BOLETIM OSINT	Edição nº 0215
INTELIGÊNCIA ABERTA NO RÁDIO	16 de novembro de 2026

FORÇAS ARMADAS ALEMÃS SÃO PROIBIDAS DE USAR QUALQUER MODELO DE DRONE CHINÊS

Na Alemanha, as Forças Armadas não utilizarão mais nenhum modelo chinês de drone por razões de segurança, anunciou hoje o Ministério da Defesa. O site do semanário alemão *Der Spiegel* já havia anunciado ontem essa proibição dos drones chineses, por receio de que eles possam transmitir dados sobre exercícios militares, locais de treinamento ou sistemas de armamento aos serviços de inteligência chineses. A Rússia é considerada a principal ameaça por Berlim, mas a China também é uma rival frequentemente suspeita de realizar operações de espionagem. A Alemanha iniciou um amplo processo de rearmamento para fortalecer suas defesas após décadas de investimentos insuficientes, a fim de poder responder aos riscos atuais.

(Deutsche Welle, 11-11-2026)

EM TAIWAN, MAIS DE 10 EMPRESAS TERIAM SIDO VÍTIMAS DE ATAQUES CIBERNÉTICOS VIA INTELIGÊNCIA ARTIFICIAL

Taiwan sofreu ataques cibernéticos e roubos de dados, e há informações que sugerem até mesmo que dados pessoais de funcionários da gigante taiwanesa de semicondutores TSMC teriam sido colocados à venda *on-line*. Chou Chih-hou, vice-diretor da Administração de Cibersegurança, subordinada ao Ministério de Assuntos Digitais, declarou que mais de 10 empresas haviam sido vítimas de ataques cibernéticos facilitados por IA, provocando o vazamento de cerca de oito milhões de dados pessoais. Os ataques tiveram como alvos plataformas de comércio eletrônico, agências de viagens, instituições financeiras como o banco Sinopac, além de órgãos governamentais como o Departamento de Assuntos Consulares do Ministério das Relações Exteriores. A TSMC confirmou que informações sobre funcionários e ex-funcionários haviam sido publicadas em sites sem autorização. O grupo declarou, porém, que, até o momento, nada comprovava que os sistemas da TSMC haviam sido invadidos e que estavam sendo feitos todos os esforços para esclarecer a situação e tomar as medidas necessárias. Chou ressaltou que o uso da inteligência artificial para facilitar ataques cibernéticos se tornou uma prática comum em escala internacional, e não apenas em Taiwan, na Coreia do Sul ou no Japão. O Ministério de Assuntos Digitais pediu às empresas que corrigissem suas vulnerabilidades o mais rápido possível e informassem os usuários, ao mesmo tempo que limitassem a coleta de dados.

(Rádio Taiwan Internacional, 12-11-2026)

ATIVIDADES DOS SERVIÇOS DE INTELIGÊNCIA

NVIDIA CONDUZ INVESTIGAÇÃO APÓS SUSPEITAS DE VAZAMENTO DE INFORMAÇÕES SENSÍVEIS PARA A CHINA

A gigante americana de semicondutores Nvidia anuncia que o conselho de administração está iniciando uma investigação independente em reação à reportagem sobre uma relação íntima entre o diretor-executivo, Jensen Huang, e uma cidadã chinesa que colabora com a inteligência chinesa. A empresa fez o anúncio no domingo, após artigo publicado no fim de outubro pelo *New York Times*. A reportagem indica que a mulher era alta executiva de uma empresa de *data centers* em Singapura e que a inteligência americana a identificou como espiã chinesa. Em comunicado, a Nvidia afirma que o conselho de administração não tem motivo para acreditar que “a segurança nacional ou segredos da Nvidia tenham sido comprometidos”. A empresa acrescenta, contudo, que a investigação do conselho examinará todas as informações disponíveis. Segundo reportagens publicadas no domingo, Huang reconheceu o relacionamento extraconjugal com uma mulher em mensagem interna dirigida à Nvidia. Ele teria declarado que foi “infiel” à esposa e estava “profundamente arrependido”. Huang estaria disposto a cooperar plenamente com a investigação. A Nvidia produz *chips* de ponta usados no desenvolvimento da inteligência artificial. Resta saber se Huang conseguirá dissipar as preocupações sobre as exportações desses chips e os possíveis vazamentos de informações para a China.

(Rádio Japão Internacional, 09-11-2026)

FBI INVESTIGA RELAÇÃO ENTRE DIRETOR DA NVIDIA E MULHER SUSPEITA DE LIGAÇÕES COM INTELIGÊNCIA CHINESA

O presidente americano Donald Trump afirma que o FBI investiga a relação íntima entre o diretor-executivo da Nvidia, Jensen Huang, e uma suposta espiã chinesa. O *New York Times* revelou no mês passado que o fundador da gigante americana de semicondutores mantinha um relacionamento com uma executiva de um centro de dados sediado em Singapura. Segundo o jornal, os serviços de inteligência americanos determinaram que ela colaborava com os serviços de inteligência chineses. Na segunda-feira, Trump declarou ter ficado espantado ao saber dessas alegações. “Sei que o FBI está investigando por outra razão e acho que ele se sairá bem”, afirmou. A Nvidia anunciou no domingo a abertura de uma investigação independente. Segundo a imprensa, a influência de Huang se estende a todo o setor de IA, e essas revelações podem ter repercussões consideráveis. Observadores do mercado estão preocupados com o futuro da direção da Nvidia. As ações do grupo caíram cerca de 8% na segunda-feira, antes de recuperar metade da queda.

(Rádio Japão Internacional, 10-11-2026)

CASO NVIDIA: PEQUIM REJEITA FORMALMENTE AS ACUSAÇÕES DE ESPIONAGEM

O porta-voz do Ministério das Relações Exteriores chinês, Guo Jiakun, rejeitou na segunda-feira uma acusação de espionagem chinesa, após informações divulgadas pela imprensa segundo as quais a Nvidia teria aberto uma investigação sobre seu diretor-executivo, Jensen Huang, depois que ele reconheceu ter tido um relacionamento extraconjugal com uma mulher que, segundo autoridades americanas, trabalhava para os serviços de inteligência chineses. “Essa suposta acusação de espionagem chinesa não tem fundamento. Trata-se apenas de uma campanha de difamação contra a China”, declarou Guo durante uma entrevista coletiva regular, ao ser solicitado a comentar essas informações.

(Rádio China Internacional, 10-11-2026)

INTELIGÊNCIA ALEMÃ AUTORIZADA A RESPONDER ÀS OPERAÇÕES REALIZADAS POR SERVIÇOS HOSTIS

Os deputados alemães aprovaram hoje uma reformulação dos serviços de inteligência do país. Com isso, concedem novos poderes de vigilância e autorização para responder às operações de serviços hostis. Até agora, os serviços de inteligência alemães tinham um papel de coleta de informações. Os serviços de inteligência interna e externa poderão agora realizar ataques cibernéticos para manipular ou apagar dados. Eles poderiam, por exemplo, modificar instruções de fabricação de armas ou sabotar os sistemas de informática de fábricas de drones ou de laboratórios de armas químicas. Por outro lado, os serviços de inteligência não terão autorização para praticar violência contra pessoas.

(Deutsche Welle, 13-11-2026)

ASSUNTOS MILITARES

CERCA DE VINTE EMPRESAS FARMACÊUTICAS IRANIANAS TERIAM SIDO ALVO DE ATAQUES AMERICANOS

As autoridades iranianas lamentam a destruição de cerca de 20 empresas farmacêuticas após os recentes ataques americanos, especialmente na ilha de Qeshm. A Agência Iraniana de Alimentos e Medicamentos informa que os ataques americanos atingiram 15 laboratórios de fabricação de medicamentos e oito empresas de distribuição. O Irã enfrenta dificuldades para garantir o abastecimento de 37 tipos de medicamentos, de um total de aproximadamente 700 medicamentos essenciais, declarou o porta-voz do órgão à agência de notícias *Tasnim*. As repercussões desses ataques poderiam afetar a produção de medicamentos e dificultar a obtenção das matérias-primas necessárias à sua fabricação, acrescentou o porta-voz. Várias explosões foram ouvidas na cidade portuária de Bandar Abbas, no sul do Irã, e na ilha vizinha de Qeshm, informou na noite de domingo a agência de notícias semioficial *Fars*. Segundo essa fonte, as detonações poderiam ser provenientes de tiros de advertência disparados contra navios suspeitos de desrespeitar as regras de navegação no Estreito de Ormuz. As autoridades iranianas ainda não se pronunciaram sobre as causas dessas explosões, esclareceu a agência. Qeshm fica perto de Bandar Abbas, na entrada do Estreito de Ormuz, uma via marítima essencial para as exportações de petróleo do Golfo.

(A Voz da Turquia, 09-11-2026)

POSSÍVEL ENVIO DE FORÇAS SUL-COREANAS AO ESTREITO DE ORMUZ PREOCUPA TEERÃ

Teerã expressou fortes preocupações com o possível envio de militares sul-coreanos ao Estreito de Ormuz. Durante entrevista coletiva na segunda-feira, ao responder a uma pergunta sobre a ampliação da área de operações da unidade naval Cheonghae, o porta-voz do Ministério das Relações Exteriores iraniano pediu a Seul que se abstivesse de enviar forças à região sob o pretexto de contribuir para a reabertura do estreito e evitasse se envolver em uma situação já suficientemente complexa. Esmaïl Baghaï lembrou que a Coreia do Sul e o Irã mantêm relações amistosas há mais de 60 anos, baseadas no respeito mútuo e interesses comuns, e pediu ao governo sul-coreano que não se torne cúmplice das agressões dos EUA, de Israel e de alguns de seus aliados. Também pediu à comunidade internacional que se conscientizasse das repercussões negativas e abrangentes que poderiam ser provocadas pelas ações ilegais de Washington e Jerusalém e se abstivesse de qualquer iniciativa capaz de agravar a situação na região. Cabe lembrar que Seul decidiu recentemente ampliar a área de operações da unidade Cheonghae, encarregada de missões de combate à pirataria no Golfo de Áden, ao largo da Somália, até as águas ao sul de Omã, próximas ao Estreito de Ormuz. Em reação às declarações de Baghaï, uma autoridade do Ministério das Relações Exteriores sul-coreano declarou na terça-feira que a Coreia do Sul pretendia prolongar a permanência de sua unidade naval e reforçar suas missões, respeitando os princípios de não participação e não ingerência no conflito, para proteger seus cidadãos e seus interesses econômicos. Acrescentou que o diálogo prosseguia com os países envolvidos, entre eles o Irã.

(KBS World Radio, 10-11-2026)

TEERÃ ANUNCIA A ATUALIZAÇÃO DE SUA LISTA DE POSSÍVEIS ALVOS MILITARES EM CASO DE RETOMADA DO CONFLITO

As Forças Armadas iranianas atualizaram sua lista de possíveis alvos militares em preparação para conflitos futuros, sem restrição geográfica para os ataques de retaliação, declarou uma alta autoridade militar. O general-de-brigada Kioumars Heydari, subchefe do Estado-Maior das Forças Armadas iranianas, informou que a lista atualizada refletia as diretrizes do líder supremo, aiatolá Ali Khamenei, que pedem “resposta imediata e eficaz, sem limites geográficos” a qualquer ameaça, segundo a agência *ISNA*. “A lista de alvos das Forças Armadas foi atualizada e está pronta para ser transmitida aos comandantes do Exército e do Corpo de Guardiões da Revolução Islâmica (IRGC)”, esclareceu o general Heydari. Ele advertiu que a resposta militar, na eventualidade de um conflito futuro, seria “verdadeiramente paralisante” para o inimigo.

(A Voz da Turquia, 12-11-2026)

ATAQUE IRANIANO TERIA ATINGIDO UM RADAR AMERICANO DE ALERTA ANTECIPADO SITUADO NO BAHREIN

O Corpo da Guarda da Revolução Islâmica do Irã declara ter destruído um sistema de radar americano de alerta antecipado no Bahrein. Mas as autoridades militares americanas afirmam que isso não ocorreu. A IRGC divulgou um comunicado na sexta-feira. Nele, indica que a operação foi uma resposta aos ataques aéreos americanos contra uma instalação de telecomunicações situada em Sirik, no sul do Irã, diante do Estreito de Ormuz. O comunicado qualifica a operação como uma “advertência séria ao agressor” por suas “provocações” nessa via navegável estratégica. Segundo algumas informações, as Forças Armadas americanas estariam dando continuidade a ataques limitados contra o Irã. A imprensa local relata explosões ouvidas em Sirik na noite de quinta-feira. A agência de notícias *Reuters* informa que essa é a primeira vez desde setembro que o Irã afirma ter atacado uma instalação militar americana em um país do Golfo. As forças americanas anunciaram na sexta-feira nas redes sociais que abateram dois drones de ataque iranianos que seguiam em direção ao Bahrein, sem feridos nem danos. As tensões persistem entre os dois países. As autoridades iranianas atacaram navios que acusam de desrespeitar suas instruções no Estreito de Ormuz. As forças americanas mantêm um bloqueio naval aos portos iranianos.

(Rádio Japão Internacional, 14-11-2026)

FORÇAS ARMADAS ISRAELENSES SÃO INSTRUÍDAS A INTENSIFICAR PREPARATIVOS PARA NOVOS ATAQUES CONTRA O IRÃ

O gabinete de guerra israelense ordenou às Forças Armadas que intensificassem seus preparativos para um possível ataque contra o Irã, informou a emissora pública israelense *KAN*. “As diretrizes emitidas pelo gabinete de segurança às Forças Armadas israelenses poderiam levá-las a realizar atividades capazes de

desencadear uma guerra", declarou a emissora. A *KAN* observou que essas diretrizes haviam sido divulgadas depois que o líder do partido Yashar, Gadi Eisenkot, publicou uma declaração pedindo ao primeiro-ministro interino, Benjamin Netanyahu, que se abstivesse de iniciar ataques desnecessários até a formação oficial do novo governo. O gabinete de guerra se reuniu pela última vez em 5 de outubro, três semanas antes das eleições gerais de 27 de outubro. Eisenkot, encarregado de formar o próximo governo israelense, advertiu Netanyahu contra o lançamento de ofensivas de segurança ou militares na ausência de ameaça imediata. Em uma carta oficial enviada a Netanyahu, o dirigente do Yashar ressaltou que o primeiro-ministro preside um governo de transição sem legitimidade parlamentar, informou o site de notícias *Ynet*. "Apenas 46 membros do Knesset ainda apoiam sua permanência no cargo de primeiro-ministro", escreveu Eisenkot, ressaltando que Netanyahu tinha a obrigação de agir com extrema prudência ao definir a política de segurança nacional durante uma transição política delicada. "O emprego das forças de segurança sem uma ameaça direta e imediata que não possa ser adiada poderia ter consequências devastadoras para a democracia israelense e a confiança do público nas instituições governamentais", advertiu Eisenkot. O primeiro-ministro designado pediu a Netanyahu que demonstrasse moderação e responsabilidade nacional, advertindo-o especialmente contra "iniciativas perigosas" que deveriam aguardar a posse de um governo que tivesse a confiança do Knesset.

(A Voz da Turquia, 12-11-2026)

KOALICJA 26.2: PAÍSES OCIDENTAIS SÃO ACUSADOS DE IGNORAR AS PREOCUPAÇÕES LEGÍTIMAS DE MOSCOU

O exercício militar Koalicja 26.2 começa nesta segunda-feira, 9 de novembro, na Polônia, e prosseguirá até 22 de novembro. Ele reúne cerca de 2.800 militares de onze países: Reino Unido, França, Bélgica, Estônia, Alemanha, Lituânia, Países Baixos, Espanha, Suécia, Turquia e Polônia. Em reação às manobras, a porta-voz do Ministério das Relações Exteriores russo, Maria Zakharova, acusou os países ocidentais de continuar ignorando as preocupações legítimas de Moscou em matéria de segurança e de alimentar a escalada das tensões. Ela considerou, em particular, "totalmente inaceitável" o envio de forças armadas estrangeiras à Ucrânia. Advertiu que qualquer unidade militar estrangeira presente em território ucraniano seria considerada pelas Forças Armadas russas um alvo militar legítimo. O exercício ocorre às vésperas da retomada anunciada das consultas trilaterais entre a Rússia, os EUA e a Ucrânia para a solução do conflito. Essas conversações devem ocorrer em Abu Dhabi, nos Emirados Árabes Unidos. As manobras tratam, especialmente, do envio de tropas, do transporte de material militar através das fronteiras, da criação de um comando unificado, da proteção das forças e do apoio logístico.

(A Voz do Vietnã, 09-11-2026)

PETR PAVEL CONSIDERA LAMENTÁVEL A NÃO PARTICIPAÇÃO DAS FORÇAS ARMADAS TCHECAS NO EXERCÍCIO KOALICJA 26.2

O presidente tcheco Petr Pavel considerou lamentável, na quarta-feira, que as Forças Armadas tchecas não participem do exercício militar Koalicja 26.2, organizado na Polônia pelo Reino Unido e pela França. Essas manobras, das quais devem participar 11 forças armadas europeias e cerca de 5.000 soldados, visam preparar uma possível missão de garantia da paz na Ucrânia após o fim da guerra com a Rússia, sem a participação de forças americanas. Segundo Pavel, a República Tcheca deveria participar desse esforço, que também envolve as garantias de segurança para a Ucrânia e a proteção dos países europeus. O presidente fez a declaração antes de uma reunião com o primeiro-ministro Andrej Babiš. O líder do SPD e presidente da Câmara dos Deputados, Tomio Okamura, havia anunciado anteriormente que o governo decidira não enviar soldados a essas manobras. Segundo ele, não cabe aos militares tchecos intervir no conflito entre a Ucrânia e a Rússia. Além disso, Praga não teria recebido um convite oficial, mas representantes das Forças Armadas tchecas participam da preparação do exercício no âmbito dos estados-maiores, a partir de Paris e Lyon.

(Rádio Praga Internacional, 11-11-2026)

PRAGA PLANEJA AUMENTAR CONSIDERAVELMENTE O NÚMERO DE MILITARES PROFISSIONAIS

A nova versão do documento estratégico sobre o desenvolvimento das Forças Armadas tchecas prevê elevar seu efetivo, no longo prazo, para até 38.000 militares profissionais, contra um mínimo de 32.000 na versão anterior. Por outro lado, o texto deixa de fixar um prazo exato para atingir esse objetivo. A versão anterior

previa que, em 2030, as Forças Armadas contariam com pelo menos 32.000 militares profissionais e 10.000 reservistas operacionais. Aprovada pelo governo na semana passada, essa nova versão modifica, assim, os objetivos de recrutamento, substituindo um patamar mínimo por um teto de efetivo. As principais prioridades de modernização das Forças Armadas permanecem, porém, inalteradas, segundo o documento publicado pelo Ministério da Defesa.

(Rádio Praga Internacional, 11-11-2026)

NOVO TIPO DE TORPEDO NORTE-COREANO É TESTADO NO MAR DO LESTE

Coreia do Norte continua sua demonstração de força e testou um novo tipo de torpedo no Mar do Leste. Segundo a agência oficial de notícias, o teste permitiu "verificar a eficácia em combate do novo sistema de torpedos" e "faz parte das atividades obrigatórias dos institutos de pesquisa em ciências da defesa para desenvolver a tecnologia dos sistemas de armas". A *KCNA* também informou que o novo torpedo equiparia a Marinha no início do próximo ano. No entanto, não foram fornecidos detalhes sobre o tipo, desempenho ou plataforma de lançamento. Em 15 de outubro, Pyongyang já havia realizado testes de um sistema de torpedo de alta velocidade e guiagem de precisão que usa inteligência artificial (IA), chamado Zam-2.0.

(KBS World Radio, 10-11-2026)

NOVAS TROPAS NORTE-COREANAS NÃO DEVEM SER ENVIADAS À RÚSSIA, SEGUNDO ANDRII KOVALENKO

A Coreia do Norte não deve enviar novos grandes contingentes militares à Rússia neste inverno. É o que estima Andrii Kovalenko, que dirigiu até setembro passado o Centro de Combate à Desinformação do Conselho de Defesa e Segurança Nacional da Ucrânia. Ele declarou esta semana, nas redes sociais, que essa ameaça parecia ter se dissipado. Em setembro, o presidente ucraniano Volodymyr Zelensky havia afirmado que Pyongyang planejava enviar mais 10.000 soldados norte-coreanos, como reforço aos 8.000 já destacados. Contudo, segundo a autoridade ucraniana, esse cenário não se concretizou, e o regime de Kim Jong-un teria finalmente optado por uma estratégia mais prudente. A Coreia do Norte evitaria, assim, participar dos combates no Donbass, no leste da Ucrânia, embora continuasse desempenhando um papel na guerra ao testar armas e fornecer munições e mísseis balísticos. Segundo Ryo Hinata-Yamaguchi, professor da Universidade Internacional de Tóquio, Pyongyang teria considerado que o envio dos novos contingentes poderia pesar muito sobre seu Exército, sem necessariamente trazer mais benefícios. Ele acrescentou que a advertência de Zelensky provavelmente visava chamar a atenção da comunidade internacional.

(KBS World Radio, 13-11-2026)

ESCALA VIETNAMITA PARA A FRAGATA FRANCESA VENDÉMIAIRE

A fragata de vigilância *Vendémiaire*, da Marinha Nacional Francesa, faz escala de 12 a 16 de novembro em Hai Phong. Essa visita dá lugar a atividades de intercâmbio, encontros profissionais e exercícios conjuntos, com o objetivo de reforçar a cooperação de defesa entre o Vietnã e a França, especialmente em matéria de segurança e proteção marítimas. Destacada regularmente na região do Indo-Pacífico para missões de longa duração, a fragata *Vendémiaire* aproveita essa escala para intensificar seus intercâmbios com as forças vietnamitas. Seu comandante e os oficiais de seu estado-maior se reunirão com os responsáveis pelo Comando da 3ª Região Militar, as autoridades municipais de Hai Phong, bem como os responsáveis pelo Comando da 1ª Região Naval e pelo Comando da 1ª Região da Guarda Costeira. Atividades esportivas e culturais também reunirão os marinheiros franceses e os militares vietnamitas. Além disso, uma delegação do Ministério da Defesa vietnamita irá a bordo do navio para uma visita e encontros profissionais.

(A Voz do Vietnã, 13-11-2026)

RUMO A UM AUMENTO DE 17% NO ORÇAMENTO DE DEFESA DA BULGÁRIA

O projeto de orçamento para 2027 prevê 3,151 bilhões de euros para o Ministério da Defesa, ou seja, 2,23% do PIB. Essa parcela deveria ser de 2,33% do PIB, mas levamos em conta a situação financeira do país, disse o ministro da Defesa, Dimitar Stoyanov, em uma coletiva de imprensa. Isso representa, ainda assim, um aumento de 17% no orçamento das forças armadas em relação a 2026. Não é possível implementar uma

política de remuneração dos militares com essas restrições orçamentárias, observou o ministro. Cerca de 41% do orçamento da defesa serão despesas de investimento (CAPEX), 14,49% serão destinados a despesas de manutenção e 44,54% a salários. São alocados 27,5 milhões de euros para o recrutamento de 1.000 militares adicionais para o Exército, que tem um déficit de efetivo de 20%.

(Rádio Bulgária, 13-11-2026)

NOTÍCIAS DO MERCADO DE ARMAS

EM MANILA, ASSINATURA DE UM ACORDO SOBRE A ENTREGA DE DRONES JAPONESES ÀS FILIPINAS

O Japão entregará drones às Filipinas, no âmbito de um programa de assistência de segurança. Será a primeira vez que Tóquio fornecerá material de defesa montado por meio desse programa. O embaixador do Japão, Kitagawa Katsuro, e a ministra filipina das Relações Exteriores, Maria Theresa Lazaro, assinaram o acordo durante uma cerimônia em Manila na segunda-feira. A Assistência Oficial em Segurança do Japão (OSA) é uma estrutura de assistência em matéria de defesa que permite fornecer material e equipamentos a países que compartilham os mesmos valores. Esse sistema de radar e esses drones constituem juntos o maior projeto da OSA até hoje, ao custo de 4,3 bilhões de ienes (aproximadamente 27 milhões de dólares). Kitagawa declarou que a tecnologia de ponta do Japão "será de grande ajuda para a proteção das vias marítimas vitais", pois reforçará as capacidades de reconhecimento e vigilância do domínio marítimo das Filipinas. Para Lazaro, as Filipinas e o Japão "deram um passo natural e histórico" ao fortalecer seus laços até o nível de parceria estratégica global. As Filipinas e a China têm reivindicações territoriais concorrentes no mar da China Meridional, onde seus navios frequentemente entram em confronto. O novo sistema de radar e os drones devem melhorar a capacidade filipina de monitorar a atividade marítima.

(Rádio Japão Internacional, 10-11-2026)

AUMENTO CONSIDERÁVEL NAS COMPRAS DE EQUIPAMENTOS DE INFILTRAÇÃO PARA AS FORÇAS ESPECIAIS SUL-COREANAS

As autoridades militares preveem aumentar consideravelmente as compras de equipamentos de infiltração destinados ao Comando de Operações Especiais do Exército (SWC), no âmbito da transferência do controle operacional em tempos de guerra (OPCON) dos EUA para a Coreia do Sul. Segundo o projeto de orçamento do Ministério da Defesa para 2027, examinado na segunda-feira pela comissão parlamentar da Defesa, a verba prevista para essa finalidade foi fixada em 131,9 bilhões de *wons*, ou aproximadamente 87,4 milhões de euros, contra 9,8 bilhões neste ano. No total, o SWC deverá adquirir 16.652 equipamentos, incluindo 13 tipos de equipamentos de infiltração em alta altitude e 11 tipos de equipamentos de infiltração submarina, contra 1.003 unidades em 2026. Os equipamentos destinados às operações aerotransportadas deverão ser modernizados, especialmente com a substituição do paraquedas obsoleto MC-4 pelo novo modelo RA-1. O Ministério da Defesa justificou esse forte aumento pela necessidade de reforçar a capacidade do comando de conduzir missões de maneira autônoma, tendo em vista a transferência do OPCON. Desde 2019, Seul e Washington trabalham na criação de seis comandos de componente combinados para preparar essa transferência. Quatro já estão operacionais. Entre os dois últimos, o de operações especiais deverá ser criado até o fim do ano, e o último, em 2027.

(KBS World Radio, 10-11-2026)

SUCESSO CRESCENTE NAS EXPORTAÇÕES DO CAÇA SUL-COREANO FA-50 FIGHTING EAGLE

O caça supersônico sul-coreano FA-50 Fighting Eagle vem obtendo sucesso crescente nas exportações graças ao seu desempenho técnico. Desenvolvido a partir da aeronave avançada de treinamento T-50, ele é capaz de voar a uma velocidade de Mach 1,5 e possui uma manobrabilidade que lhe permite realizar missões polivalentes, tanto no domínio ar-ar quanto no ar-solo. Atualmente, a Força Aérea sul-coreana opera cerca de 60 unidades e alcançou 177.000 horas de voo sem acidentes desde sua introdução em 2013. Essas vantagens conquistaram um número crescente de países estrangeiros e, até o momento, 90 unidades foram exportadas. O caça já foi fornecido às Filipinas (24 unidades), à Polônia (48) e à Malásia (18).

(KBS World Radio, 13-11-2026)

CIBERESPAÇO

PARIS ACUSA HACKERS IRANIANOS DE ESTAREM POR TRÁS DOS ATAQUES CIBERNÉTICOS QUE ATINGIRAM SUPERMERCADOS

O ministro francês das Relações Exteriores acusou o Corpo da Guarda da Revolução Islâmica iraniana (IRGC) de ter orquestrado ataques cibernéticos que provocaram um aumento da temperatura no interior dos refrigeradores e congeladores de centenas de supermercados na França. Jean-Noël Barrot afirmou na segunda-feira, diante da imprensa, que estava em condições de confirmar a responsabilidade da (IRGC). Ele classificou o incidente como o primeiro ataque cibernético de grande escala com o objetivo de sabotar o território nacional. Em outubro, *hackers* atacaram os sistemas de controle da temperatura dos congeladores e refrigeradores de mais de 700 supermercados na França. Grandes quantidades de produtos alimentícios tiveram que ser descartadas. O incidente também provocou cerca de 20 incêndios. O Ministério Público francês afirma que os ataques apresentam as características dos métodos empregados por uma unidade de ataques cibernéticos afiliada à IRGC. Os *hackers* usaram a língua persa e endereços IP localizados no Irã. O órgão esclarece que o chefe da unidade e altos dirigentes são alvo de uma investigação judicial. O Ministério francês das Relações Exteriores declarou ter convocado o embaixador iraniano para apresentar uma queixa. Também indicou sua intenção de propor aos demais Estados-membros da União Europeia que adotem novas sanções contra entidades e indivíduos iranianos suspeitos de estarem envolvidos nos ataques.

(Rádio Japão Internacional, 10-11-2026)

TEERÃ REJEITA CATEGORICAMENTE ENVOLVIMENTO NOS ATAQUES QUE ATINGIRAM SUPERMERCADOS FRANCESES

O Ministério das Relações Exteriores iraniano rejeitou na terça-feira as acusações francesas segundo as quais o Irã estaria envolvido em um ataque cibernético que atingiu os sistemas de refrigeração de centenas de supermercados na França em outubro passado, classificando essas alegações como “maliciosas e desprovidas de fundamento”. Em um comunicado, o Ministério condenou firmemente a prática “desgastada” de acusar o Irã. O Ministério afirmou que essa nova acusação se inscrevia na continuidade das alegações passadas destinadas a desviar a atenção do público das “políticas destrutivas” da França em relação ao Irã e à Ásia Ocidental em geral. Descreveu essa iniciativa como “irresponsável e absurda”, afirmando que ela visava apenas manchar a imagem do Irã e perturbar suas relações com outros países. Ressaltou que o Irã não hesitaria em tomar as medidas “necessárias e apropriadas” para proteger seus interesses nacionais e sua segurança diante de “atividades estrangeiras ilegais”. O ministro francês das Relações Exteriores, Jean-Noël Barrot, declarou na segunda-feira que o Corpo da Guarda da Revolução Islâmica do Irã era responsável pelo ataque cibernético que atingiu os sistemas de refrigeração franceses. Falando a jornalistas em Paris, ao final de uma reunião dos ministros das Relações Exteriores do G7, Barrot indicou que a França havia convocado o embaixador do Irã em Paris para lhe transmitir seus “veementes protestos” a respeito desse ataque.

(Rádio China Internacional, 11-11-2026)

NA COREIA DO SUL, ÓRGÃO RESPONSÁVEL PELA CIBERSEGURANÇA DO SETOR FINANCEIRO É VÍTIMA DE ATAQUE CIBERNÉTICO

O Financial Security Institute (FSI), responsável pela cibersegurança do setor financeiro sul-coreano, foi vítima de invasão cibernética que vazou cerca de 650 itens de dados pessoais relativos a funcionários de 48 instituições financeiras. O órgão informou ter detectado, em 9 de novembro, por volta das 15h00, uma extração de dados após acesso externo não autorizado ao sistema, e tomou imediatamente medidas de emergência, incluindo o bloqueio do acesso à plataforma. Segundo as primeiras constatações, cerca de 200 formulários administrativos, incluindo modelos de consentimento de uso de informações pessoais relativas ao crédito, foram comprometidos. O vazamento envolve cerca de 300 dados pessoais desses documentos, especialmente nomes e datas de nascimento, além de aproximadamente 350 informações relativas aos usuários do sistema. Segundo o FSI, nenhum dado sensível relativo aos clientes nem qualquer informação relacionada à segurança das instituições financeiras foi divulgado. O instituto comunicou imediatamente o incidente à Financial Services Commission (FSC) e à Korea Internet & Security Agency (KISA). Está em curso uma investigação aprofundada para determinar a origem e a extensão desse ataque cibernético.

(KBS World Radio, 11-11-2026)

LAZARUS, GRUPO HACKER NORTE-COREANO, TERIA LANÇADO OPERAÇÕES DE ESPIONAGEM VISANDO TECNOLOGIA DE DRONES

O grupo Lazarus, supostamente ligado a Pyongyang, teria lançado, por volta de junho, operações de espionagem visando às tecnologias de drones e à sua cadeia de suprimentos. É o que indica um relatório publicado recentemente pela empresa europeia de cibersegurança ESET. No caso de uma empresa do setor de defesa situada na Europa Central, um arquivo compactado protegido por senha foi enviado a um dos funcionários. Ele continha um falso documento de recrutamento que imitava os documentos de um grande grupo mundial da indústria de defesa, bem como um programa infectado por um *software* malicioso. Segundo a ESET, essa campanha, que atingiu majoritariamente empresas sediadas na Europa, explica-se pelo lugar cada vez maior ocupado pelos drones na guerra na Ucrânia.

(KBS World Radio, 12-11-2026)

O **Boletim OSINT** – **Inteligência Aberta no Rádio** traz um panorama de notícias militares, de inteligência, terrorismo e cibercrime, resultante da escuta de programas de rádio ao redor do mundo. Trata-se de um informe e não de uma análise: é o registro de escuta das rádios e, portanto, a redação é da mídia citada.

Este monitoramento regular é um excelente barômetro da evolução da situação política internacional e oferece notícias que de outro modo poderiam passar despercebidas.

O boletim é produzido por Alain Charret, ex-oficial da força aérea francesa que serviu em vários centros de escuta na França, especialmente na Alemanha antes da queda da URSS, e é traduzido para português pelo Velho General.

velhogeneral.com.br

Assine o Velho General