RECENSÃO

O MUNDO DA CIBERNÉTICA LETAL
NOVAS AMEAÇAS E SEGURANÇA INTERNACIONAL

Luís Lobo-Fernandes

VÍTOR JÚLIO DA SILVA E SÁ
E SÉRGIO TENREIRO DE MAGALHÃES

Tecnologias Biométricas por Dinâmica Gestual: Viabilidade, Requisitos e Implementações

Braga,
Editora Univ. Católica Portuguesa – Societas,
Coleção de Estudos Sociais,
2014, 255 páginas

Podemos dizer que o inovador trabalho de Vítor Júlio da Silva e Sá e Sérgio Tenreiro de Magalhães em torno da segurança dos sistemas de informação surge no momento azado, pois desponta no horizonte editorial português numa altura em que a reflexão sobre o ciberterrorismo e a ciberguerra exige maior atenção e aprofundamento no nosso país. A obra incide com especial ênfase no reconhecimento e na autenticação de quem acede aos sistemas de informação, atendendo mais especificamente ao modo como é realizada a interação com o computador. Segundo os autores, esta interação induz um cruzamento de áreas distintas mas não necessariamente divergentes, tais como a computação gráfica, a interação humano-computador (IHC), a fisiologia e a eletrofisiologia humana. Um dos méritos assinaláveis da investigação é justamente transportar o leitor para o centro da complexidade do novo cibermundo. Do mesmo modo que, como há setenta e um anos, a invenção da bomba atómica mudou as formas de fazer a guerra e os mecanismos de dissuasão, deparamo-nos hoje com uma nova corrida para desenvolver ciberarmas e sistemas de proteção contra elas. Uma ciberguerra generalizada não pode ser equiparada a um holocausto nuclear, mas constituiria uma ameaça com impacto global gravíssimo. Hodiernamente, assistimos a um número considerável de ataques diários a sistemas informáticos com origem em estados como a China e a Rússia, mas também dos Estados Unidos, que

desenvolvem, igualmente, ações de sabotagem informática, protagonizando eles próprios réplicas da internet do futuro, como é o caso do Pentágono que tem desenvolvido e testado vários cenários; o objetivo é simular, por exemplo, o que seria necessário para os contendores sabotarem ou encerrarem as centrais elétricas do país, as redes de telecomunicações ou os sistemas de aviação. O esforço visa construir melhores escudos contra esses ataques, aperfeiçoando a resistência das chamadas *firewall* informáticas norte-americanas e criar uma nova geração de armas *online*.

Num relance breve sobre o problema geral da ciberguerra convém relembrar que o ataque às torres gémeas de Nova York em setembro de 2001 abriu um ciclo de maior incerteza no sistema internacional, marcado pela emergência de novos padrões de terrorismo transnacional, onde se insere precisamente o amplo espectro dos ciberconflitos. Estas manifestações de neoterrorismo que aqui elencamos na categoria de conflitos de baixa intensidade, não sendo na essência muito diferentes de outras práticas terroristas do passado, configuram uma sofisticação acrescida, com recurso a expedientes especialmente ousados, como seja a intrusão nos sistemas de informação dos estados. As ações de violência inusitada resultaram em grande medida dos mais avançados aparatos tecnológicos para produzir danos consideráveis e dor. Este é um mundo incerto, mais desterritorializado, e com maiores vulnerabilidades, pelo que continua a ser um sistema fundamentalmente anárquico, ou seja, de paz insegura. Porém, a questão porventura mais pertinente prende-se com a necessidade de avaliar em que medida os eventos de 11 de setembro de 2001 acarretaram mudanças nos padrões convencionais de conflitualidade no sistema internacional, confrontando o domínio teórico das relações internacionais com acrescida incerteza e perda de clareza conceptual, ou até mesmo com o que chegou a ser enunciado como uma «crise de paradigmas». Tal incerteza era adensada ainda por uma insuficiência do modelo teórico centrado exclusivamente no Estado soberano, isto é, pela metamorfose do próprio sistema vestefaliano, resultante do crescimento exponencial de atores não governamentais, e da utilização por parte de outros grupos não estaduais da panóplia de recursos provenientes das novas tecnologias informáticas. O principal desafio metodológico apontava já então para a exigência de integrar o papel dos chamados *mixed actors* (atores transnacionais) na explicação dos fatores de mudança, e de, concomitantemente, garantir ciber-segurança nas novas circunstâncias internacionais. Por outro lado, é fundamental compreender que os ataques de Nova York e, refira-se, igualmente, os atentados de Madrid em 11 de março de 2004, revelaram um arrojo e uma espetacularidade assinaláveis com recurso às tecnologias globais, visando atingir grandes concentrações de pessoas. É certo que de um ponto de vista estrito das leis da guerra, apesar da sua brutalidade, o ataque às torres do World Trade Center pode ser considerado um dano «colateral»,

mas do ponto de vista dos terroristas foi uma ação de sucesso integral, fosse por gerar medo no maior centro financeiro e de negócios do mundo – verdadeiro símbolo da prosperidade ocidental –, fosse pela demonstração de insuficiências significativas em matéria de *intelligence* dentro da organização de segurança dos Estados Unidos.

Os atentados suscitaram diferentes ângulos de análise e debate. Na dimensão mediática do puro terror, Nova York fica sobretudo marcada pela transmissão em direto dos ataques, uma inovação patente. A calendarização para o início da manhã dos atentados com aviões comerciais pirateados, e a programação do ataque à segunda torre cerca de vinte minutos depois do ataque à primeira visou, objetivamente, permitir a difusão ao vivo das ações *kamikazes*, levando o hiperterrorismo a uma escala sem precedentes: a humilhação dos Estados Unidos televisionada em direto. Em contrapartida, em Madrid, o uso dos telemóveis, transformados em autênticos instrumentos letais para desencadear as explosões em comboios suburbanos, definiria o verdadeiro espírito do tempo: a reconceptualização do terror pelo lado da cibernética. Em rigor, como observou com notável acuidade e inteligência Miguel Gaspar, aquilo que ocorreu em Madrid foi um «confronto entre uma velha tecnologia – a televisão –, e uma nova tecnologia – os telemóveis com ligação à internet – usados para desencadear as explosões»[1]. A violência projetada contra civis indefesos na capital espanhola – tal como ocorrera em Nova York a 11 de setembro de 2001 – foi de excecional gravidade, evidenciando que as ameaças protagonizadas por um leque alargado de atores com *expertise* informática, representam o reverso «negro» do cibermundo. O terror, que é fundamentalmente concebido para ser mediático, encontraria, assim, nas novas potencialidades informáticas um terreno ideal e fértil, na exata medida em que é planeado de modo a obrigar os próprios *media* a referi-lo e a amplificá-lo exaustivamente.

É justamente neste esforço crítico de dilucidação das novas ameaças associadas ao ciberterrorismo e à (in)segurança dos sistemas de informação que este oportuno livro dos professores Vítor Sá e Tenreiro de Magalhães, sugestivamente intitulado *Tecnologias Biométricas por Dinâmica Gestual – Viabilidade, Requisitos e Implementações*, se apresenta ao leitor. A obra tem o mérito suplementar de apontar para uma das dimensões insuficientemente analisadas nos atentados de 11 de setembro de 2001 em Nova York, e de 11 de março de 2004 em Madrid, ou seja, o seu enquadramento numa escala de conflitos algo mais ambiciosa. Como estipulara Carl von Clausewitz, o mais decisivo ato de julgamento que o estadista e o general exercem é compreender a guerra em que se empenham, e não tomá-la por algo, ou desejar torná-la em algo que, pela sua natureza, não é. Este é, pois, segundo Clausewitz, o primeiro, o mais compreensivo de todos os problemas estratégicos. Os conflitos de baixa intensidade que incluem tipologicamente um amplo espetro de categorias que vão do terrorismo e insurgência até às ações

antiterroristas, de contrainsurgência, operações especiais, e, mais recentemente, terrorismo informático e cibernético, estão normalmente associados a uma deslocação do foco vertical das batalhas clássicas entre países – travadas fundamentalmente pelos respetivos braços militares – para um plano horizontal envolvendo mais diretamente a procura de efeitos profundamente desestabilizadores nos planos civil, psicológico, social, económico e ideológico. Conceptualmente, estamos perante uma tipologia de hostilidades localizada num dos extremos da escala, ou seja, de formas que temos denominado de *violência sem combate* e de *guerra não declarada*, constituindo os ataques informáticos uma das suas expressões contemporâneas mais pungentes. Estas modalidades de violência informal têm um caráter acentuadamente errático, difuso e transnacional. A dimensão talvez politicamente mais substantiva dos conflitos de baixa intensidade como o ciberterrorismo e a ciber-segurança, envolve uma lógica assente no desgaste sociopsicológico das populações e dos sistemas políticos nacionais, enfim, na disrupção social, cujo objeto é a destabilização dos sistemas de poderes prevalecentes.

É imperioso, pois, considerar o ponto de viragem que marcam os atentados do 11 de setembro e do 11 de março, que tornaram especialmente viva a natureza das novas ameaças transnacionais. Temos sustentado que o impacte psicológico daqueles eventos não pode, nem deve, ser minimizado. Tal circunstância implicou, por exemplo, que os Estados Unidos deixassem de basear o seu pensamento estratégico numa lógica reativa, dada a impossibilidade manifesta de dissuadir ataques irracionais, tal como as ainda fortes limitações em travar os cada vez mais frequentes ataques de cariz informático. Na leitura da Administração norte-americana, o «esgotamento» da dissuasão – fundada, como se sabe, no argumento da retaliação – em relação a grupos que atuam irracionalmente e de forma imprevisível, com recurso frequente a práticas suicidas, tornou necessária, na ótica de Washington, uma alteração qualitativa da doutrina estratégica «forçando» a adoção de medidas proativas de defesa. Como sempre acontece quando a dissuasão falha, a alternativa é a defesa *ativa*. Ora, a internet tornou-se, já, um dos palcos centrais das rebeliões contra os estados, e das consequentes tentativas apertadas de controlo por parte das autoridades estaduais. A ciberguerra envolve, pois, limites à informação e aos expedientes para contornar este tipo de ataques. Como escrevia o diário *The New York Times* em 2009, um ataque informático a um grande banco pode ter um impacto maior na economia do que o 11 de Setembro, e uma ameaça informática aos sistemas e redes de transações monetárias seria o equivalente atual de um ataque armado em grande escala. Mas, um dos problemas aparentes é que as leis e as regras dos conflitos armados convencionais não são «respeitados» no cibermundo.

Afigura-se-nos, assim, imprescindível que o especialista atento do fenómeno internacional nas suas múltiplas vertentes conheça quais são, na ótica da informática,

os desafios que colocam estes novos atores não estaduais bem como os novos padrões de conflito transnacional, cada vez mais desterritorializado. Este livro é o epítome de como o cruzamento de áreas científicas tão distintas é crucial para interpretar o cibermundo do presente. A discussão *técnica* das tecnologias biométricas pode ajudar o estudioso dos conflitos internacionais a melhor dilucidar as ameaças e os perigos da cibernética letal para a segurança internacional num quadro de interdependências complexas, possibilitando aos estados melhor desenhar as suas próprias estratégias de controlo e combate desta tipologia de ameaças. Por seu turno, a inteleção politológica do ciberconflito e do ciberterrorismo permite ao *informático* o quadro de interpretação política e de mudança do sistema internacional em que o uso e o «abuso» dos novos recursos tecnológicos toma lugar. Pode, em suma, o leitor atento encontrar nesta obra um dos contributos analíticos mais interessantes sobre algumas das dimensões emergentes no cibermundo. R:I

NOTAS

1 Cf. GASPAR, Miguel – «Telemóveis contra televisão nos atentados de Madrid». In *Público*, 23 de julho de 2004, p. 45.