CIBER(IN)SEGURANÇA

João Afonso

A TECNOLOGIA DESENVOLVIDA nas últimas duas décadas não tem precedente na história da humanidade. O brilhantismo científico, tecnológico, empresarial, cultural e social trouxe consigo uma reorganização do espaço, do tempo e dos valores mais elementares da construção civilizacional, como a família, a religião e a vizinhança. Vivemos numa era de extremos, onde o desenvolvimento das sociedades do conhecimento e da informação tem um custo: a mundialização social, com a consequente queda de barreiras, que transforma os problemas locais em problemas globais. Giddens (2006, p. 29) diz-nos que as forças da globalização criaram algo que nunca existiu antes: "uma sociedade cosmopolita global" que agita a nossa forma de viver, qualquer que seja o local onde habitemos. "Somos a primeira geração a viver nesta sociedade, cujos contornos ainda mal conseguimos vislumbrar."

O novo espaço público (multidimensional)

Hoje, o espaço público não é apenas físico. O espaço das manifestações da vida em sociedade e do crime deixou de estar limitado às ruas das cidades e às zonas rurais. Ampliou-se e multidimensionou-se. Não é apenas físico mas também, e cada vez mais, virtual. Castells (2011, pp. 534-535) observa que ao *espaço* da tradicional teoria social, entendido como "o suporte material de práticas sociais de tempo compartilhado", devemos agora adicionar o *espaço de fluxos* da Era da Informação, que já não depende da contiguidade física para se materializar e ser entendido, também, como suporte material de práticas sociais.

As novas tecnologias comunicacionais e a Internet criaram grandes redes sociais, espaços de intercomunicabilidade, que teleportam a pessoa do mundo físico para o mundo da virtualidade. A sociabilização do mundo humano está em fase de grandes mudanças, dando origem a uma *sociedade de redes* ou *sociedade em rede*, construída em torno de fluxos que dominam a vida social. A pessoa está cada vez mais ausente do espaço físico, entregando-se a um *mundo virtual* em ascensão, que provoca um certo esvaziamento do *mundo teluriano*. Com isso, o tempo flui a uma velocidade alucinante em relação ao espaço: uma catástrofe no outro lado do mundo irrompe, em segundos, pelo nosso espaço doméstico.

> "As guerras do porvir reservaram já o seu espaço no mundo cibernético."

A sociedade cosmopolita global é ladeada por este mundo virtual, uma criação do brilhantismo tecnológico informático e informacional que absorve o espírito da sociabilidade física ou presencial. Há duas décadas, Hassemer (1995) falava de um narcisismo que esvazia as instituições de controlo social como a vizinhança, a escola, o espaço profissional, as quais, de forma crescente, perdem a sua força de fixação de normas sociais da vida em coletividade. O autor estava longe de imaginar a intensidade com que esse narcisismo social cria, hoje, o isolamento e o fim da solidariedade nas grandes metrópoles. O mundo virtual (ciberespaço) criado pelas tecnologias comunicacionais concebe um universo capaz de curvar, a seus pés, o espaço físico e o tempo presente. A pessoa está cada vez mais ligada *online* e desligada da vida. A vizinhança deixa de ser o conjunto de pessoas que vivem na "porta ao lado" e passa a ser o grupo de cibernautas que partilha o "meu" ciberespaço.

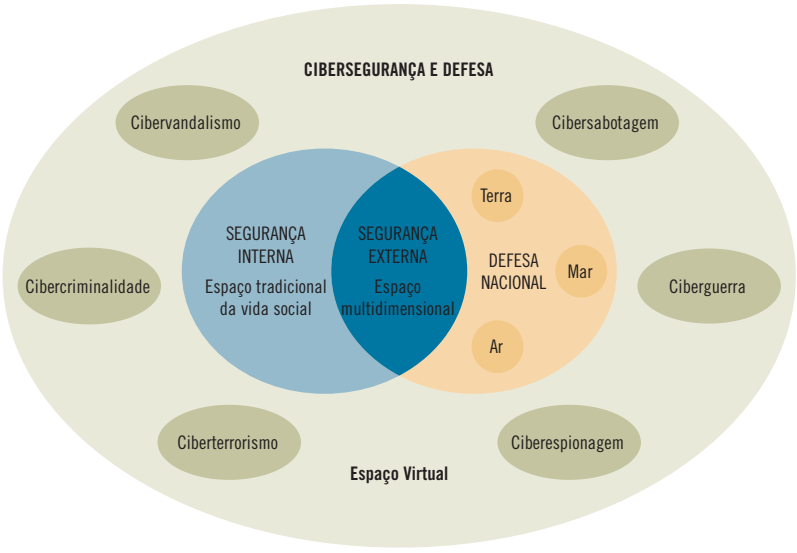
Perante o empobrecimento do espaço comum da vizinhança e a erosão do "nós teluriano", o cosmopolita — ou cidadão do mundo da era global — desprende o *espaço físico* do *espaço cívico*. O espaço público das metrópoles, enquanto universo *da* e *para* a civilização, vê-se agora confrontado com uma partilha do seu propósito, perdendo parte do instituto civilizacional para o ciberespaço. O cosmos virtual está em crescimento e assume, agora, uma relação com a civilização.

Da (in)segurança individual à (in)segurança do Estado

A pouco e pouco, o novo espaço público (cibermundo) substitui-se ao mundo físico-teluriano. Ambos formam a realidade espacial, o suporte das relações da vida social, onde se insere o crime, elemento ôntico-ontológico da sociedade humana. A materialidade perde a sua essência perante o crime cibernético, que já não depende do "bem corpóreo" ou do "dinheiro vivo". A criminalidade de massas do mundo teluriano é ainda predominante no princípio deste milénio, mas acreditamos que, no futuro, este tipo de criminalidade encontrará o seu espaço de eleição no universo virtual cibernético. Por exemplo, os ataques informáticos com *ransomware* são cada vez mais comuns e atingem já proporções preocupantes.

Mas, como o crime, a guerra é tal-qualmente um elemento epistemológico do mundo humano. Por isso, a (nova) configuração espácio-temporal do mundo cibernético das sociedades cosmopolitas influencia não apenas o processo evolutivo da instituição policial e das formas de produção do bem e valor *segurança interna*, mas, também, as instituições estatais de *defesa nacional* contra ataques externos. O ciberespaço junta-se, assim, aos tradicionais espaços de atuação militar: terra, mar e ar.

A segurança do ciberespaço constitui uma preocupação séria e é, quiçá, um dos maiores desafios para a continuidade dos Estados. As guerras do porvir reservaram já o seu espaço no mundo cibernético. O vírus *Stuxnet*, que afetou a indústria nuclear iraniana em 2010, abriu esse



Espaço multidimensional da segurança nacional
Fonte: Autor.

SEGURANÇA NACIONAL DO CIBERESPAÇO

A invisibilidade e liquidificação dos perigos cibernéticos eliminam toda a dimensão espacial da segurança, que deixa de caracterizar-se como interna ou externa: é ubíqua e distópica ao mesmo tempo.

Um ciberataque bélico ou criminoso não é necessariamente geolocalizado, como o é um ataque convencional. A característica de disseminação dum ataque cibernético não permite que haja uma resposta imediata por parte da instituição ou do Estado atingido. A estratégia de segurança fica assim limitada a um sistema de prevenção, impossibilitando a estruturação de medidas para ripostar e neutralizar a ameaça.

Ciente da seriedade desta matéria e do difícil compromisso de proteção do ciberespaço que tem pela frente, o Estado português tem-se apressado nos últimos anos a criar mecanismos eficazes de prevenção. Com o Decreto-Lei n.º 69/2014, de 9 de maio, criou o Centro Nacional de Cibersegurança no seio do Gabinete Nacional de Segurança, perspetivando a sua completa autonomização. Através da Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, lançou a Estratégia Nacional de Segurança do Ciberespaço. O Decreto-Lei n.º 136/2017, de 6 de novembro, alargou os quadros de pessoal especializado do Centro Nacional de cibersegurança. Preconizou a edificação ao nível das Forças Armadas de uma capacidade de ciberdefesa, através da Orientação Política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, de 11 de outubro, com a criação de um Centro de Ciberdefesa, no âmbito do Estado-Maior General das Forças Armadas.

A segurança do ciberespaço é, hoje, parte integrante da segurança nacional, sendo essencial para o funcionamento do Estado. Este moderno conceito — que passa por garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, de forma a evitar colapsos no plano económico e social — integra-se, por isso, nas tarefas fundamentais do Estado, prescritas no artigo 9.º da Constituição da República Portuguesa, em especial nas suas alíneas *a)* a *d)*.

caminho, sendo mundialmente conhecido pela sua particularidade: não teve quaisquer pretensões de infetar computadores domésticos ou atingir pessoas e instituições, mas sim um Estado. A empresa Kaspersky Lab (2010) afirma que o "*Stuxnet* é um protótipo funcional e temível de uma ciberarma que levará à criação de uma nova corrida armamentista no mundo", sendo o próximo passo da escala evolutiva da negrura, perversidade e malignidade cibernéticas: a década de 1990, marcada pelo cibervandalismo; a de 2000, pela cibercriminalidade; a década de 2010, manchada pelo ciberterrorismo, ciberarmas e ciberguerra.

Este tipo de ataque cibernético a infraestruturas estratégicas dos Estados multiplicou-se. Empresas petrolíferas, energéticas, metalúrgicas, de transportes urbanos, instituições governamentais ou bancárias passaram a ser alvos favoritos. Em 23 de dezembro de 2015 deu-se o primeiro ciberataque a uma rede elétrica de um Estado. Três companhias de energia foram atacadas na Ucrânia por um *malware* conhecido por *BlackEnergy*. As suspeitas viraram-se para a Rússia.

Em jeito de retaliação pela ocupação da Crimeia por parte da Rússia, um grupo de pessoas fundou a InformNapalm, uma organização internacional de voluntários, criada em março de 2014, que luta nas linhas da frente duma guerra informacional. Em 2016, a seguir ao ataque do *BlackEnergy*, formaram *backing-grupos* (Falcons Flame, Trinity, RUH8) com o objetivo de atingir a Rússia em diversas vertentes, passando de uma simples guerra de informação a uma autêntica guerra cibernética. Iniciou-se uma guerra híbrida: física e virtual, no terreno e no teclado. Esta última, uma guerra sem armas, sem disparos, é certo. Mas uma guerra de códigos maliciosos e *exploits* com potencial tão ou mais destrutivo que a guerra convencional.

O primeiro impulso foi dado, o palco está montado. A partir destes episódios, só podemos esperar novos casos. E não faltam voluntários para participar nesta espécie de *virtual reality videogame*. Se a contratação de *hackers* para ciberfraudes é hoje uma realidade, só podemos esperar que, no futuro próximo, um conjunto de mercenários se ofereçam como *backing-freelancers* numa qualquer guerra virtual entre Estados.

Os desafios duma (ciber)segurança sem dimensão

Os desafios da segurança do ciberespaço são complexos. A indústria ou a economia dum país está à mercê destes ataques invisíveis, sem possibilidade de ripostar. A invisibilidade e a liquidificação dos perigos cibernéticos eliminam toda a dimensão espacial da segurança, que deixa de caracterizar-se como interna ou externa: é ubíqua e distópica ao mesmo tempo. Todos os Estados estão em perigo! A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, expressa bem a consciência da União nesta matéria. Os efeitos dos ataques cibernéticos fazem sentir-se de forma séria no mundo real, impondo-se por isso a implementação de medidas eficazes de prevenção.

O Centro Nacional de Cibersegurança de Portugal foi criado em 2014, no seio do Gabinete Nacional de Segurança, para proteger o Estado das macrodimensões que se constituem como epifenómenos do mundo cibernético: a ciberespionagem, a ciberdefesa, o cibercrime e o ciberterrorismo. O mundo está mais diferente do que nunca. As metamorfoses do *perigo* e do *risco* exigem novas proteções e defesas. O próprio conceito de *ataque* sofreu alterações. Enquanto o ataque convencional, fixado no tempo e no espaço, é dirigido ou cirúrgico, já o ataque virtual pode formar-se a partir da combinação de diversas modalidades e dimensões: concentrado ou difuso, instantâneo ou continuado, destrutivo ou disruptivo, localizado ou ubíquo.

Quiçá a tecnologia para a prevenção e repressão da criminalidade informática venha a integrar o conceito de *polícia*, assumindo o termo de *ciberpoliciamento*. E talvez a da defesa militar contra investidas bélicas, navegando no novo espaço público, cunhe o conceito de *ciberarmada*. O futuro o dirá brevemente. ■

Referências

CASTELLS, Manuel (2011). *A Era da Informação: Economia, Sociedade e Cultura. A Sociedade em Rede*. Trad. Alexandra Lemos, Catarina Lorga e Tânia Soares. Vol. I, 4.ª edição, Lisboa: Fundação Calouste Gulbenkian. Título original: *The Rise of the Network Society*, 1996.

GIDDENS, Anthony (2006). *O Mundo na Era da Globalização*. Trad. Saul Barata. 6.ª edição, Lisboa: Editorial Presença. Título original: *Runaway World*, 1999.

HASSEMER, Winfried (1995). *A Segurança Pública no Estado de Direito*. Trad. Carlos Eduardo Vasconcelos. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 1995. Título original: *Innere Sicherheit im Rechtsstaat*, 1993.

Kaspersky Lab, comunicado de imprensa de 24 de setembro de 2010, intitulado "Kaspersky Lab provides its insights on Stuxnet worm". Disponível em www.kaspersky.com (consult. em março de 2018).