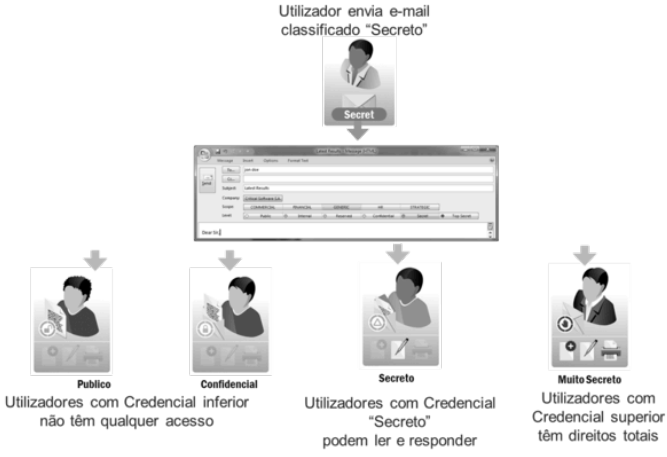
- Uma credencial de segurança é concedida a cada utilizador na organização;
- O acesso a informação classificada num determinado nível é apenas concedido a utilizadores com, pelo menos, uma credencial específica (*e.g.* informação classificada como confidencial apenas é acessível a utilizadores com a credencial confidencial ou superior).

O sistema csSECURE eleva este conceito base a um novo nível, adicionando duas novas derivadas:

- Quando é concedido acesso à informação a um utilizador, apenas certos direitos estão disponíveis para que este possa manipular os dados (e.g. o utilizador pode ser capaz de ler e editar a informação, mas tem as funcionalidades de imprimir ou copiar desativadas);
- Os níveis de classificação da informação podem ser agrupados em âmbitos de informação e estes em unidades organizacionais (e.g. a organização fictícia "Critical House" pode conter dois âmbitos [financeiro e gestão], e o âmbito financeiro pode conter três níveis de segurança: "secreto", "confidencial" e "reservado"). Este facto permite que utilizadores com diferentes perfis tenham acesso diferenciado à informação em função do seu âmbito (*e.g.* um utilizador poderá aceder a informação até ao nível "confidencial" num âmbito e apenas nível "reservado" nos restantes).

Neste tipo de abordgem o csSECURE permite a definição e a implementação de políticas de segurança da informação para gerir os direitos dos utilizadores de manipular e aceder à informação, de forma a mitigar o risco de ações não autorizadas sobre a informação, intencionais ou não. Um exemplo de políticas de segurança na solução csSECURE é apresentado na imagem seguinte.

Figura 8 – Exemplo de segurança multinível



Capacidades de Monitorização

As ações dos utilizadores sobre a informação protegida devem estar sujeitas a registo. Isto permite ao auditor de segurança saber, por exemplo, quais os ficheiros ou *e-mails* produzidos por cada utilizador e quando e como estes foram acedidos por outros.

No caso do *software* csSECURE por cada ficheiro ou *e-mail* protegido, o sistema gera um identificador único. Este identificador único pode ser usado para rastrear o ciclo de vida de um documento específico, obtendo todas as ações registadas sobre esse documento.

Este identificador único também pode ser usado para gerir uma lista negra de documentos, sendo que qualquer acesso posterior a estes documentos será negado. Isto é particularmente útil para gerir falhas de segurança identificadas dentro da organização e evitar acessos indevidos. Como a informação é permanentemente encriptada, o seu acesso depende de um processo de validação no servidor. Uma vez que o *software* está totalmente integrado com o sistema de ERM, é possível autorizar ou negar acesso a documentos individuais.

Porém, qualquer ferramenta de segurança de informação na sua própria configuração do sistema pode representar uma quebra de segurança porque o administrador pode conceder a utilizadores específicos direitos de acesso à informação da organização ou remover esses direitos. Para prevenir e monitorizar erros de administração, no csSECURE todas as tarefas de administração são registadas centralmente para auditorias futuras.

Identidade Avançada e Gestão de Acessos

É importante prevenir a perda de dados, aplicando à informação produzida dentro da organização técnicas de segurança. O csSECURE centra-se nos dados. Na maioria dos produtos de segurança, a identidade digital dos utilizadores no sistema é representada pelo *login* do utilizador. Se um utilizador ilegítimo assumir a identidade digital de um outro utilizador, este ganha acesso a todas as informações que deviam ser apenas disponíveis para o utilizador legítimo. A usurpação de identidade é um dos principais problemas em todas as soluções na área da segurança.

Os mecanismos de autenticação utilizados atualmente oferecem um nível razoável de proteção contra intrusos. No entanto, autenticação baseada em palavras-chave, ou até soluções de "autenticação forte" são fracas. Depois da fase de autenticação, não é necessária qualquer outra prova de identidade. Estes mecanismos possibilitam ataques oportunistas, especialmente de pessoas ligadas à organização

(*e.g.* deixar o computador ligado enquanto se está numa pausa para café ou em horário de almoço é uma oportunidade de ataque).

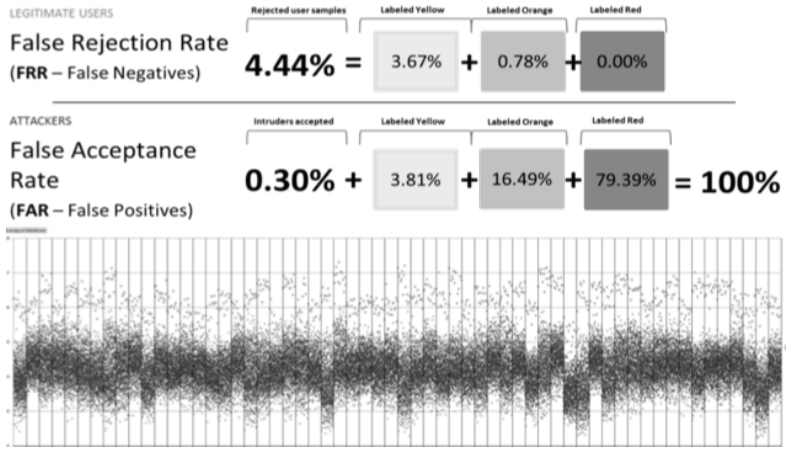
De maneira a prevenir a usurpação de identidade, necessitamos de uma técnica que contínua e passivamente monitorize as interações do utilizador, procurando indícios de intrusão. As soluções de Sistemas de Deteção de Intrusão Locais (*Host-based Intrusion Detection Systems*) satisfazem a maioria dessas condições; no entanto, as soluções atuais são focadas no sistema ao invés do utilizador. Ações que não ponham em causa a integridade do sistema são consideradas legais mesmo que executadas por utilizadores ilegítimos, pelo que continua a ser muito fácil executar ações prejudiciais e continuar indetetável.

Talvez uma das técnicas mais ajustadas será a identificação de características biométricas. O csSECURE dispõe de uma tecnologia, patenteada, que a realiza monitorizando as interações dos utilizadores com o computador, estendendo o conceito de IDS (Sistema de Deteção de Intrusões) para o nível de autenticação. O *Keystroke Dynamics* (que em português podemos apelidar de "dinâmica de digitação") é a técnica biométrica comportamental que satisfaz esta condição e que consiste na identificação e análise de padrões na atividade de digitação dos utilizadores, por forma a criar os seus perfis biométricos.

- Padrões de digitação estão continuamente a ser recolhidos após a fase de autenticação (providenciando autenticação contínua);
- É não intrusiva e transparente (a rotina do utilizador não é incomodada);
- É económica, dado que não necessita de nenhum equipamento especial.

Os resultados atuais da utilização desta tecnologia asseguram uma precisão de 99,7%.

Figura 9 – Eficácia do sistema de deteção de intrusos



Para melhor enquadrar o significado da Figura 9, seguem-se as definições de FRR e FAR.

- *False Rejection Rate*: probabilidade do sistema rejeitar indevidamente uma tentativa de acesso de um utilizador autorizado.
- *False Acceptance Rate*: probabilidade do sistema aceitar indevidamente uma tentativa de acesso de um utilizador não autorizado.

Pode-se então aferir que a solução rejeitou o acesso a 4,44% de utilizadores legítimos, sendo que a maioria desse valor (3,67%) apresenta variações muito ligeiras em relação ao seu modo de teclar mais comum. Por outro lado, apenas 0,3% utilizadores não autorizados foram aceites pela solução como sendo válidos.

Benefícios

A utilização de *software* desta natureza aumenta a consciencialização para a problemática da segurança da informação nas organizações, reforçando a necessidade de implementação de políticas de segurança, enquanto fornece às organizações meios para auditar e identificar falhas de segurança, reconhecendo tendências comportamentais e possíveis violações.

No caso do csSECURE são encontrados os seguintes benefícios:

Data Loss Prevention – aplicar políticas de segurança e regras na organização ajuda a prevenir, de maneira eficaz, a fuga de informação. As funcionalidades DLP permitem a aplicação de políticas de segurança, tais como a proteção automática de todos os ficheiros enviados via correio eletrónico ou transferidos para unidades externas.

Enterprise Rights Management - direitos detalhados sobre informação privilegiada, que bloqueia tentativas de fuga ou uso incorreto da informação interna para o exterior da organização. Ações como impressão, cópia, exportação para diferentes formatos ou reencaminhamento podem ser restringidas.

Gestão de políticas centralizada – Toda a gestão de políticas de segurança de informação é feita centralmente, através de uma consola *web.* É possível a transposição direta de políticas de segurança de informação e de procedimentos, assim como a importação de papéis e dados de perfil provenientes do diretório de utilizadores da organização.

Ampla gama de aplicações – O *software* suporta uma ampla gama de aplicações de produtividade e é facilmente extensível. A informação é encriptada de forma transparente e é acessível e eficazmente protegida na maioria das aplicações do *Office* utilizadas atualmente nas organizações. A informação está protegida, não interessando o local onde está armazenada, através de que canais foi transmitida ou onde está a ser acedida. Total proteção em repouso, em movimento e em utilização.

Sistema de deteção de intrusão do utilizador (inclui um sistema de deteção de intrusões que assegura uma taxa de confiabilidade de 99%. Esta técnica de biometria comportamental assegura uma autenticação contínua, é económica (não necessita de qualquer equipamento adicional) e é não-intrusiva, dado que não interfere nas tarefas normais do utilizador.

Capacidades de monitorização avançada – É possível monitorizar com detalhe o acesso à informação, o que possibilita que os auditores identifiquem desvios às políticas de segurança implementadas pelas organizações, detetando tendências comportamentais, configurando alarmes e medidas de prevenção. Permite que a organização obtenha uma panorâmica geral da utilização da informação.

Ciclo de vida da informação protegida – Com um identificador único de cada ficheiro e *e-mail* protegido é possível rastrear todos os acessos aos dados, analisando todo o ciclo de vida da informação protegida. Com base nesta funcionalidade, também é possível bloquear qualquer acesso a um ficheiro/*e-mail* específico, através da criação e gestão de uma lista negra.

Registos para auditoria dos administradores – A gestão do sistema permite dar acesso à informação a utilizadores não autorizados e modificar políticas de acesso e regras de DLP. Inclui um registo de todas as ações do administrador, prevenindo e monitorizando todos os possíveis erros de administração.

Considerações Finais

As soluções de segurança utilizadas atualmente são, tipicamente, centradas na rede ou na máquina, com objetivo de proteger a informação de ataques exteriores (*hackers*, vírus, cavalos de troia, etc.), mas falham no que diz respeito à segurança contra fugas de informação. De acordo com estudos recentes do IDC, as fugas de informação são maioritariamente acidentais (mais de 50%), e na maioria das vezes, para 26% das empresas, estes problemas podem significar custos diretos superiores a 100.000 US$.

As técnicas mais promissoras para controlar a fuga de informação são: ERM (*Enterprise Rights Management*) e DLP (*Data Loss Prevention*). ERM assegura que os dados são protegidos independentemente do seu estado (em repouso, em movimento ou em utilização), possibilitando também a criação de direitos detalhados para a informação (direito a imprimir, copiar, editar, exportar, responder, reencaminhar, etc.). O DLP assegura que as políticas da organização para lidar com informação digital são cumpridas por todos os utilizadores, definindo regras sobre a maneira como a informação deve ser manuseada e armazenada (*pen-drives*, *e-mail*, servidores da organização, etc.).

As desvantagens das soluções ERM (dependência do utilizador, carência de classificação automática e complexidade de administração) são precisamente as vantagens dos produtos baseados em DLP. O csSECURE, um produto com origem numa empresa portuguesa, é uma combinação das abordagens ERM e DLP, baseando-se no conceito de segurança multinível, que protege efetivamente as organizações contra fugas de informação permitindo, ao mesmo tempo, manter o controlo e monitorizar as ações executadas pelos utilizadores sobre a informação da organização, possibilitando rastrear a informação ao longo de todo o seu ciclo de vida.

Referências

International Data Corporation, IDC (2010). *Information Protection and Control*. Disponível em www.idc.com.

Kolodgy, Charles J. (2011). *Effective Data Leak Prevention Programs: Start by Protecting Data at the Source*. Framingham, MA: IDC Corporate USA.

Extra Dossiê

African Peace and Security Architecture: a Strategic Analysis

Luís Falcão Escorrega

Major de Infantaria. Professor de Estratégia e investigador no Instituto de Estudos Superiores Militares. Licenciado em Ciências Militares pela Academia Militar; Pós-graduado em Estudos da Paz e da Guerra nas Novas Relações Internacionais pela Universidade Autónoma de Lisboa; Pós-graduado em Estratégia pelo Instituto Superior de Ciências Sociais e Políticas; Curso de Estado-Maior em Portugal e nos EUA; Master of Military Art and Science in Strategic Studies no Command and General Staff College, nos EUA.

Resumo

Arquitetura de Paz e Segurança em África: Uma Análise Estratégica

Este é um estudo descritivo no campo dos estudos estratégicos, centrado numa abordagem holística dos diversos mecanismos e objetivos da Arquitetura de Paz e Segurança Africana (APSA). A intenção é analisar os mecanismos desenvolvidos (ou em fase de desenvolvimento) pela UA e pelas organizações regionais africanas para abordar questões de paz e segurança em África, com o objetivo último de contribuir para uma melhor compreensão do contexto de segurança africano ao nível estratégico. Ao utilizar o modelo estratégico Ends-Ways-Means, este estudo conclui que a APSA é uma estratégia de segurança viável para lidar com as principais ameaças em África.

No entanto, há ainda lacunas importantes e sua eficácia depende de três ingredientes fundamentais: a vontade política dos Estados membros da UA, os desenvolvimentos ao nível regional, e do tratamento das ameaças externas de uma forma muito mais consistente, abrangendo a dimensão "de segurança" da APSA na mesma extensão que a sua dimensão "de paz".

Abstract

This is a descriptive study in the realm of strategy, focused on creating a holistic and meaningful picture about the mechanisms and purpose of the African Peace and Security Architecture (APSA). The overall intent is to analyze the mechanisms developed, or in a developing stage, by the African Union (AU) and regional organizations to address peace and security issues in Africa, with the ultimate goal of contributing to a better understanding of African security context at the strategic level. By using the strategic model of Ends-Ways-Means, this study concluded that the APSA is a viable security strategy to deal with the principal threats in Africa. However, there are still important shortcomings and its effectiveness is dependent upon three critical ingredients: political will of AU Member States, developments at the regional level, and by addressing the external threats much more consistently, covering the security dimension of the APSA in the same extent of its peace dimension.

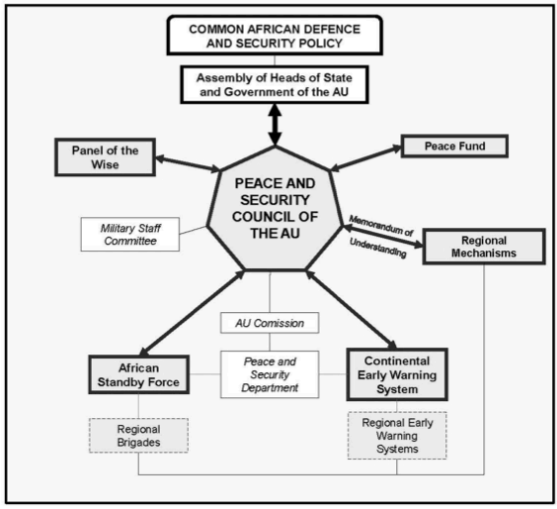
Introduction

The security architecture in Africa has evolved considerably over the past forty years. In the past, regional and sub-regional African organizations expended most of their time dealing with the aftermath of conflicts instead of prevention and early resolution. The creation of the African Union (AU) in 2002 was the most significant step towards achieving a continental collective security system, enabling African countries to unite in seeking and developing collective solutions to prevent and mitigate conflicts. The AU rejected the approach of its predecessor (Organization of African Unity – OAU) – of absolute respect for national sovereignty – and adopted a new policy in which the responsibility to protect human and people's rights, and the right to intervene in a Member State are enshrined in the Constitutive Act, the basis of the new security architecture[1] (Vines and Middleton, 2008: 8).

The Constitutive Act established provisions for intervention in the internal affairs of a Member State through military force, if necessary, to protect vulnerable populations from human rights abuses. Implicit in these provisions is the concept of human security and the understanding that sovereignty is conditional and defined in terms of a State's capacity and willingness to protect its citizens (Powell, 2005: 1). In order to provide an operational dimension to the security provisions of the Constitutive Act, the AU developed capacities for early warning, quick reaction, conflict prevention, management and resolution. At the same time, it placed "itself within a robust security system that builds on the strengths of African regional organizations and the United Nations (UN), and that draws on extensive support from other international actors" (Powell, 2005: 1).

1 The first reference to this concept is in the Protocol that established the Peace and Security Council of the AU, in 2002, in his Article 16, naming it the "overall security architecture of the Union".

Figure 1 – The African Peace and Security Architecture



Source: Created by the author.

This new African Peace and Security Architecture (APSA) pursues African solutions to African problems. The APSA is grounded on two pillars: the Common African Defense and Security Policy (CADSP)[2] and the Peace and Security Council (PSC)[3] (see figure 1). To fulfill its tasks, the PSC has three primary instruments at its disposal: the Panel of the Wise (PW), the Continental Early Warning System (CEWS) and the African Standby Force (ASF). These three instruments, together with a special fund for financing missions and activities related to peace and security (the Peace Fund) and the Regional Mechanisms for Conflict Prevention, Management and Resolution, round out the elements of the APSA.

A Strategic Analysis

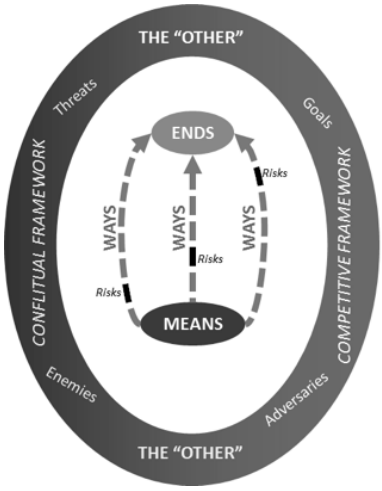
The APSA is a very complex security system, relying on regional and continental intergovernmental organizations, on the will of African peoples and on the support of a countless number of partners. Covering all processes that are underway in the APSA with the appropriate level of depth is a colossal task. The strategic

2 AU's central policy document on security, signed in 2004.
3 AU's most important organ on security issues.

model *Ends-Ways-Means* provides the adequate paradigm to analyze the strategic importance of the APSA. It allow to describe and analyze the suitability of the Ends established for the APSA, particularly the extent of its contribution for the accomplishment of the desired effect of promoting and consolidating peace and security on the African continent.

In addition, it describes and analyzes the application of the four classic strategic *Ways* – diplomatic, military, informational and economic – to the particular case of the APSA, as well as its respective *Means*. *Ways* and respective *Means* are analyzed together to scrutinize its overall feasibility (e. g. the extent in which the *Ways* can be accomplished by its *Means*). In order to do that it is indispensable to analyze the development stage of each of the *Means*: Diplomatic (PSC, Commission and PW), Military (ASF), Informational (CEWS) and Economic (Peace Fund).

Figure 2 – The Ends-Ways-Means Strategic Model



Source: Created by the author.

The Ends of the APSA

In the realm of strategy, Ends are objectives or goals that answer the question of "what" one is trying to achieve. The CADSP, signed in 2004, is essentially a strategy based on a set of principles, objectives and instruments with the overall desired effect of promoting and consolidating peace and security on the continent (Touray, 2005: 636). The CADSP establishes the security strategic goals for the APSA (AU,

2004: 8). They are "essentially to respond to both internal and external threats effectively" (Touray 2005: 643). The CADSP classifies internal and external threats as dangers to the common defense and security interests of the continent, undermining the maintenance and promotion of peace, security and stability (AU, 2004: 3).

Table 1 – Main African Common Security Threats

Internal Threats	External Threats
• Inter-state conflicts/tensions (including situations that undermine the sovereignty and territorial integrity); • Intra-state conflicts/tensions (including war crimes, genocides, and coup d'états); • Unstable post-conflict situations; • Grave humanitarian situations, as well as other circumstances (including violent and other crimes, including organized and cross border crimes). *(Note: Twenty-two (22) different threats are labeled as Internal Threats in the CADSP)*	• External aggression, including the invasion of an African country; • International conflicts and crises with adverse effects on African regional security; • Mercenaries; • International terrorism and terrorist activities; • The adverse effect of globalization and unfair international political and economic policies, practices and regimes; • The accumulation, stockpiling, proliferation and manufacturing of weapons of mass destruction, particularly nuclear weapons, chemical and biological weapons, unconventional long-range and ballistic missiles; • Cross-border crimes such as drug and human trafficking (which may constitute a threat at the regional and national levels); • Unilateral policies aimed at isolating African countries; • Dumping of chemical and nuclear wastes in Africa.

Source: African Union (2004).

Analyzing these threats, some inferences can be drawn. First, the internal threats are related to the peace dimension of the APSA (addressing conflicts) and the external threats are related with to the security dimension (addressing other security threats). Second, the number of threats identified in the CADSP is very high. The document identifies thirty-one different threats to the common defense and security interests of the continent. Although these threats are grouped into internal[4] and external to the African continent, they are extremely diverse (in its nature, capabilities or intentions) making it very complex and challenging to find balanced Ways and Means to mitigate all of these threats.

Third, most of these threats are interconnected and affect the development and security of the continent. In today's strategic context, in Africa or elsewhere, situations and problems such as terrorism, civil wars, organized crime or extreme

4 The internal threats are organized in four clusters: inter-state conflicts/tensions; intra-state conflicts/tensions; unstable post-conflict situations; and grave humanitarian situations, as well as other circumstances.

poverty, are interrelated and cannot be addressed separately. In order to mitigate all these threats, comprehensive approaches are required, overcoming narrow preoccupations and working across the whole range of issues, in a coordinated and integrated way.

Fourth, The CADSP does not specifically addresses maritime or cyber security threats. These two types of threats pose dangers to the security interests of the African continent, undermining the promotion of security and stability. As one can see in the Gulf of Aden or in the Gulf of Guinea, issues like illegal fishing, piracy, arms and drugs trade, oil bunkering or sea pollution, are extremely dangerous threats that require strategic mitigation. Likewise, cyber security threats have an enormous destabilizing potential. The low cost and virtual nature of cyber space makes it an attractive domain for use by those who seek to use cyber space for malicious purposes. As Internet penetration rates increase across the African continent, so does the risk of cyber-attacks, which threatens the protection of financial information, personal data, and intellectual property.

The Ways and Respective Means

In the strategic model, *Ways* are courses of action that explain "how" the *Means* will be used, and *Means* are the resources or instruments that will be used to execute the strategic concept defined by the different *Ways*. The *Ways* and *Means* analyzed in this section are related by its nature: the diplomatic *Way* with the PSC, the Commission, and the PW; the military *Way* with the ASF; the informational *Way* with the CEWS; and the economic *Way* with the Peace Fund.

The Diplomatic Ways and Means

The Protocol that created the PSC establishes in its Article 6 two primary diplomatic Ways to achieve the strategic goals: preventive diplomacy and peacemaking, particularly by the "use of good offices, mediation, conciliation and enquiry" (AU, 2002: 8). Preventive diplomacy strives to resolve a dispute before it escalates into violence. Peacemaking, generally, seeks to promote a ceasefire and to negotiate an agreement.

The APSA is based on a paradigm that recognizes preventive diplomacy as central to address peace and security challenges in Africa. African Leaders consider that the comprehensive and coherent use of preventive diplomacy is important in creating the conditions for sustainable peace. According to South Africa President, Jacob Zuma, preventive diplomacy initiatives are more cost-effective than

the deployment of peacekeepers once a conflict has broken out. Therefore, it is essential that the "efforts of both the African Union and the numerous sub regional organizations across the continent working on preventive diplomacy be respected and supported by the UN and the international community as a whole" (Zuma, 2011: 6).

The other diplomatic Way established by the Protocol is based on the use of diplomatic methods, mainly mediation, good offices, conciliation and enquiry. All four methods are anchored in Article 33 of the Charter of the UN, under its Chapter VI, *Pacific Settlement of Disputes*. Mediation processes have often been employed in attempts to resolve conflicts on the African continent. In recent years, the AU and sub-regional organizations have played an important role in mediating hotspot issues in Africa, namely in the Sudan, Burundi and Madagascar. "Their success shows that regional and sub-regional organizations have unique political, moral and geographic advantages in preventing and resolving local conflicts" (Jiechi, 2011: 16).

However, the APSA still requires an institutionalization of mediation processes. In order to move from *ad hoc* mediation initiatives to more institutionalized and systematic ones the AU peace and security agenda needs to enhance its mediation mechanisms and processes. "Partnerships among African states; between the AU and regional organizations; the AU, EU and UN; and between AU and civil society organizations are important in order to ensure that there is cooperation, coordination, joint solutions and support among and within the actors in the field of conflict resolution and mediation" (ACCORD, 2009: 34).

The Peace and Security Council

The PSC is the central diplomatic instrument of the APSA. It is the point of contact with international organizations such as the UNSC and the Political and the Security Committee of the EU. The Protocol relating to its creation establishes that the PSC performs functions in the areas of preventive diplomacy and peacemaking, including the use of good offices, mediation[5], conciliation and enquiry (AU, 2002: 8). It is empowered to take diplomatic initiatives and action it deems appropriate with regard to situations of potential and actual conflicts. To that end, it uses its discretion to affect entry, whether through the collective intervention of the Council or through its Chairperson and/or the Chairperson of the Com-

5 An example of using mediation: through a PSC decision, the AU assumed the political responsibility of mediating between the government of Sudan and armed resistance movements the Justice and Equality Movement and the Sudan Liberation Army.

mission, the PW, and/or in collaboration with regional mechanisms for conflict prevention, management and resolution (AU, 2002: 14). The PSC may establish subsidiary bodies that include *ad hoc* committees for mediation, conciliation or enquiry, consisting of an individual State or group of States (AU, 2002: 12).

The PSC has become a focus of "collective security decisions by African for Africans" (Sturman and Hayatou, 2010: 57). In response to urgent security issues, it has been able to act more decisively than the larger Assembly of 53 Member States of the AU and has shifted the AU from a tradition of non-interference in domestic affairs to a new approach, using sanctions and more assertive regional diplomacy (Sturman and Hayatou, 2010: 57). The focus of the decisions, so far, has been on conflict management and resolution, rather than conflict prevention[6]. This is due to capacity constraints and the intensity and complexity of conflicts, but also to a lack of political will, reflecting the power politics and interests in Africa (Sturman and Hayatou 2010, 69). Consensus[7] has remained the norm by which all decisions have been reached. This mode of decision-making seems not only time-consuming, but by institutionalizing it, it allows Member States with a strategic interest in a particular conflict to block some kind of intervention (Sturman and Hayatou, 2010: 69).

It is important to highlight that in just eight years the PSC has made significant achievements in addressing the various conflict and crisis situations and has significantly improved its methods. However, the PSC faces still important challenges. PSC authorizations to deploy peacekeepers to Burundi (AMIB), Comoros (AMISEC), Sudan (AMIS) and more recently Somalia (AMISOM) exposed a major gap between the PSC's willingness to authorize such missions and the AU's ability to implement them. Shortage of resources--human and material--has emerged as a major shortfall. This mandate-resource gap may in the long run erode its credibility (AU, 2010a: 26). Additionally, there has been some lack of interaction between the PSC and other APSA components, primarily due to the fact some of the components are still being operationalized (AU, 2010a: 31). Institutionally, the PSC is mandated to work with the Chairperson of the Commission; a link between the PSC and the PW is missing (AU, 2010a: 28).

6 "Nor has the PSC devoted much attention to the nonmilitary dimensions of security, such as environmental degradation, organized crime, and disease. This limited focus is the result of analytical and operational capacity deficiencies, as well as the regularity of hot crises, which makes it difficult for the PSC to tackle the upstream and structural aspects of conflict mitigation" (Williams, 2011: 7).

7 The PSC decisions are generally based on the principle of consensus. However, in case of failure to reach a consensus, decisions on procedural matters are by a simple majority and substantive matters by a two-thirds majority of members eligible to vote (Sturman and Hayatou, 2010: 66).

The Diplomatic Role of the AU Commission

The AU Commission has a very important diplomatic role within the APSA. Under the authority of the PSC, and in consultation with all parties involved in a conflict, the Chairperson of the AU may deploy efforts and take all initiatives deemed appropriate to prevent, manage and resolve conflicts. Therefore, at his own initiative or when requested by the PSC, he may use his good offices, either personally or through special envoys, special representatives, the PW or the Regional Mechanisms, to exercise diplomatic efforts (AU, 2002: 15).

The principal operational mechanism of mediation at the AU is, in fact, the Commission. It implements mediation interventions and takes decisions regarding their composition and nature. The mediation efforts have so far taken the form of *ad hoc* deployment of special envoys in identified conflict areas on the continent, with the support from the Conflict Management Directorate of the Commission (ACCORD, 2009: 10).

The Panel of the Wise

The creation of the PW was motivated by the need for finding homegrown solutions to African challenges, and by the African cultural belief of the wisdom, discretion and trustworthiness of elders. Within this cultural framework, similar structures are being developed in the REC's.

The PW can diplomatically intervene in crises through several ways. It can be by facilitating the establishment of channels of communication between the AU and parties engaged in a dispute; by carrying out fact-finding missions; by conducting shuttle diplomacy between parties; by encouraging parties to engage in political dialogue; carrying out reconciliation processes; or by assisting and advising mediation processes. The PW selects up to three critical crisis situations per year, which it will monitor constantly (Abdellaoui, 2009: 6). It adopted five criteria for engaging in crisis situations.

The PW became operational in December 2007, and has met ten times since then. It is expected to meet at least three times a year, or more often if necessary. So far, its meetings have focused on three themes: election related conflicts; non-impunity, justice and national reconciliation; and women and children in armed conflicts in Africa (AU, 2010a: 56).

The PW has undertaken fruitful and important tasks in preventive diplomacy. Through confidence-building missions, the PW has engaged with several countries and regions affected by crisis or conflicts (AU, 2010a: 56). However, the PW faces some constraints. The PW does not appear in the structure of the Commis-

sion raising budgetary, ownership and sustainable issues; therefore, it does not receive any funding through the AU regular budget. All its activities and those of its Secretariat have been funded through partner support, which is an unsustainable situation and hampers its activities (AU, 2010a: 56). According to Murithi and Mwaura (2010: 82), the PW also needs staff complement,[8] namely a robust mediation support unit within the Commission and significant input from qualified political officers who have experience in bilateral and multilateral negotiation settings.

The PW faces also some challenges. First, the importance of ensuring buy-in from the rest of the APSA mechanisms as well as AU Member States; this is vital for recognizing the importance of its role and therefore for its efficacy. Second, the importance of ensuring comprehensive coordination; without it there is a danger that the activities of the PW will be routinely undermined. Third, the clarification of which stage of the diplomatic process it intervenes and whether the PW will be empowered and appropriately staffed by the AU and its partners to fulfill its mandate effectively. "A pragmatic appreciation of the nexus between preventing conflicts, making peace once conflicts have escalated, and keeping peace following agreements will determine how effective the PW will be" (Murithi and Mwaura, 2010: 90).

It seems that the PW has the potential to be the most innovative and effective diplomatic Means of the APSA. Not only because was conceived within the cultural framework of the African continent, but also because it is not (or should not be) constrained by the political considerations of the Commission or the PSC.

The Military Ways and Means

The Protocol that created the PSC establishes in Article 13 two primary generic military ways to achieve the strategic security goals: peace support missions and military intervention. These two primary ways are divided in seven possible methods (AU, 2020: 19).

Both ways are primarily focused on the internal threats. It is important to note that in any relevant strategic document of the APSA[9] are defined military ways of dealing with external threats, such as terrorism or cross-border crimes. This is corroborated by the existing scenarios for employing the ASF, ranging from small-scale

8 The Panel's Secretariat has only two professional staff and an administrative assistant for its eleven core functions (AU, 2010: 57).

9 Such as the Protocol that creates the PSC or the *Solemn Declaration on a Common African Defense and Security Policy.*

observation missions to forcible military intervention. These scenarios focus on peace support operations and do not authorize the ASF to engage with external threats or other security challenges, such as those associated with antipiracy and maritime security. This land-focused approach can be too narrow for addressing all the dimensions of a complex peace-support operation, as the case of Libya demonstrated.

In addition, the participation in humanitarian assistance or in efforts to address major natural disasters is not envisioned in the scenarios for the employment of the ASF. Generally, military organizations possess important capabilities--such as transport, logistics and the ability to deploy rapidly--to participate in disaster relief operations. The CADSP mentions that the ASF "shall provide humanitarian assistance to alleviate the suffering of the civilian population in conflict areas (as well as support efforts to address major natural disasters)" (AU, 2004: 18). However, this intention was not translated into the existing scenarios of the ASF.

So far, the AU has tended to concentrate its military responses on conflict management, rather conflict prevention, through peacekeeping and peace enforcement operations. The AU authorized military missions in Burundi, Sudan/Darfur, Somalia and Comoros. Military operations have been deployed to "supervise, observe, monitor, and verify the implementation of ceasefire agreements or to help broke cease-fires between government and rebel groups" (Söderbaum and Hettne, 2010: 22).

Military intervention is a critical issue that is addressed in the APSA. According to its Constitutive Act, the AU has "the right to intervene in a Member State pursuant to decision of the Assembly in respect of grave circumstances: namely war crimes, genocide and crimes against humanity" (AU, 2002a). Scenario 6 for the employment of the ASF addresses these situations, namely "*in genocide situations where the international community does not act promptly"* (AU, 2005: 3). Despite some legal doubts about this *right to intervene* (beyond the scope of this essay) what is critical in this issue is the political will to apply this very coercive military measure when it becomes imperative. This is true for the AU and for all other organizations, like the UNSC, that need to deal with similar, and always sensitive, situations of intervention.

The African Standby Force

The African Standby Force is the primary military instrument for implementing the decisions of the PSC. It is based on standby arrangements with the continent's five sub-regions, each providing a brigade-sized contribution, supported by civilian police and other capacities. According to a recent assessment report of the AU, released in 2010, "there is no doubt that efforts to operationalize the ASF have

registered good progress although, the degree of progress varies from region to regions" (2010a: 51). Despite achieving major progress developing the ASF, there are still significant shortcomings.

Bachmann analyzed and summarized some of these shortcomings: the AU and the regions lack mission planning capacity; the police and civilian components of the ASF remain significantly weaker than their military counterparts; communications and interoperability between military, police, and civilians in the field remain low; administrative, financial and human resources management capacity remain too weak compared to the task at hand; African missions remain heavily dependent on external support for the entire range of their logistics needs, from strategic deployment to field logistics, as well as for their CIS (communications and information systems) needs. "Financial dependence on external donors characterizes African capacity-building efforts as well as operations" (Bachmann, 2011: 13).

The AU and the sub-regions have made significant progress towards establishing a viable regional peace support capability. However, the progress and status of readiness of each of the regional brigades is different. It seems that the NASBRIG is lagging in the operationalization of the standby arrangement, despite NARC's economic and military potential of its members. This is due to the fact there was no prior collaboration among the North African States at this level. Hence, they had to create all these structures to meet the requirements of the ASF (Alghali and Mbaye, 2008: 38). In addition, the progress has been hampered by a "lack of multilateral cooperation in the region, exemplified by the Algerian-Moroccan standoff over Western Sahara" (Burgess, 2009: 3) and by the recent events in Libya.

Logistics depots are important and a basic mission capability needed for the ASF. Recently, the AU and RECs launched projects focused on improving the shortcomings of logistics depots. This effort, however, "does not seem to have gone much beyond studies to identify the appropriate locations of the depots and initial drafts of their contents and costs"[10] (Bachmann, 2011: 13).

The civilian components (including police) are still underdeveloped in all sub-regions. The civilian components are essential for addressing multidimensional peacekeeping and peace-building operations. Still, according to the AU, "these components have been put in place in all sub-regions but there are still some crucial gaps" (AU, 2010b: 51).

To date, none of the RECs and Regional Mechanisms (RMs) has signed a formal Memorandum of Understanding (MoU) with their Members for the deployment of their troops. This aspect is fundamental for the operationalization and employ-

10 Following protracted studies and political discussions, the decision to create a continental depot in Douala, Cameroon, was finally approved by the defense and security ministers in December 2010 (Bachmann, 2011: 40).

ment of the ASF, requiring that the AU, RECs and RMs adopt binding legal documents with Member States for the employment of pledged troops.

The gap between aspiration and implementation remains wide. Protocols and framework documents are in place, and institutional structures are being built; but despite recent developments, operational capacity remains limited in the face of rising demands and expectations (Cilliers, 2005: 16). In December 2010, a third roadmap was proposed by an AU specialized technical committee to focus on the steps needed to reach Full Operating Capability (FOC) for a limited Rapid Deployment Capability (RDC) by 2012, and FOC for the ASF as a whole by 2015 (AU, 2010b: 1). These are ambitious objectives. In order to achieve them, the AU and the ASF need to overcome important shortfalls and vital challenges. There are shortfalls in the areas of coordination, force composition; planning; doctrine, procedures and training; interoperability and communications; and logistics (AU, 2010b: 1). Some of these deficiencies will need better management of administrative and human resources to improve; however, the greatest resource shortfall remains internal financial contributions and dependence on external donors.

Therefore, two big challenges emerge: the first one is related to balance. Military operations, equipment and logistics are expensive. African leaders need to find a balance between investing in this continental and regional security mechanism and in the immediate challenges of governance, poverty, and development. Both dimensions are not mutually exclusive as there is no development without security.

The biggest challenge is African will and ownership. If the AU Member States really want to develop African solutions for African security problems, they need to be more pro-active and innovative. The cultural paradigm, *we do it this way, because that's the way we do it,* often inhibits appropriate and effective responses to challenges. As Cilliers pointed out, sometimes Africans "deliberately take a back seat, engaging in an old game of extracting the maximum benefit from their benefactors" (Cilliers, 2008: 18). This logically will lead to more external engagement and to less African commitment, hindering African progress and development, and therefore, African solutions. Undoubtedly, African need vast financial and technical support from donors and partners; but it is vital that the "AU and the various regions ensure that they assume ownership and drive donor support and not the other way around" (Cilliers, 2008: 18).

The Informational Ways and Means

Generally, the purposes of the informational Ways are disseminating and collecting information in order to achieve strategic objectives (Worley, 2008: 4). The protocol that created the PSC establishes that, in order to facilitate timely and ef-

ficient response to conflict and crisis situations in Africa, the information gathered through the CEWS shall be used by the Chairperson of the Commission to "advise the PSC on potential conflicts and threats to peace and security in Africa and recommend the best course of action" (AU, 2002b: 17).

The AU Informational Way – materialized by the CEWS – to achieve the AU Ends is focused on the internal threats, at least theoretically, namely on inter-state conflicts/tensions and intra-state conflicts/tensions. The Indicators Module of the CEWS, which trigger the early warning cycle (and provides the information for the strategic analysis and the engagement with decision-makers), is based on a framework of generic indicators derived *ex negativo* from documents adopted by the African Heads of State and Government (AU, 2008: 6). All those documents are directly related with conflict prevention, human rights, good governance and democracy. No indicators were developed for external threats, such as terrorism or cross-border crimes.

Despite the nature and purpose of the CEWS, there are always sensitive issues when using information related with events that occurred inside a Member State. The former Director of Peace and Security at the AU, Ambassador Sam Ibok, mentioned some of them, including: the barrier of national sovereignty, which often hampered efforts to collect reliable data and information, as well as timely intervention; the issue of data ownership, which often created problems on the flexibility of the use and dissemination of data collected; and the lack of political will on the part of Member States (Cilliers, 2005: 19). These issues are critical and must be openly addressed by the AU, if the goal is effectively mitigate internal and external threats.

The Continental Early Warning System

The CEWS is one of the key instruments of the APSA. A recent assessment report indicated that significant progress has been achieved in the operationalization of the CEWS, and the system has been able to "provide reliable and up-to-date information on potential, actual and post-conflict situations" (AU, 2010b: 32).

However, the same report mentioned before identifies important shortfalls. The level of development of each of the sub-regional early warning systems is different, hindering higher level operation. Data collection and reporting are relatively advanced at the continental level, in ECOWAS and in IGAD, but not yet effective in CEN-SAD, EAC and COMESA; in most other RECs, progress has been achieved in establishing policy frameworks, specific concepts and approaches to early warning (AU, 2010b: 33). Conflict analysis and development of response options are just beginning in some regions; only IGAD is building up an integrated response mechanism at this stage (AU, 2010b: 33). There are still technical and

financial constraints to directly link each of the RECs monitoring and observation centers to the AU Situation Room (AU, 2010b: 34). There is a shortage of staff in the AU Situation room[11] and within the early warning systems of the REC's. It is also necessary to enhance the analytic capacity of staff. "Without substantial staff reinforcement it is questionable whether the monitoring units in certain RECs will be established" (AU, 2010b: 34).

Efforts to strengthen engagement with senior management and political decision makers in some of the RECs remain embryonic (AU, 2010b: 35). Coordination and collaboration with relevant international organizations to build functional and result-oriented partnerships is needed. The AU has not been able to engage with civil society organizations (CSO) because of the diversity of civil society and the very different level of development in different States and regions (AU, 2010b: 36). Different kinds of support for the CEWS were drawn from a relatively small number of donors[12]. In general, donor support has been forthcoming with adequate timing and at sufficient levels. However, "most partners tend to prioritize one or two organizations rather than continent-wide CEWS support based on a pragmatic approach which match the advancement of the individual organizations" (AU, 2010b: 36).

All these issues are important and need to be adequately addressed. Some of them are structural, such as the liaison and coordination between the AU and the RECs, and the human, technical and financial sustainability of the system. The ability of the CEWS to engage AU decision-makers appropriately and influence decision-making is the most critical issue. This is also its central role, which ultimately will enable the development of appropriate response strategies by the AU. Also imperative, however, is the capability to develop effective outreach strategies to engage other stakeholders outside the AU. The CEWS is an open source system and, by its nature, it is desirable to remain as such. Without this vital link with civil society – including non-governmental organizations, media, academia and think thanks – the flow of information will be limited and partial, hindering its primary purpose of facilitating timely and efficient response to conflict and crisis situations in Africa.

The Economic Ways and Means

Usually, in the realm of strategic theory, the economic ways are associated with

11 There are ten Situation Room assistants working on a 24/7 shift basis (AU, 2010b: 34).

12 "Programmed/budget funding is provided by EU, UNDP, GTZ and DANIDA. Flexible, ad-hoc funding is also provided by UNDP, UK, GTZ and USAID" (AU, 2010b: 35).

tariffs and quotas, economic sanctions, incentives and foreign economic aid, with the purposes of protection or coercion, but also providing a basis for developing other instruments of power or influence (Worley, 2008: 6).

The AU can impose economic sanctions under certain conditions. Article 23 of the AU Constitutive Act establishes that any Member State that fails to comply with the decisions and policies of the AU may be subjected to sanctions, "such as the denial of transport and communications links with other Member States, and other measures of a political and economic nature to be determined by the Assembly" (AU, 2002a: 12). Rule 37 of the *Rules of Procedure of the Assembly of the Union* add that economic sanctions may be applied against regimes that refuse to restore constitutional order, such as trade restrictions and any additional sanction as may be recommended by the PSC (AU, 2002c).

The AU sanctions regime addresses three main types of situations: nonpayment of membership contributions (arrears), non-compliance with the decisions and policies of the AU, and unconstitutional changes of government (AU, 2002c). All these situations include economic sanctions ranging from provision, by the AU, of funds for new projects in Member States to trade restrictions. In the last few years, the AU applied sanctions to some Member States. The AU PSC has issued a series of sanctions against Togo, the Comoros, Mauritania, and recently on Guinea, Niger and Madagascar,[13] however with mixed results in terms oversight, monitoring and the verification of implementation (Lulie, 2010).

In order to enhance AU capacity to ensure Member States implement what they bargained for, the AU decided to create a *Sanctions Committee* within the PSC. The committee will have an important role in recommending to the PSC, AU and other legitimate bodies the actions deemed appropriate in response to violations, and in lifting or hardening sanctions (Lulie, 2010).

Economic sanctions may have an important role in addressing some of internal threats to Africa. However, it is questionable if the AU has the full capacity to effectively impose these sanctions. As mentioned in a recent report of the Chairperson of Commission "over and above the suspension measure, international partners, particularly the UNSC, should lend more effective support to the sanctions decided by the AU" (AU, 2010: 6). This international support is a fundamental condition. Still, two other conditions are needed. "The first one is technical which includes the design and the infrastructure of the management of implementation. The second is political or related to the will to act quickly, evenhandedly and consistently" (ISS, 2009: 2).

13 In the case of Madagascar the economic sanctions included: the freezing of funds, other financial assets and economic resources (AU, 2010c: 2).

The Peace Fund

It is imperative to stress that the Peace Fund is not an economic instrument to be used on realm of economic sanctions or other punitive measures. Its role is to provide the necessary financial resources for peace support missions and other operational activities related to peace and security in Africa. However, it has an economic[14] (financial) nature and, above all, is one of the instruments of the APSA, contributing for achieving its peace and security objectives.

The Peace Fund is the continental mechanism created by the AU to financially support the APSA. It is made up of financial appropriations from four sources: regular budget of the AU, voluntary contributions by Member States, non-Member States contributions and miscellaneous receipts (AU, 2007: 102). With regard to the contribution from the AU Member States, only twelve percent[15] of its annual budget is allocated to the fund (AU, 2010b: 60).

However, the Peace Fund is virtually empty and "there is cause for concern regarding the funding of peace operations in Africa" (AU, 2007: 102). Some Member States have difficulties in honoring their financial obligations, and by 2009 the AU's Peace Fund had a negative balance (AU, 2010b: 60). Between 2004 and 2007, only 1.9% of the total resources channeled through the Peace Fund came from African Member States; the rest was provided by external partners (AU, 2010b: 59). The EU is so far the largest funding partner of the AU (Gänzle and Grimm, 2010: 75).

A high-level audit of the African Union in 2007 recommended that the Commission Chairperson should intensify his efforts at mobilizing funds and resources for AU peacekeeping operations from within the Continent and the Diaspora. In addition, the report stressed the need of the African countries to contribute substantially to AU peace operations and to pay regularly their respective contributions (AU, 2007: 172). If the Member States meet their financial obligations, the AU's dependency on external aid will be reduced, and that sustainability and ownership of the APSA will be guaranteed (AU, 2010b: 60).

Conclusions

Military operations, equipment and logistics are expensive. African leaders need to find a balance between investing in this continental and regional security mechanism and in the immediate challenges of governance, poverty, and devel-

14 This is the reason why it is methodologically analyzed under the economic ways.

15 In 2010, a UN report mentioned that these contributions would not be sufficient to deploy and sustain the current peace support operations, and proposed its enhancement (UN, 2010: 14).

opment. Both dimensions are not mutually exclusive as there is no development without security. This represents an enormous challenge to Africa requiring courage, will, wisdom and trust. As previously mentioned, the *Ends* of the ASPA are essentially to respond to both internal and external threats effectively. All these threats are often interrelated and cannot be addressed separately. In order to mitigate all these threats, comprehensive and integrated approaches are required, overcoming narrow preoccupations and working across the whole range of issues. Only by this way will the APSA be a viable security strategy to deal with the principal threats in Africa.

Some recommendations can be suggested. These recommendations are based on three major potential gaps in the APSA, beside the lack of human, technical and financial resources: political will of AU Member States to implement the strategy; the discrepancies between the regional level and the continental level; and the lack of *Ways* to address adequately the security dimension of the APSA (*i.e.* the external threats).

Political will is absolutely vital to operationalize all mechanisms of the APSA. Very sensitive issues such as military intervention in a Member State with regards to grave circumstances, information sharing, implementing sanctions or addressing transnational threats, require strong political commitment and will of AU Member States in order to be effective. Otherwise, the lack of political will can be exploited by the threats - internal or external - to discredit the AU and its Member States, thus hindering obtaining its strategic goals.

Another gap is the discrepancy between the regional and continental levels. The APSA is a very complex security system, relying on regional and continental intergovernmental organizations. At the continental level, there has been significant progress in the development of the AU organizational structures. However, most of the mechanisms of the APSA are completely dependent on the RECs and RMs, such as the regional brigades or the regional warning systems. Without the proper development and operationalization of these regional instruments, there will be no success for the APSA.

The other gap is the lack of Ways to address adequately the security dimension of the APSA. The African Peace and Security Architecture has, according to its name, two dimensions: peace and security. However, most of the Ways and Means of the APSA are primarily focused on the peace dimension of the APSA, not addressing effectively, or simply not addressing, the security dimension. Threats such as terrorism, mercenaries, cross-border crimes, cyber threats, or piracy require effective response strategies, both at the regional and continental levels. This will require cooperation between military, security forces (*i.e.* police), civil society and external partners, but also the development of certain capabilities such as such as air, naval, Special Forces and cyber protection components, not present in the current structure.

These three issues are critical and will require African leaders' focus and also support and contribution of external partners.

Bibliography

Abdellaoui, Jamila el (2009). *The Panel of the Wise: a Comprehensive Introduction to a Critical Pillar of the African Peace and Security Architecture*. Available at http://www.iss.co.za/uploads/PAPER193.PDF. Accessed November 2, 2011.

African Centre for the Constructive Resolution of Disputes (ACCORD) (2009). *Mediating Peace in Africa: Securing Conflict Prevention*. Available at http://www.accord.org.za/downloads/reports/ACCORD_Mediating_Peace_Africa.pdf. Accessed October 30, 2011.

African Union (AU) (2011a). *Task Force to Lead Development and Implementation of 2050 Africa's Integrated Maritime Strategy (2050 AIM-strategy) Formed*. Available at http://www.au.int/en/sites/default/files/PRESS%20RELEASE%20Nº064%202011-6.pdf. Accessed November 4, 2011.

——— (2010a). *African Peace and Security Architecture (APSA): 2010 Assessment Study*. Available at http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/RO%20African%20Peace%20and%20Security%20Architecture.pdf. Accessed November 1, 2011.

——— (2010b). *Progress Report on the Status of the Operationalization of the African Standby Force*. Available at http://www.acoc-africa.org/docs/Dec2010ProgRepASF.pdf. Accessed November 3, 2011.

——— (2010c). *Communique of the 216th Meeting of the Peace and Security Council*. Available at http://www.africa-union.org/root/au/organs/216%20Communique%20Madagascar%20_Eng%20_.pdf. Accessed November 4, 2011.

——— (2009). *Strategic Plan 2009-2012*. Available at http://www.au.int/en/sites/default/files/Strategic_Plan2009-2012.pdf. Accessed November 10, 2011.

——— (2008). *Proposal for an Indicators Module towards the Operationalization of the Continental Early Warning System for the African Union*. Available at http://www.africaunion.org/root/AU/AUC/Departments/PSC/PSC/CD/9_Proposal%20for%20an%20Indicators%20Module.pdf. Accessed September 25, 2011.

——— (2007). *Audit of the African Union (unofficial copy)*. Available at http://www.pambazuka.org/actionalerts/images/uploads/AUDIT_REPORT.doc. Accessed July 17, 2011.

——— (2005). *A Vision for the African Standby Force? A Draft Document for Discussion*. Available at http://www.africa-union.org/root/AU/AUC/Departments/PSC/Asf/doc/ASF%20visionSecond%20Draft%20Vision.doc. Accessed July 17, 2011.

——— (2004). *Solemn Declaration on a Common African Defense and Security Policy*. Available at http://www.africa-union.org/News_Events/2ND%20EX%20ASSEMBLY/Declaration%20on%20a%20Comm.Af%20Def%20Sec.pdf. Accessed July 17, 2011.

——— (2002a). *The Constitutive Act*. Available at http://www.africaunion.org/root/au/AboutAu/Constitutive_Act_en.htm. Accessed July 16, 2011.

——— (2002b). *Protocol Relating to the Establishment of the Peace and Security Council of the African Union*. Available at http://www.africa-union.org/rule_prot/rules_Assembly.pdf. Accessed November 05, 2011.

——— (2002c). *Rules of Procedure of the Assembly of the Union*. Available at http://www.africaunion.org/root/au/organs/psc/Protocol_peace%20and%20security.pdf. Accessed July 20, 2011.

Alghali, Zinurine A. and Mamadou Mbaye (2008). *Fact File: The African Standby Force and Regional Standby Brigades*. Available at http://www.humansecuritygateway.info/documents/CONFLICTTRENDS_Factsheet_AfricanStandbyForce.pdf. Accessed August 10, 2011.

Bachmann, Olaf (2011). *The African Standby Force: External Support to an 'African Solution to African Problems'?* Available at http://www.ids.ac.uk/files/dmfile/Rr67web.pdf. Accessed October 30, 2011.

Besada, Hany, Ariane Goetz and Karolina Werner (2010). "African Solutions for African Problems and Shared R2P". In Hany Besada ed. *Crafting an African Security Architecture: Addressing Regional Peace and Conflict in the 21st Century*. Farnham: Ashgate.

Burgess, Stephen (2009). *The African Standby Force, Sub-regional Commands, and African Militaries*. Available at http://www.au.af.mil/awc/africom/documents/BurgessSubregionalCommands.pdf. Accessed October 20, 2011.

Centre for Democratic Development (CDD) (2010). *Sanctions Index (2000-2010)*. Available at http://www.moibrahimfoundation.org/en/media/get/20110728_2011-cdd-codebook.pdf. Accessed November 4, 2011.

Cilliers, Jakkie (2005). *Towards a Continental Early Warning System for Africa*. Available at http://www.iss.co.za/pubs/papers/102/paper102.pdf. Accessed September 10, 2011.

——— (2008). *The African Standby Force: an Update on Progress*. Available at http://africacenter.org/wp-content/uploads/2009/07/The-African-Standby-Force An-Update-on-Progress.pdf. Accessed August 10, 2011.

Engel, Ulf and João Gomes Porto (2010). "Africa's New Peace and Security Architecture: an Introduction". In Ulf Engel and João Gomes Porto Eds., *Africa's New Peace and Security Architecture: Promoting Norms, Institutionalizing Solutions*. Farnham: Ashgate.

Gänzle, Stefan and Sven Grimm (2010). "The European Union and the Emerging African Peace and Security Architecture". In Hany Besada Ed., *Crafting an African Security Architecture: Addressing Regional Peace and Conflict in the 21st Century*. Farnham: Ashgate.

Institute for Security Studies (ISS) (2009). *Enhancing the African Union Sanctions Regime*. Available at http://www.issafrica.org/uploads/28OCT09REPORT.PDF. Accessed November 5, 2011.

Jiechi, Yang (2011). *Statement by Mr. Yang Jiechi, Minister for Foreign Affairs of the People's Republic of China at a debate of the United Nations Security Council on strengthening and consolidating preventive diplomacy*. Available at http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/CPR%20S%20PV%206621.pdf. Accessed October 30, 2011.

Lulie, Hallelujah (2010). *Institutionalizing the AU Sanctions*. Available at http://www.iss.co.za/iss_today.php?ID=915. Accessed November 5, 2011.

Murithi, Tim and Charles Mwaura (2010). "The Panel of the Wise". In Ulf Engel and João Gomes Porto Eds., *Africa's New Peace and Security Architecture: Promoting Norms, Institutionalizing Solutions*. Farnham: Ashgate.

Powell, Kristiana (2005). *The African Union's Emerging Peace and Security Regime: Opportunities and Challenges for Delivering on the Responsibility to Protect*. Pretoria: Institute for Security Studies.

Söderbaum, Fredrik and Björn Hettne (2010). "Regional Security in a Global Perspective". In Ulf Engel and João Gomes Porto Eds., *Africa's New Peace and Security Architecture: Promoting Norms, Institutionalizing Solutions*. Farnham: Ashgate.

Sturman, Kathryn and Aissatou Hayatou (2010). "The Peace and Security Council of the African Union: from Design to Reality" in Ulf Engel and João Gomes Porto (Eds), *Africa's New Peace and Security Architecture: Promoting Norms, Institutionalizing Solutions*. Farnham: Ashgate.

Touray, Omar A. (2005). "The Common African Defence and Security Policy". *African Affairs* n.º 104, pp. 635-656.

United Nations (UN) (2011). *Support to African Union Peacekeeping Operations authorized by the United Nations: Report of the Secretary-General*. Available at http://reliefweb.int/sites/reliefweb.int/files/reliefweb_pdf/node-371965.pdf. Accessed November 5, 2011.

Vines, Alex and Roger Middleton (2008). *Options for the EU to Support the African Peace and Security Architecture*. Available at http://www.chathamhouse.org/sites/default/files/public/Research/Africa/0508eu_africa.pdf. Accessed September 15, 2011.

Williams, Paul D. (2011). *The African Union's Conflict Management Capabilities*. Available at http://i.cfr.org/content/publications/attachments/IIGG_WorkingPaper7.pdf. Accessed October 30, 2011.

Worley, Robert (2008). *Instruments of Power.* Available at http://www.drworley.org/Pubs/Orchestrating/3b-Instruments.doc. Accessed November 4, 2011.

Zuma, Jacob (2011). *Statement by President Jacob Zuma at a Debate of the United Nations Security Council on Strengthening and Consolidating Preventive Diplomacy*. Available at http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/CPR%20S%20PV%206621.pdf. Accessed October 30, 2011.

Portugal, África e a Cooperação Internacional em Defesa

Ricardo Dias da Costa

Major de Artilharia. Mestre em Estudos Europeus pela Universidade de Coimbra (UC). Pós-graduado em Direito Europeu pela Faculdade de Direito da UC, em Estudos sobre a Europa pela Faculdade de Letras da UC e em Estudos da Paz e da Guerra pela UAL. Possui o Curso de Estado-Maior do IESM.

Resumo

No contexto da atual ordem internacional, onde a globalização tem aumentado a interdependência entre os vários atores do sistema internacional, Portugal tem desenvolvido relações externas, tanto de uma forma multilateral, como bilateral, sendo o principal esforço da cooperação dirigido para os Países de Língua Oficial Portuguesa. Nesse sentido, assistimos no mês passado à inauguração, com honras de Estado, da nova sede da CPLP no Palácio do Conde de Penafiel em Lisboa, espelho claro da intenção de aprofundar ainda mais os laços com os países que falam a mesma língua e, em especial, com os PALOP.

Naturalmente que a cooperação em matérias de defesa desenvolvida com os PALOP pelas Forças Armadas não pode estar dissociada dos objetivos definidos para a Política Externa Portuguesa, sendo por isso de esperar alterações à situação atual. Assim, num quadro de cooperação em matérias de defesa com os PALOP, onde a cooperação bilateral aparece cada vez mais integrada numa cooperação multilateral, procurou-se com este artigo perceber qual a forma de cooperação que Portugal deve adotar neste âmbito para o continente africano.

Abstract

Portugal, Africa and International Cooperation in Defense

Given the current international order, and knowing that globalization has increased the interdependence of the various actors in the international system, Portugal has been developing foreign relations both in multilateral and bilateral ways, and its main cooperation efforts have been directed towards Portuguese speaking countries (CPLP). In consonance with this principle, there was the official opening of the new headquarters of CPLP with state honors last month in Lisbon, which clearly mirrors an intention to further deepen the connections with Portuguese speaking countries in general, and with African Portuguese speaking countries (PALOP) in particular.

Naturally, the cooperation of the Portuguese Armed Forces in matters of defense with PALOP cannot be dissociated from the objectives defined for Portuguese Foreign Policy, which hints at a future change in the current situation. Thus, considering the frame of cooperation with PALOP in matters of defense, in which bilateral cooperation is more and more integrated in multilateral cooperation, with this article we aimed to understand the type of cooperation with the African continent that Portugal should adopt in the future.

> "…O importante desafio que se coloca a Portugal é o de saber articular, nos planos político, económico e cultural, a dinâmica da sua integração europeia com a dinâmica de constituição de uma comunidade, estruturada nas relações com os países e as comunidades de língua portuguesa no mundo (…). É neste quadro que a política de cooperação (…), vetor essencial da política externa, adquire um particular sentido estratégico..."
>
> (XIII Governo, 1999: 1)

Em fevereiro assistimos à inauguração com honras de Estado da nova sede da CPLP em Lisboa, reforçando assim a intenção já expressa várias vezes por membros do governo de aprofundar ainda mais os laços com os países que falam a mesma língua e, em especial, com África. Como objetivo principal do aprofundamento das relações com a CPLP podemos referir a fundamental contribuição diplomática para influenciar as instituições internacionais[1], bem como a divulgação e reforço da língua portuguesa, mas também interesses económicos, com Portugal a pretender aumentar as relações comerciais que tem com estes países.

Sendo a Política de Defesa Nacional indissociável dos objetivos externos definidos por Portugal, naturalmente que esta situação terá influência nas opções tomadas para a cooperação internacional no âmbito da defesa, nomeadamente em África.

Portugal, país simultaneamente europeu, atlântico e com uma forte ligação cultural a África, tem desenvolvido relações externas de segurança e defesa pelas Forças Armadas, tanto de uma forma multilateral, como bilateral.

No quadro multilateral, destacamos o empenhamento em alianças e organizações internacionais, das quais se distinguem a União Europeia, a NATO, a ONU ou a CPLP. Neste âmbito, as Forças Armadas portuguesas têm dado, desde o início dos anos 90, um importante contributo em teatros de operações como por exemplo o Kosovo, a Bósnia-Herzegovina, o Líbano, o Chade ou o Afeganistão, entre outros.

No plano bilateral, encontramos vários países que já são parceiros na União Europeia ou na NATO, bem como países de áreas regionais de interesse estratégico para Portugal e para estas duas organizações, nomeadamente os países do sul do

1 A título de exemplo refere-se que Portugal já beneficiou do apoio da CPLP na sua candidatura bem-sucedida a membro não permanente do Conselho de Segurança da ONU.

Mediterrâneo. Contudo, o principal esforço da cooperação bilateral desenvolvido por Portugal recai nos países de expressão portuguesa e em especial nos Países Africanos de Língua Oficial Portuguesa (PALOP) e em Timor.

Num quadro de cooperação internacional em matérias de segurança e defesa, onde a cooperação bilateral aparece cada vez mais integrada numa cooperação multilateral, interessa pois perceber qual a forma de cooperação desenvolvida no âmbito da Política de Defesa Nacional pelas Forças Armadas Portuguesas, que Portugal deve adotar para o continente africano.

Abordagem Conceptual da Cooperação

Razões para os Estados Cooperarem

Segundo Cabral Couto (1988: 65), as relações no sistema internacional entre os diversos atores políticos podem ser de "cooperação", de "acomodação" ou de "conflito". Assim, as relações entre os diversos intervenientes na cena internacional estão dependentes dos objetivos/interesses em causa, nomeadamente se estamos perante objetivos comuns, valores comuns ou interesses divergentes e ainda se são considerados interesses vitais, importantes ou secundários, condicionando desta forma as opções de Política Externa de cada um dos Estados.

A respeito da cooperação e embora não esteja dentro do âmbito deste artigo discorrer sobre as diversas correntes de pensamento nas Relações Internacionais (RI), é conveniente relembrar as teorias realistas e neorrealistas por defenderem o papel central do Estado nas RI e a necessidade que estes têm de, muitas das vezes, cooperar e fazer alianças por forma a manter o equilíbrio de poderes e assim assegurarem a sua sobrevivência, ou ainda os modelos transnacionalistas ou liberais que enfatizam a interação entre as sociedades, os novos atores e a importância da cooperação num sistema internacional cada vez mais interdependente, tal como é defendido no trabalho de Dougherty e Pfaltzgraff (2003).

Contudo, é também importante revisitar o trabalho de Held, McGrew, Golblatt e Perratton (1999), uma vez que a globalização assume aqui um papel fundamental ao moldar a nova realidade internacional, em que a intensificação dos principais fluxos e redes globais (nomeadamente comércio, produção e investimento, mercados financeiros, migração e cultura), a aceleração de processos e interações globais assentes na evolução de redes globais de comunicações e transportes, o alargamento de atividades sociais, políticas e económicas que cruzam Estados, regiões e continentes e o crescimento da extensão, intensidade e velocidade das interligações à escala global são uma realidade que coloca a todos os Estados novos e extraordinários desafios.

Estas características inerentes à globalização têm igualmente implicações no contexto de segurança deste século, em que as ameaças transnacionais se apresentam como uma permanente preocupação à segurança nacional e internacional. Sendo já sobejamente conhecidas, referem-se a título de exemplo a criminalidade organizada (na qual se destaca o trafico de armas, narcóticos e pessoas), o terrorismo transnacional (muitas vezes, mas não só, associado ao extremismo religioso), a proliferação de armas de destruição maciça (com especial importância em regiões de grande volatilidade) ou os ataques cibernéticos (NATO, 2010: 7-15). Estas ameaças têm nos Estados falhados o ambiente propício à sua propagação e são ainda mais preocupantes quando conjugadas entre si, atingindo assim o seu exponente máximo de perigosidade.

A globalização tem também associado um conjunto de tendências com fortes implicações na relação entre os Estados. Uma das que tem maior impacto na sociedade ocidental é a transferência progressiva do centro de gravidade da economia mundial para a região asiática, principalmente para a China, mas também para a Índia. Este facto, em conjunto com o peso demográfico que esta região representa e o assimilar dos princípios inerentes à economia de mercado que durante 200 anos garantiram a vantagem ao Ocidente, permitiu-lhes uma dinâmica de crescimento imparável (Amado, 2010: 141).

Mas também em outros pontos do globo se verifica o emergir de novas potências económicas, como por exemplo o Brasil, ou o renascer de outras mais antigas, como é o caso da Rússia. Assim sendo, é visível o crescimento de um sistema cada vez mais multipolar em torno das novas potências económicas, ao mesmo tempo que se assiste a uma diminuição cada vez maior da hegemonia e influência do Ocidente, que é, de resto, enfatizada pela crise económica que atravessa.

Indissociável da nova dinâmica da globalização é também o incremento exponencial de novos atores não estatais no sistema internacional, com quem os Estados têm cada vez mais que lidar. A interligação e coordenação com os atores não estatais assume, por isso, um papel incontornável na resolução dos problemas atuais da conflitualidade internacional. É igualmente de destacar o aumento da importância das organizações regionais no plano internacional, procurando maximizar as capacidades do Estado-Nação num mundo cada vez mais globalizado e em que o próprio conceito de soberania tradicionalmente associado ao Estado-Nação se encontra em evolução.

Como corolário do que foi descrito atrás cita-se Marcel Wissenburg (2009: 2):

> "…*States no longer have the power to make good on their claim to sovereignty: on the one hand they share power with other states and other entities low and high, on the other they cannot (always, fully) control those other entities – nor other states directly or indirectly operating within their respective territories …*".

Estes factos apontam para o reconhecimento de que este sistema internacional mais global e, por isso também mais complexo, trouxeram um conjunto de problemas que nenhum país é capaz de enfrentar totalmente sozinho. Paradoxalmente, os Estados veem as suas capacidades de interferir no sistema internacional cada vez mais reduzidas e, por isso, veem-se na necessidade de assentarem as suas políticas externas numa atuação cada vez mais coordenada, onde a cooperação assume um papel fulcral.

Tipologias de Cooperação

As abordagens clássicas às tipologias de cooperações identificam dois tipos de cooperação: a cooperação bilateral e a cooperação multilateral.

É considerada cooperação multilateral quando as atividades são desenvolvidas através de uma organização "…dotada de caráter internacional tendo por membros países cujos governos estão representados, ao mais alto nível, por pessoas no desempenho oficial das suas funções… [e em que os recursos postos à sua disposição são transformados] … num todo, de tal maneira que perdem a sua identidade para se tornarem parte integrante do seu ativo…" (IPAD, 2004: 4).

Sendo a Defesa um dos bastiões da soberania dos Estados, esta "perda de identidade" associada ao conceito de multilateralidade torna mais apropriado, embora consubstanciando um conceito bem distinto, falar-se em cooperação militar multinacional, tal como podemos verificar no seguinte documento do Ministério da Defesa Britânico, que a define como "…*any arrangement where two or more nations work together to enhance military capability. This can include exchanges and liaison, training and exercising, common doctrine, collaborative equipment procurement, or multinational formations. Nations can either cooperate on a roughly equal basis, or with one or more taking the lead and providing a framework within which others make smaller contributions. In most cooperative arrangements, nations can – and usually do – retain national control over their own forces*…" (Ministry of Defence, 2001: 12).

Por outro lado, a cooperação é considerada bilateral se realizada diretamente entre dois países, podendo ser de vários tipos/naturezas, dos quais destacamos (IPAD, 2004: 4):

- Cooperação Técnica, que tem por objetivo essencial "… aumentar o nível de conhecimentos, qualificações, *know-how* técnico…";
- Ajuda a Programas, que engloba "… as contribuições destinadas a ajudar o país beneficiário a implementar vastos programas de desenvolvimento num setor particular, como a agricultura, o ensino, os transportes, etc. …".

Em termos militares, o Ministério da Defesa Nacional (MDN) define a Cooperação Militar Bilateral[2], como sendo as atividades onde são desenvolvidas "… ações concretas entre dois Estados, contribuindo de forma inequívoca e relevante para um maior conhecimento e melhor compreensão dos objetivos e interesses nacionais no domínio da Segurança e da Defesa, acrescida transparência, conciliação de posições e eventual definição de objetivos comuns…" (DGPDN, 1999: 6).

Apesar disso, uma análise aos Tratados, acordos, convenções e memorandos de entendimento celebrados bilateralmente por Portugal no domínio da Defesa constantes no Anuário Estatístico da Defesa Nacional, permite concluir que os mesmos já não espelham a aplicação do conceito puro de cooperação bilateral apresentado anteriormente. Isto porque já não estão limitados a uma cooperação entre dois países de forma isolada, estando estas cooperações bilaterais englobadas num enquadramento mais vasto de cooperações multilaterais (MDN, 2008: 63-73).

Temos assim o exemplo da cooperação com os países da Bacia do Mediterrâneo inserido no contexto da Iniciativa de Defesa 5+5; da cooperação com os países do Leste Europeu, que tem a sua origem num quadro de alargamento da NATO e da União Europeia; da cooperação com países do continente sul-americano com interesses relacionados com a conferência ibero-americana; da cooperação com diversos países membros da NATO ou da União Europeia, ou em que essas organizações têm interesses específicos.

Este conceito de cooperação bi-multilateral foi definido em 2005 no documento intitulado de *Visão Estratégica para a Cooperação Portuguesa* como tendo o propósito de encontrar maneiras de "…potenciar a cooperação bilateral, colocando-a em parceria com esforços multilaterais, e de, ao mesmo tempo, assegurar que os esforços do âmbito bilateral sejam dirigidos de forma coordenada no sentido da convergência com as intervenções de outros parceiros…" (Conselho de Ministros, 2005: 32), em particular na conjugação com a União Europeia.

Dos conceitos de cooperação bilateral e multilateral pode ainda ser deduzido o conceito de cooperação trilateral, pela aplicação dos mesmos a uma esfera específica constituída por três países, onde são conjugados os interesses convergentes e maximizadas as potencialidades de cada um.

2 Ou relacionamento bilateral no domínio da defesa.

A Estratégia Portuguesa para a Cooperação

Documentos Oficiais Identificadores dos Interesses Estratégicos Portugueses Definidos para a Cooperação

As "Grandes Opções do Plano 2010-2013" definidas em 2010 pelo XVIII governo português estão, de alguma forma, alinhadas com o que foi descrito anteriormente. No documento, pretende-se que a política externa portuguesa esteja associada à participação de Portugal no seio das organizações multilaterais a que pertence, como por exemplo as Nações Unidas, a NATO, a UE, a OSCE e a CPLP, sendo também destacadas as ligações bilaterais com os países de língua portuguesa, com a Comunidade Ibero-americana, com os países asiáticos, com a Rússia, com a Ucrânia e com os EUA.

Naturalmente que é dado um especial enfoque à participação na construção europeia, bem como à política de cooperação no âmbito da CPLP, realçada ainda mais pela importância concedida à política de promoção da língua e cultura portuguesa no mundo. Refere-se também o realçar da importância da segurança humana no desenvolvimento da política de defesa nacional, sempre em concordância com a construção da Política Comum de Segurança e Defesa (PCSD) da União Europeia, com a participação empenhada na NATO e também com o aprofundar da relação com os países da CPLP, em que a Cooperação Técnico-Militar tem particular importância (XVIII Governo, 2010: 75-84).

Todavia, estas linhas de atuação não são novas, tendo a cooperação assumido desde há longa data um papel fulcral na política externa do Estado português e na elaboração de uma estratégia com vista à defesa dos interesses nacionais.

Desde logo podemos referir a aprovação em 1999, pelo Conselho de Ministros do XIII Governo, de um documento intitulado "A cooperação Portuguesa no Limiar do Século XXI", que pretendia definir a orientação estratégica para Portugal. No cerne do documento encontrava-se a necessidade de o país saber articular, nos planos político, económico e cultural, a dinâmica da integração na União Europeia com a dinâmica da constituição de uma comunidade assente nos países de língua portuguesa, ou seja, com a CPLP, que entretanto tinha visto o ato constitutivo ser assinado em 1996. Nesta intenção estava presente um sentido estratégico de permitir a Portugal, entre outras coisas, definir um elemento de diferenciação e de afirmação de uma identidade própria na diversidade europeia, assumindo a cooperação para o desenvolvimento um papel fundamental nesse sentido (XIII Governo, 1999: 14).

Esta ideia seria ainda mantida num documento aprovado em 2005 e intitulado "Uma Visão Estratégica para a Cooperação Portuguesa", mas agora influenciada pela necessidade de garantir a Portugal uma inserção mais dinâmica nas redes da globalização, possibilitando assim uma maior rentabilização da cooperação portu-

guesa. Pretendia-se, desta forma, orientar a cooperação bilateral e multilateral de modo a aproveitar as vantagens em algumas áreas da coordenação internacional. Tendo como pano de fundo os "Objetivos de Desenvolvimento do Milénio", aprovados em 2000 na Cimeira do Milénio, esta estratégia para a cooperação refletia a política externa portuguesa nas suas três grandes linhas de ação (Cooperação Portuguesa, 2005: 12):

- A intensificação da relação com os países de língua portuguesa, com especial ênfase para os PALOP e para Timor-Leste, sendo realçado que "…a relação com os países africanos de expressão portuguesa constitui um dos pilares fundamentais da nossa política externa, juntamente com a integração europeia e a aliança atlântica…";
- A promoção da língua portuguesa no mundo, pois esta "… contribui para a sedimentação, longevidade e proficuidade de uma comunidade linguística que constitui, a um só tempo, um importante contributo histórico português para o mundo, e um trunfo relevante na era da globalização…";
- A promoção da capacidade de interlocução e influência em redes internacionais cujos centros de decisão são supranacionais, pois "…uma das características mais salientes da cooperação nos anos mais recentes é o enorme reforço da coordenação internacional através dessas redes…".

Na prática, a importância da CPLP foi consubstanciada pela definição de prioridades para a cooperação portuguesa, como por exemplo a intenção de concentrar os projetos de cooperação no quadro dos países de expressão portuguesa, incluindo as organizações regionais e sub-regionais em que se inseriam, bem como pela determinação do "apoio à lusofonia" como um dos princípios orientadores da cooperação.

Em 2010 é aprovada a "Estratégia Portuguesa de Cooperação Multilateral" que tem como objetivo operacionalizar a "Visão Estratégica da Cooperação Portuguesa" de 2005, passando este documento a servir de base à orientação e à estruturação da coordenação entre os diversos intervenientes institucionais da cooperação portuguesa.

Este documento engloba sete estratégias definidoras das principais linhas de ação a desenvolver no âmbito da cooperação com diversas instituições a que Portugal pertence, nomeadamente: a União Europeia; a CPLP; os fundos e programas do sistema das Nações Unidas para apoio ao desenvolvimento; a OCDE; o fundo global de combate à SIDA, tuberculose e malária; as instituições financeiras internacionais; a Conferência Ibero-americana.

A estratégia de cooperação com a CPLP é apresentada neste documento como uma ferramenta fundamental, em particular pela possibilidade de utilizar a língua comum como potenciadora de intervenções envolvendo vários países lusófonos. Também na estratégia portuguesa de cooperação com a União Europeia é dada

especial importância ao apoio ao compromisso europeu para o desenvolvimento de África, prioritariamente apoiando os interesses dos países com quem Portugal coopera. É aqui claramente destacado o interesse em reforçar a influência da CPLP junto da UE, em particular no domínio do desenvolvimento (IPAD, 2010: 26).

Compete ao IPAD a definição da política de cooperação para o desenvolvimento, incluindo a coordenação dos Programas Integrados de Cooperação (PIC), que constituem os documentos de programação da cooperação. Pretende-se que sejam realizadas reuniões regulares de coordenação com vista à troca sistemática de informação, quer internamente ao nível do Ministério dos Negócios Estrangeiros (MNE), quer com as Embaixadas e Missões diplomáticas, quer com os diversos ministérios sectoriais.

Embora não haja referência expressa nesta "Estratégia" à cooperação no âmbito da defesa, consideramos que estas reuniões também venham a incluir a participação do Ministério da Defesa Nacional (MDN), até porque a Cooperação Técnico-Militar aparece nos PIC, muito embora seja de relembrar que o fornecimento de serviços militares[3] não é contabilizado pela ONU como Ajuda Pública ao Desenvolvimento (IPAD, 2004: 3).

Em relação à participação das Forças Armadas, relembra-se que uma das quatro missões principais das Forças Armadas definidas no "Conceito Estratégico de Defesa Nacional" (CEDN) é o garante "… da concretização dos objetivos do Estado e da satisfação dos seus compromissos internacionais, atuando como instrumento da política externa …" (Conselho de Ministros, 2003: 8).

Nesse sentido, o CEDN já definia em 2003 no seu n.º 5 o espaço estratégico de interesse nacional, quer permanente, quer conjuntural. Em relação a este último é identificado o sistema de alianças e organizações internacionais em que Portugal se insere, nomeadamente a ONU, a OSCE, a NATO, a UE, os EUA e a CPLP. Assim, a CPLP é reconhecida neste documento como um instrumento relevante para a afirmação lusófona nas instituições internacionais, sendo a importância no âmbito da defesa nacional consubstanciada nos seguintes objetivos (Conselho de Ministros, 2003: 7):

- Reforçar a sua dimensão de defesa;
- Desenvolver a cooperação de defesa, militar e não militar, numa base solidária, profissional e de respeito mútuo pela individualidade dos Estados;
- Intensificar a cooperação multilateral no âmbito da CPLP, de forma a contribuir para a valorização do conjunto dos países de língua portuguesa ao nível das Nações Unidas;
- Intensificar as relações bilaterais entre Portugal e os Estados lusófonos.

3 E também o fornecimento de equipamentos e o perdão de dívida com fins militares.

Implicações para a Cooperação Portuguesa em Segurança e Defesa em África

A "Visão Estratégica da Cooperação Portuguesa" de 2005 definia como orientações gerais para a cooperação uma atenção especial a África assente num "… reforço do espaço lusófono, utilizando a língua comum como potenciadora de intervenções e da constituição de redes no espaço lusófono, por forma a contribuir para o reforço da capacidade de resposta dos países da CPLP aos desafios da globalização…" (Conselho de Ministros, 2005: 6).

Cinco anos mais tarde e de forma a operacionalizar essa estratégia, a "Estratégia Portuguesa de Cooperação Multilateral" de 2010 apresentava como um dos objetivos da cooperação portuguesa a contribuição para o reforço da presença e capacidade de influência de Portugal sobre as organizações multilaterais a que pertence, nomeadamente através da operacionalização da abordagem bi-multilateral em todos os níveis de intervenção[4] (IPAD, 2010: 12).

Também ao nível da cooperação militar, já não é possível falar-se na aplicação dos conceitos puros de cooperação bilateral e multilateral. A cooperação efetuada com o continente africano, de um modo geral, e com os Países Africanos de Língua Oficial Portuguesa (PALOP), em particular, são disso um excelente exemplo.

Pela sua especificidade, o MDN distingue a Cooperação Técnico-Militar (CTM) efetuada com os Países de Língua Oficial Portuguesa (PLOP)[5], das restantes cooperações bilaterais, compreendendo esta atividade um "…conjunto de ações que têm por objetivo a organização, reestruturação e formação dos Ministérios da Defesa Nacional e Forças Armadas dos PLOP, e respetivos militares, obedecendo a princípios de apartidarismo, subordinação aos órgãos de soberania democráticos e legítimos, respeito pelo Estado de Direito e pela boa governação, capacitando aqueles Estados como produtores de Segurança e de Desenvolvimento…" (MDN, 2008: 75).

Verificamos aqui também a necessidade do abandono da diferenciação clássica entre os conceitos bilateral e multilateral, pois se por um lado a CTM com os PALOP é executada através de programas-quadro bilaterais constituídos por projetos, por outro lado ela não se limita apenas à cooperação país a país[6]. A título de exemplo, relembra-se que no Anuário da Defesa Nacional de 2008 a componente de defesa da Comunidade dos Países de Língua Portuguesa (CPLP) é definida como um conjunto de ações de cooperação cujo objetivo é "…criar uma plataforma comum de partilha de conhecimentos e de promover uma política comum de cooperação

4 Como por exemplo, ao nível das sedes ou no terreno dos países parceiros da cooperação.

5 Excluindo o Brasil.

6 Embora formalmente se continue a diferenciar a CTM (como cooperação bilateral e assente nos programas-quadro), da cooperação multilateral desenvolvida no seio da CPLP (de que são exemplo os exercícios da série Felino).

nas esferas da Defesa e militar, bem como de contribuir para o desenvolvimento das capacidades internas com vista ao fortalecimento das Forças Armadas dos países da CPLP…" (MDN, 2008: 75).

Assim, a cooperação está hoje ligada a uma esfera mais vasta de atuação, que poderá ser entendida como uma atuação bi-multilateral relacionada com a segurança e o desenvolvimento, podendo ser desenvolvida no seio de um variadíssimo número de organizações presentes em África, das quais destacamos a Organização das Nações Unidas, a União Europeia, a NATO, a União Africana (UA) ou a Comunidade dos Países de Língua Portuguesa (CPLP).

No entanto, os Estados com menor capacidade de participação ativa poderão ver os seus interesses estratégicos a serem postos em causa quando a cooperação é integrada numa esfera muito superior, e onde poderá prevalecer a influência de outros atores presentes numa determinada região. Esta situação poderá também aconselhar a opção por uma cooperação militar trilateral em conjunto com outros Estados que tenham grandes interesses e influência na região, mas em que a participação dos Estados de menor dimensão salvaguarde os seus interesses estratégicos. Esta forma de cooperação é identificada no Programa de Apoio às Missões de Paz em África (PAMPA), sendo referido que "…Portugal estará recetivo ao desenvolvimento de ações de cooperação trilateral com países terceiros que declarem pretender fazê-lo, em favor de um país africano recetor, identificando países a envolver, áreas a cooperar e meios a afetar…" (PAMPA, 2006: 3).

Assim, é conveniente ter em consideração as vantagens e desvantagens comparativas de Portugal face a outros atores presentes em África, palco do principal esforço da cooperação portuguesa. A "Visão Estratégica para a Cooperação Portuguesa" de 2005 identifica claramente essas vantagens e desvantagens. Elenca os escassos recursos que Portugal pode colocar à disposição da cooperação como a principal desvantagem, situação ainda mais gravosa pelo facto de existir uma tradição de descentralização orçamental, administrativa e política que se constitui como o maior obstáculo à eficiência da cooperação portuguesa. Apresenta a língua e a história em comum como as principais vantagens comparativas de Portugal, nomeadamente em relação aos PALOP (Conselho de Ministros, 2005: 13).

Síntese dos Principais Atores Presentes no Continente Africano

Principais Atores Externos

Neste início de século assistiu-se a um redirecionamento do interesse de várias potências para África. Muito embora as razões que levaram a esse incremento sejam diversas, é de realçar a necessidade de acesso aos recursos energéticos, pro-

curando estas potências diversificar (e não substituir) as suas fontes. Face à impossibilidade de abordar neste artigo todos os atores externos presentes no continente africano, optámos por apenas fazer uma breve apresentação da China, da Rússia, dos EUA e da União Europeia.

O interesse chinês no continente africano tem vindo a crescer significativamente nos últimos anos. A estratégia chinesa de atuação em África assenta na utilização coerente de instrumentos políticos, diplomáticos, económicos, militares, culturais, entre outros, o que tem garantido à China uma expansão e afirmação no continente africano.

Neste âmbito, salienta-se o *modus operandi* chinês de conceder empréstimos junto dos países africanos para depois perdoar parte da dívida em troca do fortalecimento das relações políticas e económicas, com especial enfoque junto dos países produtores de petróleo, que obtêm vantagens mais significativas. Nestas vantagens incluem-se, a título de exemplo, o apoio político na ONU, a possibilidade de anulação total da dívida ou o reforço do financiamento, quer para a construção de infraestruturas, para projetos de desenvolvimento ou para cooperação militar (Carriço, 2008).

Embora a cooperação chinesa tente alargar ao máximo a sua esfera de influência a todos os países africanos que lhes possam garantir o acesso aos recursos de que necessitam, está presente com maior significado nos países onde a influência ocidental é mais diminuta (como é o exemplo do Sudão), muito devido ao facto de a China, ao contrário do que é feito pelos países ocidentais, não fazer depender a sua ajuda externa de contrapartidas nas áreas dos Direitos Humanos, da Governação, etc. Não obstante, a sua presença é já significativa em diversos países africanos, como por exemplo Angola, Sudão, Argélia, Guiné Equatorial, Congo, Egito, Nigéria, Líbia, Tunísia, Mauritânia, Chade, etc.

Assim, podemos resumir a atuação da China em África em três grandes linhas de ação:

- Aumentar a sua influência política junto dos países africanos de forma a ampliar a sua capacidade de intervenção em África;
- Garantir o acesso aos recursos energéticos e às matérias-primas que lhe permita manter o crescimento da sua economia;
- Permitir a abertura dos mercados africanos às suas empresas e aos seus produtos.

Em relação à Rússia, é de referir que a sua presença no continente africano não é muito significativa. Podemos, no entanto, apontar como exemplo das ações desenvolvidas pelos Russos no continente africano, a sua atuação ao nível da segurança, com Moscovo a aumentar a sua participação em operações de apoio à paz sob a égide da Organização das Nações Unidas e também a incrementar o seu papel na luta contra a pirataria no Golfo de Áden. Em contrapartida, tem mantido,

tal como a China, o apoio a alguns regimes não democráticos, como é o caso do Sudão, evitando assim colocar em causa os seus interesses económicos na região (Jesús, 2010: 72-73).

É, por isso, possível identificar dois grandes objetivos no relacionamento da Rússia com África:

- Por um lado, manter a ligação aos países que estiveram sob a esfera comunista, contrariando assim a influência das potências ocidentais em África;
- Por outro lado, encetar relações com países africanos numa base mais económica do que política, com o objetivo primário de garantir o acesso aos recursos energéticos, situação de especial importância no que respeita ao controlo do gás que é fornecido à Europa pelos países do norte de África.

Sobre os Estados Unidos, a importância dada a este continente é passível de ser verificada na criação do AFRICOM, bem como no desenvolvimento de programas de apoio à segurança.

Se tivermos em consideração a *U.S. Policy in Africa in the 21st Century,* verificamos que esta assenta em quatro grandes prioridades: a primeira é o providenciar de programas de apoio à segurança que garantam a paz no continente africano; a segunda é a promoção de práticas e sistemas democráticos; a terceira é a promoção do crescimento económico sustentado assente numa economia de mercado; e a quarta é a promoção da saúde e do desenvolvimento social (Carter, 2009: 21).

Em relação à primeira prioridade identificada, que é a mais relevante para o presente artigo, é de referir que tem como objetivo o apoio ao desenvolvimento de capacidades africanas de segurança a três níveis: ao nível da União Africana, ao nível das organizações sub-regionais de segurança e ao nível dos Estados africanos. São exemplos desta forma de atuação o apoio em termos de aconselhamento e equipamentos dado ao QG da União Africana, nomeadamente no planeamento e monitorização, bem como o apoio logístico fornecido à ECOWAS.

Nesse âmbito, realça-se também o programa *Africa Contingency Operations Training and Assistance* (ACOTA), criado em 2002, com o objetivo de treinar forças militares africanas, com vista à integração no *Africa Standby Force*. Sobre este ponto convém ainda referir o apoio prestado à concretização dos centros de instrução e treino localizados em diversos países de África, como por exemplo no Senegal, no Ghana, na África do Sul, no Mali e no Quénia.

É por isso possível reconhecer que o interesse dos EUA em África é moldado principalmente pela necessidade de deter o crescimento do terrorismo islâmico no continente africano, mas também pelo interesse em assegurar o acesso aos recursos energéticos, procurando assim diversificar as suas fontes. A estas necessidades está também associado o objetivo de contrapor a crescente influência de outros atores internacionais em África, nomeadamente da China.

Assim, os interesses americanos concentram-se fundamentalmente no norte de África e na região do "Corno de África", por razões inerentes à luta contra o terrorismo, e no Golfo da Guiné, por razões de acesso aos recursos.

No tocante à União Europeia, destaca-se o apoio dado à implementação do NEPAD em 2001 com o objetivo de apoiar o desenvolvimento socioeconómico do continente africano, fazendo depender essas ajudas da concretização pelos países africanos de metas ligadas à boa governação, ao respeito pelos direitos humanos e pelas liberdades individuais, etc. A aprovação da "Estratégia Conjunta UE-África" em 2007 reforça assim o objetivo de aprofundar a cooperação entre os dois continentes para melhor apoiar o desenvolvimento do continente africano.

Mas o interesse da União Europeia em África também tem de ser visto na ótica da forte ligação histórica existente entre este continente e alguns dos seus Estados membros, como é o exemplo da França, da Inglaterra ou de Portugal. Assim, o estreitamento dos laços entre a UE e África, nomeadamente através da União Africana e demais organizações regionais africanas, também procura responder à crescente ameaça que passou a pairar sobre os interesses estratégicos de alguns dos seus Estados membros, pelo facto de os países emergentes de um modo geral, e a China em particular, terem cada vez maior influência junto dos países africanos francófonos e anglófonos (e naturalmente também lusófonos).

No âmbito da segurança e defesa realça-se o programa EURORECAMP que procura garantir o treino individual dos militares africanos e o treino das unidades africanas em Operações de Apoio à Paz com vista à formação da *African Standby Force* (ASF), em particular das brigadas a fornecer pela ECOWAS/CEDEAO, a SADC e a ECCAS/CEEAC.

Atores Regionais Africanos

Na cimeira de Lomé, em 2000, é adotado o Ato Constitutivo da União Africana, tendo a primeira assembleia sido reunida dois anos depois em Durban a 9 de julho de 2002. Muito embora a Paz e Segurança não fizesse inicialmente parte do Ato Constitutivo, uma retificação em 2003 alterou esta situação, passando a União Africana a atuar fundamentalmente em três eixos principais:

- A promoção da integração política e socioeconómica;
- A promoção do desenvolvimento sustentado;
- A promoção da paz e segurança.

Em relação a este último eixo, refere-se o desenvolvimento da Arquitetura de Paz e Segurança Africana (APSA) assente no desenvolvimento de capacidades a dois níveis (que se pretendem interligados e complementares): ao nível da União Africana e ao nível das organizações sub-regionais africanas.

A ligação entre estes dois níveis é feita principalmente através do Conselho para a Paz e Segurança (PSC), que tem a função de decisão e execução dos assuntos relacionados com a prevenção, a gestão e a resolução de conflitos em África (incluindo a edificação de um *Early Warning System*). De forma a permitir o cumprimento das decisões feitas pelo PSC no que respeita à execução de Operações de Apoio à Paz, a UA definiu no artigo 13.º do Protocolo para a implementação do PSC a intenção de criar a *African Standby Force* (ASF).

A respeito do *Early Warning System*, pretende-se que seja um mecanismo transversal a todas as organizações e que permita o alerta oportuno de potenciais conflitos e ameaças à paz, de forma a possibilitar a previsão e prevenção dos mesmos. Tal como o financiamento, também aqui o grau de desenvolvimento é muito diferente consoante a organização em causa. A este nível, apenas a ECOWAS e a IGAD dispõem de um sistema operacional, embora ainda existam limitações na troca de dados com a UA.

Sobre a *African Standby Force*, refere-se que a sua constituição tem como principal objetivo guarnecer a União Africana (e suborganizações) de uma capacidade que permita desenvolver Operações de Apoio à Paz (nas suas várias vertentes). Pretendia-se que esta força tivesse cerca de 15.000 efetivos até junho de 2010 e fosse formada com base em cinco Brigadas assentes nas seguintes cinco organizações sub-regionais: a "*Economic Community of West African States*" (ECOWAS/CEDEAO), a "*Southern African Development Community*" (SADC), a "*Economic Community of Central African States*" (ECCAS/CEEAC), a "*Intergovernmental Autority for Development*" (IGAD) e a "*Union du Maghreb Arabe*" (UMA).[7]

Apesar dos esforços nesse sentido realizados pelos países africanos, pelas organizações africanas e pela comunidade internacional, esse objetivo não foi cumprido e ainda está longe de ser alcançado. Como razões para esse facto destacam-se os diferentes níveis de integração que as comunidades têm, mas também os fortes condicionamentos dos recursos financeiros e humanos disponíveis.

Em relação aos recursos financeiros, refere-se que a situação é bem diferente consoante a organização em causa, muito embora para todas elas e por norma os recursos disponíveis sejam considerados insuficientes. Indissociável desta situação está a proveniência dos fundos, que são o resultado quer de contribuições dos respetivos Estados Membros da UA[8], quer (e principalmente) de contribuidores externos a África.

7 Destas comunidades realça-se, pela importância que têm para Portugal, a ECOWAS/CEDEAO, devido ao facto de a Guiné-Bissau e Cabo Verde serem seus membros, a SADC por englobar Angola e Moçambique e a ECCAS/CEEAC por incluir Angola e S. Tomé e Príncipe.

8 Sendo que as contribuições internas, além de reduzidas, são muitas vezes agravadas pela consecutiva falha de alguns países membros.

A ECOWAS é uma das organizações sub-regionais que mais apoios tem recebido, nomeadamente de França, pela importância que tem a presença dos países francófonos nesta organização.[9] Talvez por isso, esta organização seja considerada uma das que mais evoluiu no âmbito da APSA (a par da IGAD e logo seguida pela SADC), sendo de destacar o emprego de forças militares em diversas Operações de Apoio à Paz, nomeadamente na Libéria em 1990-1997 e 2003, na Serra Leoa em 1997-1999, na Guiné-Bissau em 1998-1999 ou na Costa do Marfim em 2003-2004[10] (Klingebiel, Blohm e Eckle, 2008: 36).

Mas os problemas não são apenas de índole financeira, pois em muitos casos a credibilidade e legitimidade destas organizações é colocada em causa, uma vez que existe sempre a possibilidade de os órgãos responsáveis pela APSA, aos vários níveis, incluírem na sua composição países que não respeitem os valores da democracia ou dos direitos humanos.

A CPLP e o PAMPA

A "declaração constitutiva" da Comunidade dos Países de Língua Portuguesa é aprovada em Lisboa a 17 de julho de 1996, tendo como objetivos, entre outros, a cooperação em todos os domínios, com exceção da segurança e defesa. Este domínio seria posteriormente formalizado em 2002 na IV Conferência de Chefes de Estado e do Governo, embora desde 1998/99 se realizassem reuniões de ministros da defesa e reuniões de CEMGFA.

Também a dinâmica da Cooperação Técnico-Militar foi fundamental para o aprofundamento dos laços entre Portugal e os diversos países da CPLP, tendo a relação bilateral existente sido complementada com um novo relacionamento multilateral que potenciasse o aproveitamento das capacidades que os vários membros da CPLP tinham nas mais diversas áreas. Procurava-se assim obter benefícios mútuos num quadro alargado que ficou conhecido por "globalização da cooperação técnico-militar".

O aumento da cooperação levou à assinatura em 2006 do Protocolo de Cooperação da CPLP no Domínio da Defesa, tendo sido identificadas novas áreas de cooperação a serem desenvolvidas, nomeadamente, a preparação e o treino de unidades militares que possibilitassem a participação no quadro de operações huma-

9 Refere-se ainda a presença de outros contribuidores, como a União Europeia, o Reino Unido, o Canadá, os EUA e a Alemanha.

10 Não obstante existirem ainda graves lacunas, como é o exemplo da deficiente unidade de Comando e Controlo, das grandes diferenças no treino e nas capacidades dos diversos contingentes nacionais, na ausência de logística conjunta e combinada, etc.

nitárias e de manutenção de paz; a criação e sustentação de estabelecimentos de ensino militar para utilização comum; a realização de ciclos de conferência anuais sobre segurança e defesa; e a criação do Centro de Análise Estratégica (CAE).

A preparação e o treino de unidades militares que possibilitassem a participação em operações de apoio à paz no âmbito das organizações regionais e sub-regionais africanas[11], bem como a necessidade de formação dos militares que as integrariam, deu origem à aprovação na CPLP do "Programa Integrado de Intercâmbio no Domínio da Formação Militar", ao desenvolvimento de "Centros de Excelência" de formação de formadores (como é o exemplo da criação do Centro de Instrução de Operações de Apoio à Paz, em Angola) e ao "Programa Integrado de Exercícios Militares Combinados no Âmbito da CPLP" (este último materializado na condução anual de exercícios da série "Felino").

Neste âmbito, mas ao nível nacional, destaca-se a aprovação em 2006 pelo governo português do Programa de Apoio às Missões de Paz em África (PAMPA). Este programa, inspirado no seu congénere francês RECAMP, desenvolve-se em torno de quatro grandes eixos de ação (PAMPA, 2006: 1):

- 1.º Eixo – Capacitação institucional no âmbito da segurança e defesa, apoiando para isso os processos de reestruturação da Estrutura Superior da Defesa e das Forças Armadas dos PALOP;
- 2.º Eixo – Formação de militares dos países africanos. Constituindo este eixo uma componente fundamental do PAMPA, pretende desenvolver programas de formação e instrução militar com vista à valorização do fator humano das forças armadas dos PALOP;
- 3.º Eixo – Cooperação com organizações regionais e sub-regionais africanas, sendo explicitado no programa a intenção de apoiar a capacitação dos PALOP na área das operações de manutenção de paz e humanitárias, com vista à sua participação em ações desenvolvidas pela União Africana, pela SADC, pela CEDEAO, ou mesmo pela CPLP.
- 4.º Eixo – Mobilização da agenda africana nas políticas e estratégias das organizações de segurança e defesa (em particular NATO e UE), no sentido de garantir a prossecução de políticas e estratégias direcionadas ao apoio à Reforma do Setor de Segurança (RSS) em África e que isto seja conseguido, preferencialmente, através da incorporação nestas organizações do conhecimento, da experiência e da visão portuguesas.

11 Nomeadamente a União Africana, a ECOWAS, a ECCAS e a SADC.

Conclusões

A globalização, o aumento da importância dos atores regionais, o emergir de novas potências económicas e a multiplicação de atores no sistema internacional, tem levado à diminuição da capacidade de intervenção dos Estados no sistema internacional. Esta situação obrigou a uma alteração na forma como os Estados se relacionam entre si, potenciando a importância da cooperação na política externa dos Estados com o objetivo de defenderem os seus interesses estratégicos.

Portugal não é exceção e tem desenvolvido nos últimos anos intensos esforços no sentido de maximizar as suas atividades de cooperação nos diversos domínios, tendo na afirmação da língua portuguesa no mundo o elemento catalisador de todas estas ações de cooperação.

A UE, as Nações Unidas, a NATO, a OSCE, os EUA e a CPLP são referenciados nos principais documentos estruturantes da política externa portuguesa como fazendo parte do espaço estratégico conjuntural. Mas é a CPLP, e em particular os PALOP, que constituem o laboratório privilegiado para as ações de cooperação portuguesas com vista à projeção do país nas outras organizações internacionais a que pertence, nomeadamente na União Europeia.

A cooperação no domínio da defesa, como parte integrante da política externa portuguesa, obedece às mesmas linhas gerais de atuação, tendo a Cooperação Técnico-Militar vindo a desempenhar um papel fulcral ao longo dos anos. Assim, a defesa dos interesses estratégicos de Portugal aconselha a um aumento da cooperação com outros países ou organizações presentes em África que façam parte do espaço estratégico de interesse conjuntural português, como por exemplo a União Europeia e os EUA, de forma a contrariar interesses concorrentes de outros países, como sejam a China ou a Rússia. Contudo, a opção pelo tipo de cooperação no domínio da defesa a desenvolver é distinta consoante os atores que estão em causa.

Em relação à cooperação bilateral portuguesa em defesa com os PALOP, espelhada nos programas-quadro, poderemos dizer que tem vindo a "globalizar-se" e, embora na sua maioria ainda seja bilateral, tem sido cada vez mais integrada numa abordagem bi-multilateral no âmbito da CPLP. A evolução da cooperação bilateral neste sentido é a que nos parece mais acertada, pois permite maximizar as capacidades dos vários países em benefício mútuo, onde Portugal, a par do Brasil, conseguirá assumir um papel de liderança. Naturalmente que a clara ascensão do Brasil como potência global, implicará um aprofundar da relação com este país lusófono num conjunto de áreas, incluindo a cooperação em segurança e defesa.

Já no caso da cooperação com África no âmbito da União Europeia, a opção de cooperação bi-multilateral com a União Europeia apresenta vantagens, mas também desvantagens. Como vantagens refere-se a possibilidade de cativar recursos e ao mesmo tempo de se afirmar no seio da UE como ator importante na cooperação

com África, permitindo assim minimizar as desvantagens comparativas portuguesas, nomeadamente os escassos recursos que dispõe, e maximizar as suas vantagens comparativas, em particular a língua, a história e a cultura que partilha com os PALOP. Apesar disso, a cooperação bi-multilateral também apresenta grandes problemas, pois existe sempre o perigo de Portugal perder a influência que tem junto dos PALOP e de ver as suas ações diluídas numa cooperação direta com a União Europeia, ou com outros países da União Europeia com maior capacidade de intervenção, como sejam a França e a Inglaterra, e cujos interesses assentam na expansão, respetivamente, da francofonia e anglofonia.

Esta dualidade aconselha que Portugal tenha opções distintas consoante a situação em causa. No nosso entender, deverá desenvolver uma cooperação bi-multilateral com a União Europeia nas áreas em que possa liderar os projetos (incluindo os que tenham a participação de outros países europeus), obtendo assim acesso a fundos que de outra forma não conseguiria. Mas deve optar por outra solução nas situações em que não consiga maximizar as suas vantagens comparativas. Nestes casos, a opção de cooperação trilateral com os EUA (que têm especial interesse no Golfo da Guiné), apresenta-se como uma alternativa bastante viável, pois permite contrapor os interesses de outros atores europeus, nomeadamente franceses e ingleses. É, no entanto, fundamental que nestas situações sejam evitadas eventuais tentativas de subalternização da participação portuguesa.

Em termos de áreas de atuação, consideramos que a formação é sem dúvida uma área fulcral para os interesses de Portugal, pois aliada à grande competência, ao conhecimento e experiência que os militares portugueses já adquiriram com os anos da CTM, existe ainda a facilidade no relacionamento com os países beneficiários da cooperação (em relação a outros atores), quer seja por motivos relacionados com a língua em comum, quer seja pela história e cultura que nos liga aos PALOP.

Assim, consideramos que o desenvolvimento dos projetos no âmbito do PAMPA permite, mediante as situações, fazer a opção entre a bi-multilateralidade ou a trilateralidade descrita atrás, nomeadamente no que respeita à formação de militares dos PALOP e ao treino das respetivas unidades com vista à participação em Operações de Manutenção de Paz e Humanitárias no âmbito da *African Standby Force* da União Africana e das Brigadas da SADC, da CEDEAO ou da ECCAS.

Nesse sentido, o desenvolvimento de "Centros de Excelência" de formação de formadores distribuídos pelos PALOP, no âmbito da CPLP, com vista a permitir a sua utilização por outros países africanos pertencentes às três organizações subregionais com interesse para a CPLP, representa também uma mais-valia que deve ser explorada. Apresentamos como exemplo o Centro de Instrução de Operações de Apoio à Paz em Angola, muito embora reconheçamos que não é fácil competir com os centros congéneres francófonos e anglófonos.

De forma resumida, poderemos concluir que a área primordial para cooperação portuguesa em defesa em África deverá ser a formação, sendo a opção pelo tipo de cooperação no domínio da defesa agrupada em três grandes tipos:

- Abordagem bi-multilateral no âmbito da CPLP com Portugal, a par do Brasil, a liderar;
- Cooperação bi-multilateral com a União Europeia nas áreas em que Portugal possa liderar os projetos, com o objetivo de se afirmar no seio da UE como ator importante na cooperação com o continente africano e ao mesmo tempo cativar recursos de que tanto necessita;
- Cooperação trilateral com os EUA como forma de evitar que as suas ações sejam diluídas numa cooperação direta com a União Europeia. No entanto, deveram ser acauteladas eventuais tentativas de subalternização da participação portuguesa.

Desta forma, a opção pela cooperação internacional em defesa assente na bi-multilaterização e na trilaterização permite contribuir para a afirmação de Portugal na CPLP e na União Europeia, bem como para a sua projeção no mundo.

Bibliografia

Amado, Luis (2010). *A Política Externa Portuguesa: Pilares da Estratégia Nacional*. Lisboa: Prefácio.

Astor, Luis Díaz-Bedia (2008). "La Política de Securidad de Estados Unidos na África Subsahariana". *Revista General de Marina*, março de 2008, pp. 18-24.

Bernardino, Luís Manuel Brás (2008a). "A Comunidade dos Países de Língua Portuguesa: Uma Década de Segurança e Defesa". *Revista Militar*, abril de 2008, pp. 11-16.

Bernardino, Luís Manuel Brás, (2008b). *Estratégias de Intervenção em África.* Lisboa: Prefácio.

Berschinski, Robert G. (2007). *Africom's Dilema: The "Global War on Terrorism", "Capacity Building", Humanitarianism, and the Future of U.S. Security Policy in Africa*. Carlisle: Strategic Studies Institute, U.S. Army War College.

Bogland, Karin e Egnell, Robert (2008). *The African Union – A Study Focusing on Conflict Management*. Stockholm: FOI - Swedish Defence Research Agency.

Cardoso, Fernando e Ferreira, Patrícia (2005). *A África e a Europa: Resolução de Conflitos, Governação e Integração Regional*. Lisboa: Instituto Estudos Estratégicos Internacionais.

Carriço, Alexandre (2008). "A China em África e o Caso da Cooperação Sino Moçambicana" (Parte 1). *Revista Militar*, fevereiro 2008. Disponível em http://www.revistamilitar.pt/modules/articles/article.php?id=241> [Acedida em 18 de janeiro de 2012].

Carter, Phillip (2009). *U.S. Policy in Africa in the 21st Century*. Washington, DC: The Africa Center for Strategic Studies. Disponível em http://www.state.gov/p/af/rls/rm/2009/117326.htm> [Acedida em 17 de fevereiro de 2012].

Cilliers, J. (2004). *Human Security in Africa: A Conceptual Framework for Review*. Disponível em http:// www.africanreview.org> [Acedida em 20 de janeiro de 2012].

Combined Joint Task Force–Horn of Africa. *About the Combined Joint Task Force–Horn of Africa.* [em linha] Disponível em http://www.hoa.africom.mil/> [Acedida em 17 de janeiro de 2012].

Conselho de Ministros (2003). *Conceito Estratégico da Defesa Nacional*. Lisboa: Resolução do Conselho de Ministros n.º 6/2003. [em linha] Disponível em http://www.emfa.pt/www/conteudos/informacaofa/legislacao/DefesaNacional/ConceitoEstrategicodeDefesaNacional.pdf> [Acedida em 24 de janeiro de 2012].

Conselho de Ministros (2005). *Uma Visão Estratégica para a CooperaçãoPportuguesa*. Lisboa: Resolução da Presidência de Conselho de Ministros n.º 196/2005 de 24 de novembro. Disponível em http://dre.pt/pdf1sdip/2005/12/244B00/71807201.PDF> [Acedida em 18 de janeiro de 2012].

Conselho de Ministros (1999). *A Cooperação Portuguesa no Limiar do Século XXI*. Lisboa: Resolução da Presidência de Conselho de Ministros n.º 43/1999 de 29 de abril. XIII Governo. Disponível em http://ns1.ipad.mne.gov.pt/images/stories/legislacao/res43-1999-secXXI.pdf> [Acedida em 27 de janeiro de 2012].

Conselho de Ministros (2010). *Grandes Opções do Plano 2010-2013*, Lisboa. XVIII Governo. Disponível em http://www.parlamento.pt/OrcamentoEstado/Documents/gop/GOP_2010-2013_VF.pdf> [Acedida em 24 de fevereiro de 2012].

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

Comunidade dos Países de Língua Portuguesa (1998). *Iª Reunião dos Ministros da Defesa*. Lisboa: CPLP.

Comunidade dos Países de Língua Portuguesa (1999). *IIª Reunião dos Ministros da Defesa*. Lisboa: CPLP.

Comunidade dos Países de Língua Portuguesa (2006). *Protocolo de Cooperação da CPLP no Domínio da Defesa*. Praia: CPLP.

Comunidade dos Países de Língua Portuguesa (2010). *Estatutos da Comunidade dos Países de Língua Portuguesa*. CPLP.

Comunidade dos Países de Língua Portuguesa. *Sobre a CPLP*. Disponível em http://www.cplp.org/id-45.aspx> [Acedida em 10 de janeiro de 2012].

Comunidade dos Países de Língua Portuguesa. *Objetivos do CAE*. Disponível em http://www.caecplp.org/quem_somos/index.html> [Acedida em 12 de fevereiro de 2012].

Cruz, António Martins da (2009). *Portugal no Mundo*: *Pilares de uma Estratégia Nacional*. Lisboa: IDN.

Dougherty, J. e Pfaltzgraff, R.L. (2003). *Relações internacionais – As Teorias em Confronto*. Lisboa: Gradiva.

Direção Geral de Política de Defesa Nacional (1999). *Súmula n.º 61– Relações Bilaterais na Área da Defesa e Militar com Países da Europa, do Magrebe, EUA, Brasil e também China*. Lisboa: Direção Geral de Política de Defesa Nacional do Ministério da Defesa Nacional.

Economic Community of Central African States. *About ECCAS*. Disponível em http://www.ceeac-eccas.org> [Acedida em 5 de janeiro de 2012].

European Center for Development Policy Management (2009). "A Estratégia Conjunta UE-África: Dez Desafios para o Sucesso". *InBrief n.º 23 de março*. Maastricht: ECDPM

Economic Community of West African States (s.d). *About ECOWAS*. Disponível em http://www.comm.ecowas.int> [Acedida em 5 de janeiro de 2012].

Energy Information Administration (s.d.). *Country Analysis Brief China.* Disponível em http://www.eia.doe.gov/emeu/cabs/China/Background.html> [Acedida em 12 de janeiro de 2012].

EURORECAMP (s.d.). *About AMANI AFRICA – EURORECAMP.* Disponível em http://www.amaniafricacycle.org/spip.php?article2> [Acedida em 12 de janeiro de 2012].

Fanta, Emmanuel (2009). *The Capacity of African Regional Organisations in Peace and Security*. Florence: European University Institute. Disponível em http://erd.eui.eu/media/fanta.pdf> [Acedida em 12 de fevereiro de 2012].

Ferreira, Manuel Ennes (2009). "O gás africano e o cerco russo". *Expresso*, 18 de julho de 2009.

Ford, Neil (2007). "Power Struggle". *Jane's Intelligence Review*, janeiro, pp.15-17.

Forum on China-Africa Cooperation. Disponível em http://www.fmprc.gov.cn/zflt/eng/> [Acedida em 20 de janeiro de 2012].

Held, David; Mcgrew, Anthony; Golblatt, David e Perratton, Jonathan (1999). *Global Transformations: Politics, Economics and Culture*. Stanford: Stanford University Press.

Huntington, Samuel P. (2003). "America in the World". *The Hedgehog Review*, Spring, pp.17-22.

Ihonvbere, Julius O. (1994). "Pan-Africanism: Agenda for African Unity in the 1990s". *The All-African Student's Conference*. Peter Clark Hall, University of Guelph, Ontario, Canada.

International Institute for Strategic Studies (2008). "Russia. Arms Trade". *The Military Balance 2008*.

International Institute for Strategic Studies (2009). "Russia Arms Trade". *The Military Balance 2009*.

Instituto Português de Apoio ao Desenvolvimento (2004). *O que é a APD?* Lisboa: IPAD.

Instituto Português de Apoio ao Desenvolvimento (2010). *Estratégia Portuguesa de Cooperação Multilateral*. Lisboa: IPAD.

Jesús, Carlos Echeverría (2010). "El Papel de las Grandes Potencias con una Proyección Significativa en África Subsahariana". *Monografías del CESEDEN* n.º 117, maio, pp. 20-27.

Jiang, Wenran (2007). "Hu's Safari: China's Emerging Strategic Partnership in Africa". *China Brief* Volume: 7 Issue: 4, pp.21-25.

Klingebiel, S.; Blohm, T.M. e Eckle, R. (2008). *Donor Contributions to the Strengthening of the African Peace and Security Architecture*. Bonn: German Development Institute (DIE).

Landsberg, Christopher (2004). *The Fifth Wave of Pan-Africanism. Adebajo, West Africa's Security Challenges – Building Peace in a Troubled Region*. Boulder: Lynne Rienner.

Lake, Anthony e Tood, Whitman Christine (2005). *More than Humanitarianism: A Strategic U.S. Approach Toward Africa*. Independent Task Force Report nº56, Council on Foreign Relations.

Marchueta, Maria Regina, (2003). *A CPLP e seu Enquadramento*. Lisboa: Instituto Diplomático, Ministério dos Negócios Estrangeiros.

Martins, Vasco (2010). "BRICing Angola: Russia steps". *IPRIS - Lusophone Countries Bulletin*, janeiro, pp.13-17.

Ministério da Defesa Nacional (2006). *Programa de Apoio às Missões de Paz em África*. Lisboa: MDN.

Ministério da Defesa Nacional (2008). *Anuário Estatístico da Defesa Nacional 2008*. Lisboa: Ministério da Defesa Nacional.

UK Ministry of Defence (2001). *Paper 2 - Multinational Defence Cooperation*. London.

Monjardino, Carlos Valente (2002). *A Comunidade dos Países de Língua Oficial Portuguesa*. Lisboa: Academia Internacional da Cultura Portuguesa.

Moreira, Adriano (2009). "A Língua e o Conceito Estratégico Português" em *Pilares da Estratégia Nacional*. Lisboa: Instituto da Defesa Nacional/Prefácio.

Nathan, Laurie (2010). "The Peacemaking Effectiveness of Regional Organizations". *Centre, C.S.R. Working Paper no. 81 - Global and Regional Axes of Conflict*, London: Department for International Development.

NATO (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisboa: NATO.

Ney, Joseph S. Jr (2002). *Compreender os Conflitos Internacionais – Uma Introdução à Teoria e à História*. Lisboa: Gradiva.

Obama, P.E. (2009). "President addresses the Ghanaian Parliament in Accra". Office of the Press Secretary.

ONGD Plataforma Portuguesa (2010). *A Estratégia Conjunta África-UE: Análise e Desafios da implementação*. Lisboa: IPAD.

ONU (2003). *Human Security – Now*. New York:UN.

ONU (2003). *United Nations Peace Operations 2009 year in review*. New York: UN.

Pout, Christian E. B. (2007). "The European Union (EU): African Peace and Security Environment's Champion?". *Poits de vue*, Fondation pour la Recherche Stratégique.

Quivy, Raymond e Campenhoudt, Luc Van (2003). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

RECAMP. *About RECAMP.* Disponível em http://www.un.int/france/frame_anglais/france_and_un /france_and_peacekeeping/recamp_eng.htm> [Acedida em 20 de fevereiro de 2012].

Rios, Xulio (2008). *China-África: el Modelo de Pekín*. Instituto Galego de Análise e Documentación Internacional.

Roque, Fátima Moura (2007). *África, a NEPAD e o Futuro*. Luanda: Texto Editores.

Southern African Development Community. *About SADC.* Disponível em http://www.sadc.int/> [Acedida em 24 de janeiro de 2012].

Sautman, Barry V (2006). "Friends and Interests: China's Distinctive Links with Africa". Working Paper No. 12. Center on China's Transnational Relation.

Serafino, Nina M. (2006). *The Global Peace Operations Initiative: Background and Issues for Congress.* CRS Report for Congress.

Teixeira, Nuno Severiano (2009). *Contributos para uma Política de Defesa: julho de 2006 a julho de 2009*. Lisboa: Ministério da Defesa Nacional.

União Africana (2000). *Ato constitutivo da UA*. Lomé: União Africana.

União Africana (2003). *Protocol on Amendments to the ConstitutiveAact of the African Union*. União Africana.

União Africana. *AU in a Nutshell.* Disponível em http://www.au.int/en/about/nutshell> [Acedida em 18 de fevereiro de 2012].

UE-UA (2007). *The Africa-EU Strategic Partnership: A Joint Africa-EU Strategy*. Lisboa: UE-UA.

USAFRICOM. *About United States Africa Command*. Disponível em http://www.africom.mil/> [acedida em 12 de janeiro de 2012].

US Department of State. *IMET.* Disponível em http://www.state.gov/t/pm/ppa/sat/c14562.htm> [Acedida em 06 de fevereiro de 2012].

Wissenburg, Marcel (2009). *Political Pluralism and the State – Beyond Sovereignty.* New York: Routledge.

REVISTA NAÇÃO E DEFESA

Números temáticos publicados

1998	84	Inverno	Uma Nova NATO numa Nova Europa
	85	Primavera	Portugal e o Desafio Europeu
	86	Verão	O Desafio das Águas: Segurança Internacional e Desenvolvimento Duradouro
	87	Outono	O Estado em Mudança
1999	88	Inverno	Mulheres nas Forças Armadas
	89	Primavera	Portugal na NATO: 1949-1999
	90	Verão	Economia & Defesa
	91	Outono	Operações de Paz
2000	92	Inverno	Portugal e as Operações de Paz na Bósnia
	93	Primavera	Novos Rumos da Educação para a Cidadania
	94	Verão	Democracia e Forças Armadas
	95/96	Outono-Inverno	Prevenção de Conflitos e Cultura da Paz
2001	97	Primavera	Nova Ordem Jurídica I nternacional
	98	Verão	Forças Armadas em Mudança
	99	Outono	Segurança para o Século XXI
	100	Inverno	De Maastricht a Nova Iorque
2002	101	Primavera	Europa e o Mediterrâneo
	102	Verão	Repensar a NATO
	103	Outono-Inverno	Novos Desafios à Segurança Europeia
	Extra	Dezembro	Cooperação Regional e a Segurança no Mediterrâneo (C4)
2003	104	Primavera	Evolução das Nações Unidas
	Extra	Abril	A Revolução nos Assuntos Militares
	105	Verão	Soberania e Intervenções Militares
	106	Outono-Inverno	A Nova Carta do Poder Mundial
2004	107	Primavera	Forças Armadas e Sociedade. Continuidade e Mudança
	Extra	Julho	Educação da Juventude. Carácter, Liderança e Cidadania
	108	Verão	Portugal e o Mar
	109	Outono-Inverno	Segurança Internacional & Outros Ensaios
2005	110	Primavera	Teoria das Relações Internacionais
	111	Verão	Raymond Aron. Um Intelectual Comprometido
	112	Outono-Inverno	Número não Temático
2006	113	Primavera	Número não Temático
	114	Verão	Segurança na África Subsariana
	115	Outono-Inverno	Portugal na Europa Vinte Anos Depois

2007	116	Primavera	Número não Temático
	117	Verão	Número não Temático
	118	Outono-Inverno	Políticas de Segurança e Defesa dos Pequenos e Médios Estados Europeus
2008	119	Primavera	Transição Democrática no Mediterrâneo
	120	Verão	Número não Temático
	121	Outono-Inverno	Estudos sobre o Médio Oriente
2009	122	Primavera	O Mar no Pensamento Estratégico Nacional
	123	Verão	Portugal e a Aliança Atlântica
	124	Outono-Inverno	Que Visão para a Defesa? Portugal-Europa-NATO
2010	125	Primavera	Visões Globais para a Defesa
	126		O Conceito Estratégico da NATO
	127		Dinâmicas da Política Comum de Segurança e Defesa da União Europeia
2011	128		O Mar no Espaço da CPLP
	129		Gestão de Crises
	130		Afeganistão
2012	131		Segurança em África
	132		Segurança no Mediterrâneo

Política Editorial

Nação e Defesa é uma publicação periódica do Instituto da Defesa Nacional que se dedica à abordagem de questões no âmbito da segurança e defesa, tanto no plano nacional como internacional. Assim, *Nação e Defesa* propõe-se constituir um espaço aberto ao intercâmbio de ideias e perspectivas dos vários paradigmas e correntes teóricas relevantes para as questões de segurança e defesa, fazendo coexistir as abordagens tradicionais com as problemáticas de segurança mais recentes.

A Revista dá atenção especial ao caso português, sendo um espaço de reflexão e debate sobre as grandes questões internacionais com reflexo em Portugal e sobre os interesses portugueses, assim como sobre as grandes opções nacionais em matéria de segurança e defesa.

Editorial Policy

Nação e Defesa (Nation and Defence) is a journal edited by the portuguese National Defence Institute, dedicated to questions in the area of security and defence both at a national and international level. Thus, *Nação e Defesa* aims to constitute an open forum for the exchange of ideas and views of the various paradigms and theoretical approaches relevant to security and defence issues.

The publication pays special attention to the portuguese situation, being a space for reflection and debate over the broad choices that Portugal faces in terms of security and defence, as well as on important international matters with potential impact over the portuguese interests.

NORMAS DE COLABORAÇÃO

O artigo proposto para publicação deverá ser enviado via correio electrónico para idn.publicacoes@defesa.pt
O texto terá de observar as seguintes normas:

- Ter entre 30.000 a 50.000 caracteres (espaços incluídos) em Word for Windows.
- Ser acompanhado de um resumo em português e em inglês (até 1000 caracteres cada).
- Ser redigido de acordo com a norma de Harvard
  disponível em http://libweb.anglia.ac.uk/referencing/harvard.htm

O artigo, sem indicação do autor e acompanhado pela Ficha de Identificação (disponível em http://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf) devidamente preenchida, será apreciado em regime de anonimato pelo Conselho Editorial da revista.

Os artigos aprovados pelo Conselho Editorial pressupõem o direito de publicação exclusiva na revista Nação e Defesa.

A revista Nação e Defesa poderá publicar artigos já editados noutras publicações mediante autorização por parte da respectiva Editora.

Todo o artigo publicado é da inteira responsabilidade do autor, sendo a revisão das provas tipográficas da responsabilidade do Instituto da Defesa Nacional.

O pagamento dos honorários aos autores (150 € por artigo) será efectuado por transferência bancária até 30 dias após a edição da revista. Cada autor receberá três exemplares da revista na morada indicada.

Os casos não especificados nestas Normas de Colaboração deverão ser apresentados ao Coordenador Editorial da Nação e Defesa.

PUBLICATION NORMS

The submitted article will have to be sent by email to idn.publicacoes@defesa.pt
The text should obey to certain requirements:

- It should have between 30.000 and 50.000 characters (spaces included), and must be presented as a Microsoft Word document.
- The author should provide an abstract of the article (until 1000 characters).
- Written according to the Harvard reference system available at
  http://libweb.anglia.ac.uk/referencing/harvard.htm

The article should not contain any reference to its author. The sole means of identifying the author is a duly filled ID form (http://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf), so its submission is compulsory.

The magazine's Editorial Board, on an anonymous basis, will appraise the text. The article's approval by the Editorial Board implies the possession of exclusive publishing rights by *Nação e Defesa*. The publication of non-exclusive articles by this magazine depends upon acknowledgment of the legitimate holder of the article's publishing rights.

The author shall hold full responsibility for the content of the published article. The *Instituto da Defesa Nacional* is responsible for the article's typographical revision.

The author's honorarium for each published article (150 €) will be paid by bank transfer up to 30 days after the article's publication. Three issues of the magazine will be sent to the address indicated in the ID form.

All cases not envisioned in these Norms should be presented to the Editorial Coordinator of *Nação e Defesa*.

NAÇÃO E DEFESA

Revista quadrimestral

Nome/Name _____

_____

Morada/Adress _____

_____

Localidade/City _____

Cód. Postal/Zip _____ - _____ _____

_____ NIF _____

Country _____

E-mail _____

Tel./Phone _____

☐ Renovação/Renewal – Assin. nº/Subscrip. nr. _____

☐ Nova assinatura/New subscription

Assinatura/Signature _____

Data/Date _____

Assinatura Anual/Annual Subscription (3 nºs /issues)

☐ Instituições/Institutions 40,00 €

☐ Individuais/Individuals 25,00 €

☐ Estudantes/Students 20,00 € (anexar comprovativo deste ano)

Números Anteriores/Previous Issues – 8,50 € cada/each + portes/ /postage charges

☐ ☐ ☐ ☐ ☐ ☐

Pré-Pagamento/Prepayment

☐ **Numerário**

☐ **Cheque** nº _____ Banco _____ à ordem do IDN

☐ **Transferência Bancária** NIB 0781 0112 0000 000 7777 20
(anexar comprovativo da Transferência)

☐ **Bank Transfer** (compulsory for foreign subscriptions)

IBAN – PT50 0781.0112 0000 000 7777 20
BIC (SWIFT) – IGCPPTPL

INSTITUTO DA DEFESA NACIONAL
Calçada das Necessidades, 5, 1399-017 Lisboa
PORTUGAL

www.idn.gov.pt
idn.publicacoes@defesa.pt
tel. + 351 21 392 46 00 Fax + 351 21 392 46 58