

“2011: A tipping point for Data Security”

Seminário AFCEA Portugal / McAfee

Embaixada dos Estados Unidos da América, 12 Out 2011

Discurso de Abertura proferido pelo Dr. António Figueiredo Lopes

1. Os desafios globais num mundo em transformação

Com o fim do “muro de Berlim” e o colapso do sistema comunista que vigorava no Leste Europeu, começou a soprar mais forte o vento da globalização e a revelar-se um panorama de mudanças e de muitas incertezas, que colocam a problemática da segurança no centro das preocupações das sociedades modernas.

O fim da bipolarização Leste-Oeste conduz inexoravelmente à emergência de uma nova ordem internacional marcada pelo aumento da interdependência dos Estados que passam a assumir novas posições. Neste contexto e desaparecidos os condicionamentos estruturais próprios da Guerra Fria que limitavam a sua margem de manobra, os Estados reconhecem a necessidade de aprofundar vínculos de interdependência e um multilateralismo eficaz.

Os acontecimentos que ocorrem em diferentes partes do sistema internacional afectam-se mutuamente e são cada vez menos as ameaças e conflitos tradicionais de natureza interestatal, surgindo progressivamente um novo tipo de conflitos infra-estatais e de ameaças e riscos transnacionais bem distintos das ameaças tradicionais.

Já em pleno séc. XXI, o sistema internacional sofre um novo abalo e é particularmente afectado pelos atentados terroristas de 11 de Setembro de 2001 em Nova Iorque e Washington e de 11 de Março de 2004 em Madrid, assim como, pouco depois, as bombas no Metro de Londres.

Os atentados às Torres Gémeas ocorrido em 11 de Setembro de 2001, em Nova Iorque, e ao Pentágono, em Washington, nesse mesmo dia, marcaram, efectivamente, o início de uma nova era mundial.

Em matéria de Segurança e Defesa, nada voltará a ser como antes devido aos efeitos deste rude golpe, desferido em pleno coração do Mundo Ocidental – um golpe cujas consequências se vêm, desde então, multiplicando por todo o globo, marcando de forma trágica o fenómeno da transnacionalização da insegurança, facilitada, além disso, pela globalização.

Os acontecimentos que ocorrem em diferentes partes do sistema internacional afectam-se mutuamente e, perante os complexos cenários de ameaças e riscos, de antiga e nova tipologia, cresce a sensação de vulnerabilidade e agudiza-se o sentimento de insegurança dos cidadãos.

Enquanto no passado as ameaças e conflitos tradicionais eram originadas por adversários politicamente identificados e geograficamente localizados, as novas ameaças têm na sua génese adversários múltiplos não identificados e de difícil localização.

A maior parte das ameaças à segurança dos Estados e dos cidadãos nos tempos de hoje, não são de natureza militar nem resultam de disputas de fronteiras. São antes problemas de natureza económica e social; são os conflitos étnicos e os antagonismos religiosos; são os estados frágeis que permitem as migrações clandestinas e os tráficos da droga e de seres humanos, são ainda o crime organizado, o terrorismo e a corrupção.

Por seu lado, a globalização, que é, sem dúvida, um factor de progresso e de desenvolvimento económico e social da humanidade, torna-se também fonte de sérias preocupações para a segurança. Com a abertura dos mercados e o derrube das fronteiras, constata-se que, a par do comércio e da livre circulação das pessoas, dos bens e das comunicações legais, se processa também a transacção de ameaças e riscos que se materializam no território nacional nas diversas formas de criminalidade que lhe está associada.

O efeito de aproximação gerado pela globalização surge, assim, também como causa de problemas que vão desde as crises financeiras até aos seus efeitos directos e indirectos sobre a segurança, fazendo com que ameaças e riscos longínquos gerem a mesma insegurança que aquelas que estão mais próximas. É o caso da recente recuperação do poder pelos talibãs no Afeganistão e a hipótese do domínio do Paquistão nuclear pelos fundamentalistas radicais. Trata-se de uma ameaça de tal modo grave que justifica a presença de forças multinacionais na área.

Também as alterações climáticas, a ecologia, a fome, as catástrofes humanitárias, as pandemias e a cibersegurança entram na área estratégica e passam a integrar o elenco de riscos e ameaças com que as sociedades modernas se confrontam.

2. A dimensão estratégica do ciberespaço

Vivemos, pois, num mundo em mudança acelerada provocada sobretudo pelos avanços que se verificam nas tecnologias de comunicação e informação, enquanto suporte da chamada sociedade do conhecimento. Uma sociedade cada vez mais dependente da Internet, com as consequentes vantagens e os correspondentes riscos e vulnerabilidades. Não admira por isso que o ciberespaço tenha adquirido uma dimensão estratégica evidente e a cibersegurança corresponda hoje a uma prioridade política no quadro da segurança nacional e internacional.

Os ciberataques às bases de dados – cuja análise não deixará de ser tecnicamente desenvolvida durante este seminário nas suas diversas vertentes - são hoje uma das mais temidas ameaças com que os Estados se confrontam dada a complexidade e dificuldade da defesa contra tal ameaça.

Segundo Joseph Nye, professor na Universidade de Harvard e autor do livro *The Future of Power* (O Futuro do Poder), “As maiores potências provavelmente não são capazes de dominar este campo do mesmo modo como dominam outros, como por exemplo o mar, a terra e o ar. Embora tenham maiores recursos, também são muito mais vulneráveis, e, nesta fase, o ataque é superior à capacidade de defesa, no ciberespaço.

Mesmo os grandes estados, como os Estados Unidos, a Rússia, a Grã-Bretanha, a França e a China, apesar de terem mais capacidade do que outros mais pequenos, ainda não detêm o domínio no ciberespaço. Na verdade, a dependência de complexos cibersistemas no que se refere ao suporte de actividades militares e económicas cria vulnerabilidades, mesmo nos Países mais poderosos.

O mesmo autor sublinha a importância e gravidade das novas ameaças cibernéticas com esta frase lapidar: “as montanhas e os oceanos são difíceis de mover, mas partes do ciberespaço podem ser conectadas e desconectadas com um simples click do rato”. Reconhecendo logo a seguir que “é mais barato e mais rápido mover electrões através do globo do que fazer com que enormes navios percorram as grandes distâncias dos oceanos.... Por outro lado, as barreiras de acesso ao ciberdomínio são tão insignificantes que pequenos Estados e entidades não-estatais podem produzir um impacto significativo, a um custo reduzido”.

Este autor e especialista de defesa – antigo Sub-secretário da Defesa dos EUA, em 1995 - considera a integridade e a capacidade de resistência do ciberespaço “como vital para a segurança e a economia, tendo em conta que a internet desempenha hoje um papel crítico na maioria dos aspectos da vida de cidadãos e das empresas, assim como na prestação de serviços públicos”.

Citando um outro especialista e investigador nestas áreas, se é certo que o século passado viu os exércitos envolverem-se em confrontos em terra, no mar e no ar, no século XXI, a ameaça de conflito já se alargou ao ciberespaço e é aí que tem de ser enfrentada.

Como é sabido, são cada vez mais frequentes e preocupantes as intromissões no ciberespaço, aproveitando as possibilidades que oferecem as novas tecnologias da informação e comunicação e o processo de globalização. De particular importância é a espionagem económica, que consiste na aquisição ilícita de informação, patentes ou tecnologias críticas, e procura exercer influência de modo ilegal em decisões políticas de carácter económico.

Há fortes evidências de que os criminosos, terroristas e espões se têm vindo a tornar cada vez mais qualificados e mais capazes de usar o espaço cibernético, num momento em que a maioria dos países está cada vez mais dependente do cyberespaço para funcionar.

A análise e a gestão do risco social associado ao ciberespaço, carecem, assim, de uma cuidada atenção, não só pelas vulnerabilidades decorrentes da crescente dependência

tecnológica das infra-estruturas críticas, mas também pela necessidade de serem criados instrumentos para sua protecção e segurança.

Como já foi dito, as ameaças ao ciberespaço incidem directamente sobre o bem-estar das populações, o normal funcionamento dos governos e das Instituições assim como a segurança dos Estados. A cibersegurança adquire, por isso, um lugar destacado nos documentos estratégicos que diversos Países têm vindo a adoptar nos últimos anos, ao reverem e actualizarem os conceitos e as políticas de segurança nacional, um conceito abrangente e compreensivo, incluindo capacidades militares e policiais (*security*), assim como a protecção e o socorro (*safety*).

Refiro-me, em particular, às novas Estratégias de Segurança Nacional dos EUA, da Grã Bretanha, da França e da Espanha, assim como o novo Conceito Estratégico da NATO e a Estratégia Europeia de Segurança. Ao constatarem a subida gradual da ameaça cibernética, os Governos destes Países fazem bem em colocá-la no topo das principais ameaças.

Assim, por exemplo, na sua *National Security Strategy*, a Grã Bretanha qualifica os ciberataques como uma ameaça de primeiro nível, ao lado do terrorismo internacional e dos conflitos convencionais.

Também na “Estratégia Espanhola de Segurança”, um documento recentemente aprovado pelo Governo espanhol e elaborado por um Grupo de especialistas coordenados por Javier Solana, antigo Alto Representante para a Política Estrangeira e de Segurança Comum da EU, é consagrado um longo capítulo à Ciberameaça reconhecendo que a economia, a estabilidade e prosperidade económica do país dependerão em boa medida da segurança do ciberespaço.

Os especialistas em segurança têm ainda muitas dúvidas quanto ao significado preciso de termos como "ataque, defesa, dissuasão ou guerra" no ciberespaço, porque se trata de um domínio em que estamos a dar os primeiros passos, mas poucos têm dúvidas de que as ameaças à cibersegurança são hoje bem mais graves e imprevisíveis do que eram há uma dezena de anos.

Faz, por isso, todo o sentido reflectir sobre esta nova realidade que é a entrada da cibersegurança na área estratégica, passando a integrar o elenco de riscos e ameaças com que a humanidade se confronta, neste mundo crescentemente interligado e em rede.

É um desafio fundamental para políticos e técnicos encontrar as melhores formas e meios de defender os nossos sistemas e infraestruturas críticas contra o ataque de cibercriminosos. Deste modo, está-se a promover ao mesmo tempo a confiança nas transacções electrónicas que nos dias de hoje assumem uma importância crítica para o comércio, as relações bancárias, a telemedicina, o governo electrónico e outras aplicações de grande utilidade para o bem-estar das populações. Reduzir o cibercrime pode trazer dividendos económicos substanciais para os nossos Países. Há um desafio que neste domínio se impõe que é o de

garantir aos investidores que podem desenvolver os seus negócios num País seguro, mesmo no domínio da cibersegurança.

Como tudo isso depende das práticas de segurança de cada país, empresa e cidadão utilizador destes importantes recursos, “precisamos de desenvolver uma cultura global de cibersegurança”, como muito bem recomendava o antigo Secretário-Geral das Nações Unidas, Kofi A. Annan.

Penso que estão assim certos os promotores deste Seminário subordinado ao tema principal “2011: tipping point for data security”, sublinhando o facto de que nos encontramos num ponto de viragem para a cibersegurança, quando verificamos, como já foi dito, que os ciberataques são uma ameaça cada vez mais ao dispor de possíveis agressores, podendo colocar em risco infra-estruturas críticas vitais, cuja destruição total ou parcial pode afectar, directa ou indirectamente, o funcionamento normal dos órgãos e estruturas do Estado e da Segurança Nacional assim como a actividade económica e a vida de milhões de cidadãos.