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