Paulo Portas: “na NATO teremos de investir num quarto ramo das forças: o ramo digital”

itsecurity.pt/news/analysis/paulo-portas-na-nato-teremos-de-investir-num-quarto-ramo-das-forcas-o-ramo-digital

A crescente centralidade do **ciberespaço** e a ameaça de ataques digitais sofisticados marcaram o debate no evento que assinalou os **vinte anos** da **VisionWare**, no SUD Lisboa, onde **Paulo Portas**, Ex-Ministro dos Negócios Estrangeiros, Ex-Vice-Primeiro-Ministro e Ex-Ministro da Defesa, defendeu que a **União Europeia** deve investir em capacidades digitais capazes de proteger democracias, economias e sociedades abertas.

Com um keynote sobre "Ameaças Híbridas, ciberespaço e o papel da Europa na nova era da ciberdefesa", Paulo Portas arrancou o evento numa data que permanece como símbolo mundial de um ponto de viragem na forma como conhecemos o mundo: o 11 de setembro.

A era digital, de acordo com o antigo governante, trouxe riscos e oportunidades inéditas, com impacto particular nas democracias. *"Os sistemas digitais são consequência direta da digitalização da sociedade, um dos maiores avanços tecnológicos do mundo moderno"*, afirmou, acrescentando que esses riscos *"são muito mais perigosos nas sociedades abertas do que nas autocráticas"*. A velocidade da inovação *"é sempre superior à velocidade da regulação"*, diz, o que deixa a Europa numa posição delicada porque *"tem tendência para regular demais e terá de arrepelar caminho para a frente. Não é possível parar a digitalização"*.

O Ex-Ministro da Defesa alertou para a centralidade crescente do ciberespaço nas ameaças globais, ao apontar que *"na guerra clássica sei quem é o inimigo, na guerra ciber demoro meses a saber quem é"* e que muitas vezes o objetivo vai além do fator económico para *"provocar o caos e ganhar atenção mediática"*. Para o ex-ministro, a ciberdefesa deve ser assumida como pilar estratégico das democracias, ao ponto de defender que *"na NATO teremos de investir num quarto ramo das forças: um ramo digital"*, já que ataques ciber *"podem destruir a nossa vida num segundo – algo que nem mesmo uma bomba nuclear conseguiu"*.

Ameaças híbridas e desinformação no centro do debate

Numa entrevista durante o evento, António Gameiro Marques, Ex-Diretor Geral do Gabinete Nacional de Cibersegurança (GNS) e do Centro Nacional de Cibersegurança (CNCS), sublinhou que a Europa *"não está a dormir"* e que mecanismos como o EU-Cyclone têm sido ativados em resposta a grandes incidentes. Ainda assim, considerou fundamental reforçar a cooperação entre defesa, inteligência e setor privado, bem como investir de forma muito mais robusta em inteligência artificial e cibersegurança. *"Não podemos ficar satisfeitos com mil milhão de euros por ano, devíamos multiplicar esse valor por 20 se queremos proteger a democracia, a liberdade e a economia"*, afirmou. Para o responsável, a soberania digital tem também uma dimensão ética, sendo que *"a tecnologia não pode ser cúmplice da erosão democrática. Tem de servir a verdade, a participação e uma sociedade mais justa, informada e livre"*.

Paralelamente, Dan Cimpea, Diretor Geral do Gabinete Nacional de Cibersegurança da Roménia, lembrou que a desinformação é também um problema de cibersegurança, já que *"compromete a integridade e a disponibilidade da informação"* e pode *"mudar o destino de um país numa eleição"*. Recordou o caso das presidenciais romenas, em 2024, em que identificaram 80 mil máquinas em operações coordenadas e manipulação massiva de redes sociais – sobretudo via TikTok – ao ponto de *"um candidato ter mais visualizações do que a Taylor Swift ou a Rihanna em apenas seis dias"*, situação que levou mesmo o Tribunal Constitucional a anular o ato eleitoral pela primeira vez.

A aposta na inteligência e inovação

Em 2005, num mundo certamente menos digital, a empresa portuguesa VisionWare dava os primeiros passos; hoje, credenciada pela NATO, acompanha de perto um cenário em que as ameaças híbridas e a desinformação deixaram de ser fenómenos emergentes para se tornarem realidades consolidadas. *"Não temos um ciberataque sem ter de perceber qual é a morfologia do ataque, quem é o grupo, qual é o consórcio empresarial que está por trás do grupo criminoso, como é que ele funciona, qual é o deepfake"*, afirmou Bruno Castro. Para responder a essa complexidade, a VisionWare criou uma unidade de intelligence que *"se dedica exclusivamente a perceber o que é real, o que é falso"*. Uma frente de combate que, sublinhou, é já *"crítica para nós"*.

Ao olhar para o futuro, garante que aquela ousadia inicial permanece inalterada no espírito da equipa: *"estamos constantemente a procurar coisas novas, inovadoras e a procurar o que é que está a acontecer no ciberespaço"*. Essa inquietação, que rejeita *"zonas de conforto"* e se traduz numa *"área de inovação ultra-agressiva"*, continua a ser, segundo o responsável, a força que guia a empresa na resposta aos desafios cada vez mais complexos do ciberespaço.