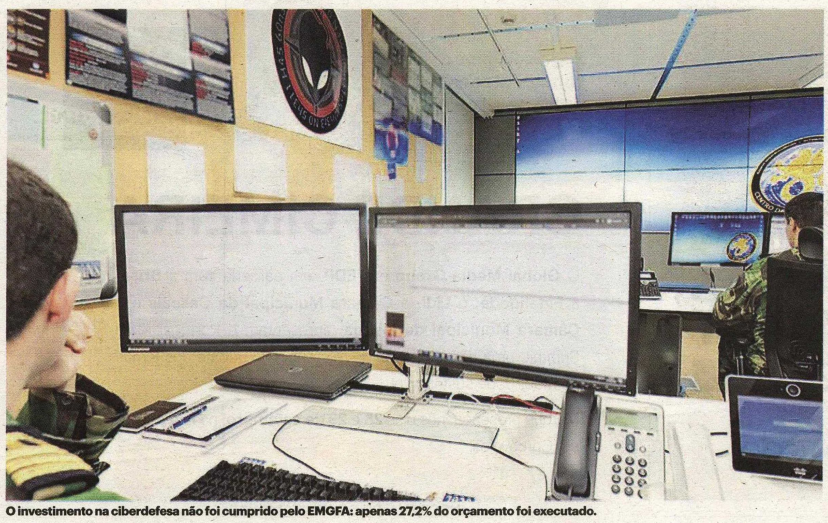
manchete

Diário Notícias

09-09-2022

Periodicidade: Semanal
Classe: Informação Geral
Âmbito: Nacional
Pagina(s): 8



O investimento na ciberdefesa não foi cumprido pelo EMGFA: apenas 27,2% do orçamento foi executado.

Ciberataque na Defesa: "Esperamos que este caso não seja um Tancos 2"

SEGURANÇA Pelo menos quatro crimes graves podem estar em causa no ciberataque contra a Defesa Nacional que expôs documentos secretos da NATO, mas os militares não chamaram a PJ.

TEXTO **VALENTINA MARCELINO**

"Espero que não estejamos perante um Tancos 2, porque se pode repetir o esconder de responsabilidades que sucedeu nesse processo. Aqui o caso tem gravidade acrescida por implicar a segurança de Portugal e da Aliança Atlântica, num difícil contexto da guerra da Ucrânia. Estão claramente em causa, pelo menos, crimes informáticos e crimes contra o Estado, que de acordo com a Lei de Organização da Investigação Criminal são da competência de investigação da PJ e é incompreensível que não tenha sido chamada. Aguardamos que as autoridades judiciárias nos esclareçam sobre este assunto e temos direito a esse esclarecimento porque o alarme é óbvio", declara o constitucionalista Jorge Bacelar Gouveia, presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT).

Espionagem, violação do segredo de Estado, acesso ilegítimo a sistema informático (Lei do Cibercrime) e acesso indevido (Lei da Proteção de Dados Pessoais) são os crimes que podem ter sido cometidos no ciberataque que atingiu o Estado-Maior-General das Forças Armadas (EMGFA) e o Ministério da Defesa Nacional (MDN). Um ciberataque "prolongado e indetetável", que, conforme o DN noticiou, terá resultado na exfiltração de "centenas" de documentos classificados NATO, secretos e confidenciais e a exposição de parte deles para venda na *darkweb*. O governo terá sido avisado pelos serviços de informações dos EUA.

Tudo crimes da competência de investigação da Polícia Judiciária (PJ) que, no entanto, não foi informada da situação, apesar de o caso ser há várias semanas do conhecimento de várias entidades. Pelo menos do próprio primeiro-ministro, António Costa (que terá sido o primeiro a ser informado, pela embaixada norte-americana em Lisboa), da ministra da Defesa, Helena Carreiras, do secretário de Estado para a Digitalização, Mário Campolargo, do Chefe de Estado-Maior-General das Forças Armadas, almirante Silva Ribeiro, do diretor-geral do Gabinete Coordenador de Segurança (GNS), vice-almirante Gameiro Marques, do diretor-geral do Serviço de Informações Estratégicas de Defesa (SIED), Carlos Lopes Pires, e do diretor-geral do Serviço de Informações de Segurança (SIS), Neiva da Cruz, que reuniram mais do que uma vez nas últimas semanas para acompanhar o caso. "No limite, todas as pessoas que tiveram conhecimento do ciberataque e não o comunicaram às entidades competentes, DCIAP e PJ, podem também incorrer em crime de denegação de justiça e prevaricação", sublinha ao DN fonte judicial.

> No limite, todas as pessoas que tiveram conhecimento do ciberataque e não o comunicaram às entidades competentes, DCIAP e PJ, podem também incorrer em crime de denegação de justiça e prevaricação.

Esta fonte adianta que, "além do crime de espionagem, por se poder tratar de um ataque com origem em forças estrangeiras, o facto de poder ter sido facilitado por alegada quebra de procedimentos de segurança para a transmissão destes documentos, pode configurar sucessivas violações do segredo de Estado. É preciso investigar o que aconteceu e quem autorizou que os procedimentos definidos não fossem cumpridos".

O DN questionou a PJ e a Procuradoria-Geral da República sobre se tinha sido ou iria ser instaurado algum inquérito-crime, mas não obteve resposta até ao fecho desta edição.

70% das verbas por gastar

A agravar a situação, o investimento na estrutura de Ciberdefesa no EMGFA – que deve prevenir e anular este género de ataques na Defesa – tem sofrido reveses numa altura em que os ciberataques foram declarados como a maior ameaça à segurança em Portugal, tal como a todos os países que se opuseram à invasão da Ucrânia pela Federação Russa. De acordo com o relatório de execução da Lei de Programação Militar (LPM), em 2021 apenas 27,2% do orçamento previsto para a Ciberdefesa foi executado (1,3 de 4,8 milhões de euros).

"No ano de 2021 a concretização dos objetivos ficou aquém do planeado em termos de indicadores e respetivas metas a atingir. O desenvolvimento da capacidade de Ciberdefesa em termos de recursos humanos teve em 2021 uma evolução pouco significativa em função das restrições impostas no âmbito da pandemia, bem como à escassez de recursos especializados existentes nas FFAA, refletindo-se nos 45% de lotação preenchida no Centro de Ciberdefesa (CCD)", reconhece o MDN. "Fatores exógenos à capacidade de gestão do EMGFA", que teve uma execução orçamental de apenas 29%, "fundos disponíveis atribuídos ao EMGFA" que "não permitiram a assunção de compromissos de cerca de 65% (5,4 milhões) das dotações inicialmente disponíveis" constituíram, assim, "um forte constrangimento à execução financeira da LPM, obrigando, entre outras medidas, à decisão de suspensão de aquisições programadas nos projetos das capacidades de Comando e Controlo (afetando os projetos da Rede Fixa de Comunicações Militares) e da Ciberdefesa".

Numa reportagem feita pelo DN no Centro de Ciberdefesa, em 2019, Gouveia e Melo, ex-coordenador da *task force* da vacinação e atual chefe do Estado-Maior da Armada, era então adjunto de Planeamento e Coordenação EMGFA, responsável pela estratégia de ciberdefesa e por este Centro. A ambição era que fosse criado um ciberexército com cerca de 100 militares, mas ainda só tem pouco mais de meia centena.

Nessa altura, a Defesa tinha acabado de sofrer outro ciberataque que atingiu o sistema de correio eletrónico de militares e civis no Ministério da Defesa Nacional.

valentina.marcelino@dn.pt