**NÓMADAS DIGITAIS**
VIAJAR ENQUANTO SE TRABALHA

**PRÓTESES IMPRESSAS EM 3D**
PROJETO NACIONAL PARA MELHORAR A VIDA DE AMPUTADOS

# EXAME INFORMÁTICA

**SUPERTABLETS**
TESTE AOS MODELOS QUE PODEM SUBSTITUIR PCs

ABRIL 2022 • Nº 322 • MENSAL • ANO 28 • €4 • PORTUGAL CONTINENTE

# CIBER GUERRA

## ESTARÁ PORTUGAL PREPARADO PARA UM CONFLITO DIGITAL DE LARGA ESCALA?

**SAMSUNG S22, OPPO FIND X5 E XIAOMI 12**
QUAL O MELHOR ANDROID DO MERCADO?

**AUTEL NANO+**
O DRONE QUE VENCE A DJI

**COMO ESCOLHER UMA E-BIKE**
FUJA DOS PREÇOS DOS COMBUSTÍVEIS

**DVD**
CONVERSÃO DE VÍDEOS
PEGA O SEU NA BANCA!
€3,90

**VOLT**
ENSAIOS
RENAULT MÉGANE E-TECH + AIWAYS U5

**VIDA NOVA A PORTÁTIL VELHO**
COMO INSTALAR O CHROME OS

Especialistas ouvidos pela *Exame Informática* consideram que Portugal não está pronto para um conflito digital. Há falta de preparação, do Estado às empresas privadas – e a existência de máquinas ligadas à internet ainda com a mesma vulnerabilidade que permitiu o WannaCry é apenas um exemplo deste receio. Portugal precisa de munir-se, alertam, para um ataque de grande escala – e há inclusive quem defenda que o País deve criar as suas próprias armas cibernéticas

**Texto:** Rui da Rocha Ferreira **Fotos:** D.R.

# O FANTASMA DA CIBERGUERRA

"A partir do momento em que estamos tão dependentes do digital, qual é o pior cenário que pode acontecer? Tudo o que está ligado ao digital desligar-se de repente. E o que é que fica? Uma sociedade em polvorosa, porque basicamente nada vai funcionar". André Barrinha, professor de Relações Internacionais na Universidade de Bath, no Reino Unido, lembra que este cenário catastrófico no qual tudo o que é digital vai abaixo por causa de um ataque informático cirúrgico "faz parte do nosso imaginário e dos nossos medos". Ou como os americanos lhe chamam, um Cyber Pearl Harbor, numa referência ao devastador ataque aéreo japonês à base naval americana, em 1941. Mas o investigador que estuda o impacto da cibersegurança nas relações internacionais reconhece que este é um perigo real, pois "à medida que aumentamos o nível de digitalização das nossas sociedades, acabamos por ficar cada vez mais vulneráveis àquilo que acontece no ciberespaço".

Basta recuar algumas semanas no tempo para perceber o verdadeiro impacto de um 'míssil digital'. O ataque informático à Vodafone Portugal deixou centenas de milhares de pessoas e dezenas de organizações com comunicações limitadas – não era possível fazer chamadas, enviar mensagens ou aceder à internet móvel. Hospitais e outras organizações críticas ficaram com alguns serviços parados. A ideia de um ataque contra um serviço essencial para o funcionamento do País deixou de ser mito e tornou-se bem real. E este é o grande receio num cenário de ciberguerra – que o ataque digital tenha efeitos nefastos no mundo físico. Bruno Castro, diretor executivo da Visionware, empresa especializada em análise forense de ataques informáticos, diz que no mundo digital "acontece cada vez mais uma analogia muito semelhante ao da guerra bélica – são ataques direcionados a infraestruturas críticas, na ótica de fazer disrupção de serviço – a ideia é quase bombardear um serviço digital para desestabilizar um país", explica.

Não é – e poderá nunca vir a ser – possível classificar o ataque informático à

"O QUE DISTINGUE UM ATAQUE INFORMÁTICO LEVADO A CABO POR CRIMINOSOS DE UM ATAQUE COM FINS ESTRATÉGICOS É A MOTIVAÇÃO E A QUESTÃO DOS RECURSOS"

**ANDRÉ BARRINHA**
PROFESSOR DE RELAÇÕES INTERNACIONAIS NA UNIVERSIDADE DE BATH



Vodafone como um ato de ciberguerra, apesar da semelhança das consequências. Para isso seria necessário perceber quem esteve por trás, a motivação do ataque e a tipologia dos recursos que foram usados. "Se descobrirmos que esse ataque foi levado a cabo por um ator estatal, diria que sim, pode ser visto como tal", analisa André Barrinha.

O ataque à Vodafone, o ataque ao Ministério dos Negócios Estrangeiros, o ataque ao site do Parlamento e a descoberta de atividades de espionagem, em Portugal, por parte de um dos mais persistentes e meticulosos grupos de hackers associados à China, conhecido como APT15, são exemplos recentes de que o País está vulnerável. "Estes ataques todos podem ser um aviso para o que poderá acontecer mais tarde", alerta Rui Silva, professor no Instituto Politécnico de Beja (IP Beja).

### PREPARADOS OU NÃO, AÍ VÊM ELES

"Na cibersegurança em Portugal, embora tenha começado a desenvolver-se nos últimos dois, três anos, ainda não existe um investimento muito sério na temática, seja a nível militar, seja a nível das instituições privadas. Neste momento, sozinhos, não temos essa capacidade", comenta Sérgio Silva, diretor executivo da CyberS3c, academia de formação especializada em segurança informática, sobre um eventual cenário de ciberguerra. "Na minha opinião, [Portugal] não está preparado", resume. Bruno Castro também considera que "Portugal não está preparado" e exemplifica: "Já tivemos ataques a serviços muito sensíveis, em Portugal e fora de Portugal, em que a teoria, em termos de investigação forense, foi claramente que tenha sido um ataque de outras nações", avança o executivo, mas sem revelar, por sigilo profissional, as entidades afetadas. Mas revela os motivos por trás dos ataques: "São de espionagem ou na ótica de disrupção".

Rui Silva é coordenador do mestrado de Segurança Informática do IP Beja e fundador do laboratório de segurança digital e cibercrime Ubinet. "Tivemos o primeiro laboratório de hacking do país", salienta. Este laboratório tem colaborado com forças de segurança, como a Polícia Judiciária, e com grandes tecnológicas, como a Fujitsu, em investigações e programas de aumento de defesa de entidades através de auditorias nas quais colocam à prova a segurança de sistemas informáticos. "Da nossa experiência, já existe uma consciência superior para os perigos [do digital], mas em algumas situações de testes de penetração que temos feito a organizações, até do Estado, quando apresentamos o resultado da nossa auditoria de segurança ofensiva e dizemos que o sistema está permeável à execução de código remoto e permite aceder ao sistema todo, os decisores ainda dizem 'O que é que isso quer dizer?'", revela o professor. "Se estamos preparados para um ciberataque... não sei se a nível de organizações teremos um nível de preparação necessário", conclui.

É importante sublinhar que existem diferentes tipologias de organizações: as que estão diretamente ligadas ao Estado, seja um ministério ou um serviço público como a linha SNS 24; existem empresas privadas que gerem infraestruturas consideradas como críticas, como são as áreas da banca, energia, telecomunicações e transportes; existem empresas privadas que, não gerindo infraestruturas críticas, têm propriedade intelectual importante para o desenvolvimento e funcionamento da sociedade; existem empresas privadas de menor impacto direto no funcionamento do país, como uma pequena ou média empresa no setor fabril ou da restauração; e existem ainda os utilizadores finais. A maturidade de segurança, até por exigência legal, de umas (sobretudo as de infraestruturas críticas) é diferente de outras – mas por vezes é um ataque a um pequeno fornecedor que abre as portas de acesso a uma grande empresa.

Miguel Romão, líder do centro de operações de segurança da empresa S21Sec, prefere contextualizar a situação portuguesa naquela que é uma realidade mais global. "Portugal, caso sofra um ataque por trás de um objetivo de ciberguerra, não estará preparado tal como outras nações não vão estar. Não existem infraestruturas 100% seguras. Se Portugal está num grau de maturidade de acordo com o expectável e o necessário para dar uma resposta, diminuindo o tempo de recuperação ante um incidente? Poderíamos estar muito mais avançados, sem dúvida", defende. E dá um exemplo. "Umas horas após o início da guerra entre a Rússia e a Ucrânia, o governo espanhol lançou uma guia de boas práticas [de cibersegurança] a todos utilizadores da função pública. Foi uma atividade simples, que chegou a todos os membros, foi noticiada pelos meios de comunicação e até a rede CSIRT [de Portugal] usou esse exemplo para partilhar conhecimento na rede. Poderíamos ter feito isso, poderíamos ter chegado a esse ponto".

## COMO FUNCIONA UM SoC

A S21Sec tem três centros de operações de segurança informática (SoC no acrónimo em inglês): um em Lisboa, outro na Maia e o maior está em Madrid, Espanha. Nestes três SoC trabalham 120 pessoas divididas por turnos para garantir que há 'olhos' 24 horas por dia, sete dias por semana. O tamanho pode diferir, mas a estrutura é a mesma. Tudo começa numa parede de ecrãs gigantes com informações em tempo real. Depois, numa primeira fila, sentam-se os operadores, que fazem uma triagem dos alertas que as diferentes tecnologias de monitorização do SoC geram. Atrás, numa segunda fila, está a equipa de analistas, que vai aprofundar o conhecimento sobre aquele alerta. Mais atrás, em mesas isoladas, estão os coordenadores do centro de operações, ladeados pelo gabinete de crise, uma espécie de aquário no qual a equipa reúne em caso de um incidente grave – e no qual os vidros passam de transparentes a foscos se necessário. Há depois uma terceira fila de operacionais, os engenheiros, que definem a modulação dos ataques que o SoC deve detetar. "O que fazemos é coletar informação da infraestrutura dos nossos clientes, selecionando a informação mais valiosa para poder prestar esta monitorização. E aplicamos conhecimento que se baseia em duas fontes importantes: alarmística e casos de uso que detetam situações suspeitas", explica Miguel Romão, líder do SoC da tecnológica espanhola.

"A PARTE DEFENSIVA É A MAIS MADURA NO MERCADO. PORTUGAL NÃO FOGE A ESSA TENDÊNCIA, SEM NO ENTANTO EU ACHAR QUE ESTÁ VULNERÁVEL E CONTINUA VULNERÁVEL A ATAQUES DE GRANDE DIMENSÃO"

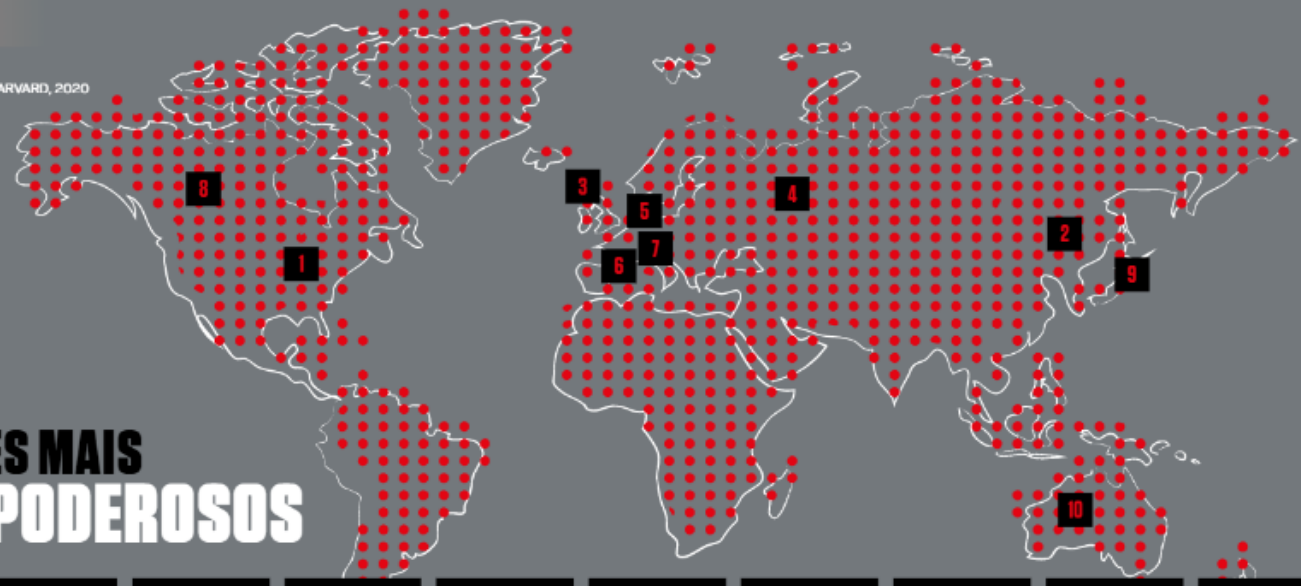
**BRUNO CASTRO**
DIRETOR EXECUTIVO DA VISIONWARE

Para evitar males maiores, "devia ser feito um varrimento nacional para encontrar quais as empresas e os sistemas que estão vulneráveis e tentar corrigir o mais rapidamente possível essas falhas", defende, por seu lado, Sérgio Silva. "Em Portugal ainda vemos empresas com máquinas ligadas à internet com a mesma vulnerabilidade que permitiu o WannaCry [malware de 2017]. Isto é uma porta aberta a um ataque", avisa.

### QUANDO OS MÍSSEIS SÃO FEITOS DE BITS

André Barrinha defende que a própria definição de ciberguerra, como um conflito paralelo que é travado no mundo digital, pode não fazer muito sentido do ponto de vista conceptual. "Nunca vamos ter um contexto em que vamos ter simplesmente ações limitadas ao que se passa no ciberespaço", justifica. "O que faz sentido é a utilização do ciberespaço para alcançar fins estratégicos". E isso é o que vários países têm feito há já muitos anos. O caso mais marcante de uma ofensiva de guerra cibernética foi o Stuxnet (software malicioso, deteta-

FONTE: BELFER CENTER, HARVARD, 2020




# OS PAÍSES MAIS CIBERPODEROSOS

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| EUA | CHINA | REINO UNIDO | RÚSSIA | PAÍSES BAIXOS | FRANÇA | ALEMANHA | CANADÁ | JAPÃO | AUSTRÁLIA |

do em 2010, com apenas 500 kilobytes de tamanho, que inutilizou dezenas de centrifugadoras nucleares do Irão), cuja criação tem sido atribuída a americanos e israelitas. Mais recentemente, a invasão da Rússia à Ucrânia tem deixado um rasto de agressões digitais de parte a parte – dos russos mais até antes da invasão física, quase como uma forma de abrir caminho para a guerra cinética, e dos ucranianos como uma resposta à invasão, por forma a deitar abaixo serviços russos que servem de apoio aos militares no terreno.

"Este panorama de ciberguerra existe e tem vindo a agudizar nos últimos anos, é uma realidade no mundo digital", comenta Bruno Castro. "É mais barata, é menos violenta humanamente, é menos violenta mediaticamente, é mais segura para o opressor e as baixas são muito inferiores" diz o CEO da Visionware sobre as vantagens de um ciberconflito. "A outra vantagem é que até poderá fazer um ataque não oficial a um país. Num bombardeamento, são os meus aviões e os meus mísseis, é quase um ato oficial, uma ciberguerra pode não comprometer as nações. No fim do dia é sempre anónima, a não ser que se queira afirmar", diz Bruno Castro. E a questão da atribuição é sempre uma das mais difíceis na investigação de um ciberataque. "A ofuscação é tão fácil que permitirá a cada um apontar o dedo para outro lado", complementa Miguel Romão.

Também há desvantagens na guerra cibernética: os ataques precisam de muito investimento e tempo de desenvolvimento, e assim que essa arma é usada uma vez, os sistemas podem ser corrigidos e deixa de ser eficaz. Mas isto levanta uma outra questão: da mesma forma que Portugal tem submarinos, caças de combate F-16 e outro armamento militar, deveria ter também as suas próprias armas cibernéticas?

## CONTRA OS HACKERS, MARCHAR, MARCHAR

Portugal tem uma unidade militar dedicada ao espaço cibernético, o Centro de Ciberdefesa, incorporado no Estado-Maior-General das Forças Armadas, constituído por militares da Marinha, Exército e Força Aérea e que, na prática, funciona como o braço das Forças Armadas no mundo digital. Existe também o Centro Nacional de Cibersegurança, a autoridade nacional em matéria de cibersegurança, e do qual faz parte o CSIRT, centro de resposta a incidentes cibernéticos. A *Exame Informática* fez pedidos de entrevista ao Centro de Ciberdefesa, ao Centro Nacional de Cibersegurança e ao Centro Nacional de Segurança – dos quais não obteve resposta. A *Exame Informática* contactou ainda várias empresas de infraestruturas críticas – Meo e Nos (telecomunicações), SIBS (pagamentos) e REN (energia) – que não estiveram disponíveis para entrevistas sobre o seu papel numa eventual ciberguerra.

"HÁ TRÊS DOMÍNIOS QUE SE COMPLEMENTAM EM TERMOS DE RISCO: VULNERABILIDADES, CONFIGURAÇÕES FRACAS E A CONSCIÊNCIA DOS UTILIZADORES"

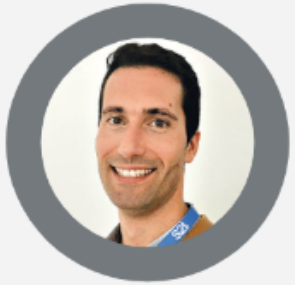
**RUI SILVA**
COORDENADOR DO MESTRADO DE ENGENHARIA DE SEGURANÇA INFORMÁTICA DO IP BEJA E DO LABORATÓRIO UBINET

Mas a *Exame Informática* ouviu um profissional que trabalha em ciberdefesa e que pediu para não ser identificado. "Temos de associar mais a parte de ciberdefesa como uma parte integrante da garantia da estabilidade e da democracia em Portugal", sublinha. "O ciberdomínio, sendo transversal a todos os outros [domínios militares], é um domínio no qual é necessário investir. Embora seja necessário haver coordenação entre os vários domínios, não deixa de ser uma capacidade que é necessária. Vemos vários países a investir nisso. Portugal não deve ficar para trás nesse investimento", alerta.

A opinião dos diferentes especialistas ouvidos é unânime: o País tem entidades, legislação e acima de tudo profissionais capazes do lado defensivo. Mas isso pode não ser suficiente em tempos de verdadeira crise. "Tem de ter a capacidade não só de defender, mas ter em consideração o aumento do conflito, também tem que ter capacidades ofensivas", referiu o profissional de ciberdefesa ouvido pela *Exame Informática*.

"Só se consegue ter consciência de defender se souber como se ataca", argumenta igualmente Rui Silva. "Estaremos tanto mais preparados quanto mais pessoas houver nestas atividades. Temos que ensinar quais as vulnerabilidades que são usadas pelos atacantes – e que têm uma criatividade brutal –, é importantíssimo estimularmos esta criatividade de ataque, para que ganhemos maior capacidade de defesa".

O professor no IP Beja lembra que "ao nível dos estados, as atividades ofensivas podem ser necessárias e temos que nos preparar para isso", indo mesmo mais longe, dizendo que "sem dúvida nenhuma" Portugal deveria desenvolver as suas próprias ciberarmas. A acontecer algo do género, considera Bruno Castro, "a construção de armas tem que ser patrocinada pelo Estado – e altamente confidencial".



"PRESENCIAMOS ATAQUES A ORGANIZAÇÕES EM PORTUGAL MUITO FORA DA CAIXA. O ÚNICO OBJETIVO ERA ENTRAR PARA NEGAR O ACESSO À INFORMAÇÃO DA PRÓPRIA ORGANIZAÇÃO. O INTUITO ERA A DESTRUIÇÃO"

**MIGUEL ROMÃO**
GESTOR DE SOC NA S21SEC

André Barrinha defende por seu lado que "não é por um país sofrer um ciberataque que tem de responder com um ciberataque" e que ter capacidades ofensivas "mostra mais o nível de desenvolvimento do país nesse domínio do que propriamente aquilo que quererá vir a fazer". "Não sei se Portugal começar a envolver-se em ataques cibernéticos como resposta a ações por parte de outros estados é o melhor caminho". O perito em relações internacionais defende, acima de tudo, que o País deve investir em "defesas robustas" e ter uma "doutrina clara" sobre o que fazer em caso de um conflito digital. Pois como o próprio resume, a questão da segurança informática deveria neste momento ser quase um desígnio nacional: "O objetivo do País é ser uma sociedade mais digitalizada e uma economia digital – e precisa de ter as condições de segurança para que isso aconteça". ■