

## NA UCRÂNIA, UNIDADES DE ASSALTO COMPOSTAS POR DRONES SUPREM FALTA DE EFETIVOS DO EXÉRCITO

A Ucrânia implementou unidades de assalto por drones que utilizam diferentes tipos para enfrentar as forças russas, superiores em número. O Ministério da Defesa ucraniano anunciou isso na quarta-feira nas redes sociais. Ele especifica que essas unidades associam drones aéreos e terrestres à infantaria dentro de um sistema único, e destaca que elas já foram engajadas em combates reais. O Ministério explica que essa nova abordagem já deu frutos no sul da Ucrânia, onde afirma ter recuperado grande parte do território desde fevereiro graças a essas unidades. A Ucrânia dedica esforços significativos ao desenvolvimento de drones, na esperança de suprir sua falta de efetivos, enquanto a Rússia prossegue com sua invasão. Além disso, o presidente ucraniano Volodymyr Zelensky encontrou-se na quinta-feira com o primeiro-ministro holandês Rob Jetten. Eles assinaram uma declaração de intenção conjunta sobre a cooperação de defesa a longo prazo. Prevê o fortalecimento da coordenação bilateral no desenvolvimento de sistemas de defesa aérea, envolvendo drones e outros equipamentos, como material de guerra eletrônica.

*(Radio Japão Internacional, 18-04-2026)*

## EMPRESAS EUROPEIAS DE DRONES PARA A UCRÂNIA PRESTES A SE TORNAR ALVOS DO EXÉRCITO RUSSO

O ministro das Relações Exteriores tcheco, Petr Macinka, convocou o embaixador russo em Praga após ameaças visando duas empresas tchecas, para que ele explicasse essas declarações. Um porta-voz do Ministério especificou que o embaixador A. Zmeyerovský deve se encontrar com o chefe da diplomacia no início da próxima semana. O Ministério da Defesa russo publicou na quarta-feira uma lista de empresas europeias que fabricam drones para a Ucrânia. Duas empresas com filiais na República Tcheca figuram nela: o endereço em Praga da filial tcheca da empresa ucraniana DeVIRO, bem como a empresa PBS. A Rússia alertou que essas empresas poderiam se tornar alvos militares. A polícia tcheca não dispõe de informações sobre riscos concretos na sequência das declarações russas de que as filiais de empresas ucranianas que produzem drones poderiam se tornar alvos potenciais das forças armadas russas. Ela indicou na quinta-feira que estava avaliando as informações e as possíveis ameaças. O vice-presidente do Conselho de Segurança da Rússia e ex presidente Dmitri Medvedev indicou na rede X que “a lista das fábricas europeias que produzem drones e outros equipamentos constitui uma lista de alvos potenciais para as forças armadas russas”.

*(Rádio Praga Internacional, 17-04-2026)*

## ... TERRORISMO ...

### GOVERNO SOMALI ANUNCIA A NEUTRALIZAÇÃO DE 27 MEMBROS DO AL-SHABAAB

Cerca de 30 militantes do Al-Shabaab teriam sido mortos pelo Exército somali. Pelo menos é o que o Ministério da Defesa somali informou. Vinte e sete militantes do Al-Shabaab teriam sido mortos, segundo o governo somali, durante uma operação de grande escala no estado semiautônomo de Jubaland. Segundo o Ministério, esta ofensiva, apoiada por forças aéreas e apoio internacional, visava áreas do baixo e médio Juba. Ele não nomeou os parceiros estrangeiros envolvidos, mas os EUA realizaram ataques aéreos contra este grupo islâmico. Segundo as autoridades, armas e minas terrestres foram apreendidas e vários altos funcionários do Al-Shabaab estariam entre os mortos.

*(Deutsche Welle, 14-04-2026)*

## ... ATIVIDADES DOS SERVIÇOS DE INTELIGÊNCIA ...

### IRÃ TERIA ADQUIRIDO SATÉLITE ESPÃO CHINÊS EM 2024, DIZ O FINANCIAL TIMES

A informação volta a sugerir o apoio chinês às autoridades iranianas. Desta vez, o jornal britânico garante que as bases americanas no Oriente Médio, onde aviões americanos estão estacionados e que foram atingidas por ataques iranianos, foram vigiadas por um satélite espião chinês. De fato, segundo o *Financial Times* de 15 de abril, o Irã adquiriu secretamente, no final de 2024, um satélite espião chinês. Teerã pôde, portanto, capturar imagens de bases militares americanas em todo o Oriente Médio desde o início da guerra contra o Irã, desencadeada em 28 de fevereiro. As imagens foram capturadas em março, antes e depois de ataques de drones e mísseis contra esses locais, segundo o *FT*. Assim, de acordo com o jornal, o satélite capturou imagens da base aérea Prince Sultan, na Arábia Saudita, nos dias 13, 14 e 15 de março, bem como da base aérea de Muwaffaq Salti, na Jordânia, o quartel-general da Quinta Frota dos EUA localizado no Bahrein, e também do aeroporto iraquiano de Erbil. A cada vez, ataques iranianos se seguiram às datas de captura das imagens, e mesmo que Washington não tenha publicado um balanço, sabe-se que caças e aviões espões foram destruídos nessas bases. O Conselho da Guarda Revolucionária Iraniana obteve acesso a estações terrestres comerciais operadas pela Emposat, uma fornecedora de serviços de controle de satélites e dados com sede em Pequim, garantem também os jornalistas do diário econômico. A Casa Branca não comentou esta informação por enquanto, mas no fim de semana passado, o presidente americano Donald Trump alertou que a China enfrentaria “grandes problemas” se fornecesse sistemas de defesa aérea ao Irã. Contatada pelo diário econômico, a embaixada da China em Washington declarou “rejeitar firmemente” essas informações, que considera uma “propagação de desinformação especulativa e insinuante contra a China”.

(*A Voz da Turquia*, 15-04-2026)

O jornal britânico *Financial Times* afirma ter descoberto o uso pelo Irã de um satélite comercial lançado por uma empresa chinesa para coletar dados sobre bases militares americanas, em todo o Oriente Médio, durante o recente conflito. O jornal relatou na quarta-feira que documentos militares iranianos vazados mostram que o Corpo da Guarda Revolucionária Islâmica (IRGC) adquiriu este satélite no final de 2024, após seu lançamento no espaço pela China. Como parte deste acordo, o IRGC teria obtido acesso a estações terrestres comerciais operadas por um provedor de serviços de controle de satélites e dados com sede em Pequim. O jornal também relata que o satélite é capaz de capturar imagens com uma resolução de cerca de meio metro, o que permite aos analistas identificar aeronaves e monitorar a atividade das bases militares. O *Financial Times* especifica que o satélite militar iraniano mais avançado é muito menos preciso. A análise de coordenadas com registro de tempo, imagens de satélite e dados orbitais sugere que os comandantes militares iranianos usaram o satélite para monitorar e coletar imagens de bases militares americanas no Oriente Médio no momento em que o IRGC conduzia ataques de drones e mísseis contra esses alvos. Questionado sobre as conclusões da investigação do *Financial Times*, o Ministério das Relações Exteriores da China classificou essas informações como falsas.

(*Radio Japão Internacional*, 17-04-2026)

### EM TAIWAN, NOVAS CONDENAÇÕES DE MILITARES ACUSADOS DE ESPIONAGEM PARA A CHINA

O Supremo Tribunal de Taiwan condenou na quarta-feira seis militares taiwaneses, ativos e aposentados, por espionagem em benefício da China, com penas de até oito anos e meio de prisão. Cinco foram considerados culpados de terem constituído uma organização a serviço de Pequim, em violação da lei de segurança nacional: Wang Wen-hao, Tan Chun-ming, Lu Fang-chi, Chiu Han-lin e Yang Chien-hui. Um outro, Yang Po-chih, foi condenado por divulgar informações secretas relacionadas à defesa nacional, em violação ao Código Penal das forças armadas. As penas variam de quatro anos e seis meses a oito anos e seis meses. É possível recorrer. Um chinês portador de um passaporte de Hong Kong, Ding Xiaohu, havia sido indiciado neste caso, mas sua morte em fevereiro de 2026 levou ao arquivamento do processo contra ele. Segundo a promotoria, que indiciou sete pessoas em novembro de 2025, a investigação foi aberta em 2024 pelo Bureau de Investigação em Taipé, na sequência de suspeitas de atividades de espionagem envolvendo Ding, que recrutou vários oficiais aposentados para formar uma rede encarregada de estabelecer contatos e coletar

informações confidenciais. Estes, em seguida, abordaram outros militares, ativos ou aposentados. A operação também visava influenciar os militares da ativa para que adotassem uma atitude passiva em caso de conflito no Estreito de Taiwan. De acordo com os promotores, o Bureau de Investigação e o Ministério da Defesa, o equivalente a 325.000 euros foram transferidos para Taiwan para financiar essas atividades.

*(Rádio Taiwan Internacional, 15-04-2026)*

## **DOIS AMERICANOS ACUSADOS DE FACILITAR CONTRATAÇÃO DE PROFISSIONAIS DE TI NORTE-COREANOS**

Dois americanos que ajudaram trabalhadores norte-coreanos a obter empregos sob falsas identidades em empresas de TI americanas foram condenados a penas de prisão, foi o que anunciou o Departamento de Justiça dos EUA na quarta-feira. De acordo com a *AFP*, os dois homens de Nova Jersey foram condenados a nove anos e a sete anos e oito meses de prisão, respectivamente, por conspiração para cometer fraude eletrônica e lavagem de dinheiro. Eles operavam “fazendas” de computadores, permitindo que pessoas que residem no exterior se conectassem remotamente se passando por americanos, e assim ajudaram norte-coreanos a conseguir empregos remotos. Sua rede teria como alvo mais de 100 empresas americanas, incluindo empresas listadas na *Fortune Global 500*, bem como subcontratadas do setor de defesa. John Eisenberg, procurador-geral adjunto de segurança nacional, disse que essas operações fraudulentas permitiram que profissionais de TI norte coreanos fossem colocados nas folhas de pagamento das empresas sem o conhecimento delas e acessassem seus sistemas de TI, o que ameaçaria a segurança dos EUA.

*(KBS World Radio, 16-04-2026)*

## **... MILITAR ...**

## **HOUTHIS ESTÃO PRONTOS PARA INTENSIFICAR OPERAÇÕES EM CASO DE NOVOS ATAQUES CONTRA O IRÃ**

O grupo iemenita houthi declarou no domingo que intensificaria suas operações militares se os EUA e Israel retomassem seus ataques contra o Irã e o chamado “eixo de resistência”. O Ministério das Relações Exteriores do governo liderado pelos Houthis em Sanaa declarou que “*a firmeza do negociador iraniano na mesa de negociações representa uma nova vitória para a República Islâmica e o eixo da jihad e da resistência*”, segundo a agência de notícias oficial *Saba*. Qualquer escalada provocada pelos EUA na região, especialmente no mar, afetaria negativamente as cadeias de suprimentos, os preços da energia e a economia global, acrescenta o comunicado. Desde o final de março, os Houthis lançaram mísseis e drones em direção a Israel em apoio às “forças aliadas” na região, notadamente as do Irã, Iraque, Líbano e Palestina. O grupo controla Sanaa e a maior parte do norte do Iêmen desde o final de 2014, e apoiou o Irã durante o conflito de 12 dias com os EUA e Israel no ano passado.

*(Rádio China Internacional, 13-04-2026)*

## **EUA CONTINUAM O ENVIO DE TROPAS PARA O ORIENTE MÉDIO**

Segundo o *Washington Post*, 10.000 militares americanos estão sendo enviados nos últimos dias. Entre eles estão o porta-aviões nuclear *USS George Bush* e 4.200 fuzileiros navais com um grupo anfíbio de infantaria naval. Esse envio de tropas acompanha o bloqueio marítimo imposto desde segunda-feira aos portos iranianos e ao Estreito de Ormuz pelas forças armadas americanas. Esta estratégia da administração do presidente Donald Trump visa exercer pressão econômica sobre Teerã, uma vez que 80 a 90% da sua economia depende das suas exportações. O Secretário de Defesa dos EUA, Pete Hegseth, confirmou ontem a manutenção do bloqueio: “*Controlamos o tráfego no Estreito de Ormuz usando apenas 10% da nossa marinha*”, garantiu. Ele especificou que 13 barcos foram abordados ou forçados a dar meia-volta desde segunda-feira. O CENTCOM, Comando Central dos EUA, garante que nenhum navio furou o bloqueio desde segunda-feira. A empresa de rastreamento Tanker Trackers garante o contrário. Imagens de satélite mostrariam vários petroleiros que teriam contornado o bloqueio dos portos iranianos. Mas isso não tem nada a ver com o tráfego pré-guerra na área, onde 120 a 140 navios passavam pelo estreito todos os dias.

*(A Voz da Turquia, 17-04-2026)*

## PYONGYANG CONTINUA DISPAROS DE MÍSSEIS DE CRUZEIRO A PARTIR DO SEU NOVO DESTRÓIER

A Coreia do Norte teria realizado no domingo testes de disparo de mísseis de cruzeiro estratégicos a partir de um novo tipo de destróier. Na terça-feira, a televisão central do estado coreano transmitiu imagens do líder Kim Jong-un assistindo ao disparo de mísseis de cruzeiro e mísseis antinavio do destróier *Choe Hyon*, um navio com capacidade de 5.000 toneladas. A mídia explica que esses testes permitem verificar o sistema de controle de armas integrado do navio. Dois mísseis de cruzeiro estratégicos teriam seguido a trajetória designada por mais de duas horas e três mísseis antinavio por mais de 30 minutos, sobre o Mar Amarelo, a oeste da península coreana, antes de atingir seus alvos. Kim Jong-un teria reiterado o seu compromisso de acelerar o desenvolvimento nuclear e de mísseis balísticos, sublinhando que o reforço constante e ilimitado da dissuasão nuclear, poderosa e fiável, é a prioridade na política imutável de defesa nacional do Partido dos Trabalhadores. Pyongyang também mostra sua intenção de fortalecer suas capacidades navais. No mês passado, a Coreia do Norte já havia realizado dois disparos de mísseis de cruzeiro a partir do destróier. De acordo com alguns especialistas sul-coreanos, esses testes de mísseis de cruzeiro estratégicos podem indicar que Pyongyang quer mostrar que as armas em sua posse são capazes de transportar ogivas nucleares.

*(Radio Japão Internacional, 14-04-2026)*

Kim Jong-un assistiu, no domingo, a testes de disparo de mísseis realizados a partir do novo destróier norte-coreano de 5.000 toneladas, batizado de *Choe Hyon*. De acordo com a *KCNA* na terça-feira, dois mísseis de cruzeiro estratégicos e três mísseis antinavio foram lançados como parte de um teste destinado a avaliar a operacionalidade da embarcação, que deve entrar em serviço em breve. Os primeiros seguiram uma trajetória predefinida no espaço aéreo sobre o Mar Amarelo durante 7.869 a 7.920 segundos, enquanto os segundos voaram durante 1.960 a 1.973 segundos, antes de atingirem os seus alvos com grande precisão. A agência oficial de notícias norte-coreana especificou que o objetivo desta operação era inspecionar o dispositivo de controle de lançamento do sistema integrado de comando de armas, familiarizar os marinheiros com as manobras de implementação do poder de fogo dos mísseis e verificar a precisão e a capacidade de atingir os alvos do sistema de navegação anti-interferência ativa. Fotos publicadas pela *KCNA* mostram o líder norte coreano no cais na companhia de altos oficiais militares. Após observar os disparos, ele foi informado do plano de configuração dos sistemas de armas dos destróieres nº 3 e nº 4, cuja construção está prevista para breve. No seu discurso, Kim saudou os recentes avanços no campo das ciências da defesa, que melhoraram o estado de prontidão do Exército norte-coreano para operações estratégicas. Ele também enfatizou que o fortalecimento contínuo e ilimitado da força de dissuasão nuclear constituía uma linha imutável da política de defesa nacional e a principal prioridade do regime.

*(KBS World Radio, 14-04-2026)*

## NOVO EDIFÍCIO COM INSTALAÇÕES DE ENRIQUECIMENTO DE URÂNIO TERIA SIDO CONSTRUÍDO EM YONGBYON

A Coreia do Norte teria quase concluído a construção de um novo edifício, que abrigaria instalações de enriquecimento de urânio, no seu principal complexo nuclear em Yongbyon. Foi o que estimou ontem o *Beyond Parallel* com base nas últimas imagens de satélite, tiradas em 2 de abril. Segundo o site gerido pelo *Centro de Estudos Estratégicos e Internacionais (CSIS)*, um *think tank* com sede em Washington, as obras do edifício começaram em dezembro de 2024 e o exterior estava quase concluído em junho de 2025. As mesmas fotos mostram os locais para os geradores de emergência, para os escritórios administrativos ou ainda para o estacionamento de veículos. As últimas obras interiores estão em andamento, sendo frequentemente visíveis veículos e supostos trabalhadores no local de construção nos últimos quatro meses. O novo edifício está localizado a cerca de 480 metros a nordeste do laboratório radioquímico (RCL), ou seja, a usina de reprocessamento de combustível nuclear, e a 1.800 metros ao norte da sala das centrífugas. Como lembrete, o chefe da Agência Internacional de Energia Atômica (AIEA) anunciou no mês passado que continuava a monitorar de perto o novo edifício em Yongbyon. Rafael Grossi especificou então que este é semelhante a outro local de enriquecimento de urânio, localizado em Kangson, devido à sua infraestrutura e escala.

*(KBS World Radio, 14-04-2026)*

## AVANÇO NUCLEAR NORTE-COREANO PREOCUPA AGÊNCIA INTERNACIONAL DE ENERGIA ATÔMICA

É discretamente, à sombra do conflito no Oriente Médio que monopoliza a atenção da maioria das chancelarias, que a Coreia do Norte prossegue com os seus avanços em matéria nuclear. Ontem, na Coreia do Sul, o chefe da Agência Internacional de Energia Atômica (AIEA) expressou assim preocupação com um sério avanço das capacidades nucleares norte-coreanas. A construção do que parece ser um novo local de produção de urânio enriquecido permitiria ao regime aumentar a sua produção de armas atômicas. Um novo edifício recém-construído preocupa a comunidade internacional. Identificado por imagem de satélite, este novo anexo do centro de pesquisa atômica de Yongbyon, a 80 km ao norte da capital Pyongyang, vem reforçar o programa nuclear do regime norte-coreano. A Agência Internacional de Energia Atômica confirma um rápido aumento das atividades no centro de Yongbyon, observando notavelmente a operação de um reator de água leve e outras instalações do complexo nuclear. Um sinal, para Rafael Grossi, de que Kim Jong-un tem a firme intenção de desenvolver o seu arsenal nuclear, que já contaria com algumas dezenas de ogivas nucleares. Em março de 2026, Chung Dong-young, o ministro da Unificação da Coreia do Sul encarregado das relações intercoreanas, estimou que a Coreia do Norte poderia ter extraído cerca de 100 kg de plutônio nos últimos 30 anos, incluindo 16 quilos no ano passado. Uma quantidade suficiente para produzir cerca de 20 armas nucleares.

*(Rádio Vaticano, 16-04-2026)*

## COREIA DO NORTE TERIA REALIZADO ATAQUES POR ONDAS ELETROMAGNÉTICAS A SATÉLITES SUL-COREANOS

Entre o início da década de 2010 e o ano de 2024, o Exército norte-coreano lançou frequentemente ataques por ondas eletromagnéticas contra satélites sul-coreanos, militares e civis, a fim de impedi-los de cumprir as suas missões. Isso foi revelado pelo deputado Yoo Yong-won do Partido do Poder Popular (PPP), baseando-se em documentos recebidos do Estado-Maior Conjunto (JCS). Segundo este último, campanhas de interferência de sinais de GPS por Pyongyang teriam perturbado particularmente a transmissão de fotos de satélite. Mas esses problemas não duraram muito e o Sul reagiu imediatamente após a detecção dos sinais. Como lembrete, a Coreia do Norte havia emitido, em 2012, ondas de interferência de alta potência em direção ao primeiro satélite de telecomunicações sul-coreano de uso misto, chamado Mugunghwa 5, a partir de uma antena gigante, localizada perto da sua capital. Uma provocação provavelmente visando testar as capacidades de resposta da nave espacial. Em 2024 também, o regime de Kim Jong-un praticou este tipo de incômodo, derrubando um helicóptero de reconhecimento não tripulado em abril e um drone em novembro. O legislador conservador sugeriu que o Norte está aperfeiçoando essas capacidades de ataque com a ajuda da Rússia. Ele acrescentou que, diante de tal ameaça, o Sul deve legislar sobre o espaço de defesa nacional.

*(KBS World Radio, 17-04-2026)*

## REPÚBLICA TCHECA CRITICADA POR AMERICANOS POR ORÇAMENTO DE DEFESA INFERIOR A 2% DO PIB

O governo tcheco fará tudo para cumprir seus compromissos com a OTAN, declarou o primeiro-ministro Andrej Babiš na noite de quinta-feira, após seu encontro na quinta-feira em Praga com o secretário-geral da Aliança, Mark Rutte. Segundo Babiš, o governo considera a defesa e seus compromissos como importantes e prioritários. O chefe da Aliança indicou que a República Tcheca é, desde sua adesão, um aliado confiável e determinado a contribuir para a defesa comum. Ele lembrou que, face à situação de segurança global, a OTAN decidiu no ano passado aumentar os gastos com defesa. O governo tcheco é criticado notavelmente pelo fato de que, no orçamento deste ano, os gastos com defesa serão inferiores a 2% do PIB. Diplomatas americanos expressaram-se recentemente de forma crítica sobre este assunto. Babiš afirma que o governo tcheco e os representantes da OTAN dispõem de dados diferentes em relação às despesas e à sua participação no PIB; eles, portanto, trocarão esses dados e os discutirão antes da cúpula da OTAN prevista para julho em Ancara. *“É importante que saibamos mutuamente quais são nossas expectativas e nossas possibilidades”*, declarou o primeiro-ministro tcheco durante uma coletiva de imprensa. Rutte saudou a continuação da iniciativa tcheca de munições destinada a apoiar a Ucrânia, que segundo ele tem um impacto real. Ele apelou aos aliados para que continuem a financiá-la. *“A Ucrânia precisa da nossa ajuda para poder dissuadir a Rússia hoje, estar numa posição de força para alcançar a paz e ser capaz de prevenir qualquer agressão futura”*,

declarou Rutte. O governo Babiš, após sua chegada ao poder, não pôs fim a esta iniciativa, mas deixou de financiá-la através do orçamento tcheco.

*(Rádio Praga Internacional, 17-04-2026)*

### **A FORÇA AÉREA DA NOVA ZELÂNDIA É ACUSADA DE ASSÉDIO POR PARTE DA CHINA**

A China afirma ter apresentado uma queixa séria sobre o assédio repetido que teria sofrido por parte da Força Aérea neozelandesa perto do seu espaço aéreo, o que as forças de defesa negam. O porta-voz do Ministério das Relações Exteriores da China, Guo Jiakun, declarou que um avião de patrulha antissubmarino P-8A da Força Aérea da Nova Zelândia havia realizado recentemente várias missões de reconhecimento aproximado e de assédio no espaço aéreo sobre o Mar Amarelo e o Mar da China Oriental. *“Esta ação prejudicou os interesses de segurança da China, aumentou os riscos de mal-entendidos e de erros de cálculo, e perturbou gravemente a ordem da aviação civil no espaço aéreo em questão”*, declarou Guo. *“A China reagiu com firmeza e apresentou sérios protestos à Nova Zelândia.”* Guo declarou que a China instava a Nova Zelândia a respeitar o direito internacional e as normas fundamentais que regem as relações internacionais, a respeitar a soberania e as preocupações de segurança da China e a manter a segurança e a ordem da aviação civil. O porta-voz do Ministério da Defesa Nacional da China, Zhang Xiaogang, declarou que tais atos maliciosos por parte da Nova Zelândia prejudicavam a soberania e a segurança da China, perturbavam gravemente a ordem da aviação civil no espaço aéreo em questão e podiam facilmente desencadear incidentes marítimos e aéreos. *“Instamos o lado neozelandês a impor uma disciplina e uma supervisão mais rigorosas às suas forças da linha da frente, e a pôr termo imediatamente aos atos irresponsáveis que assediam e põem em perigo a segurança da aviação civil.”* Um porta-voz das forças de defesa neozelandesas declarou que os aviões de patrulha marítima P-8A da Nova Zelândia conduziam atividades de vigilância das evasões às sanções norte-coreanas no mar no Norte da Ásia, de acordo com as resoluções do Conselho de Segurança das Nações Unidas. O porta-voz indicou que a Nova Zelândia contribui para o monitoramento das sanções da ONU desde 2018. *“Estas atividades não são dirigidas contra a China, mas visam antes monitorar as violações das sanções das Nações Unidas contra a Coreia do Norte, que ocorrem efetivamente no Mar Amarelo e no Mar da China Oriental.”* O porta-voz declarou que a tripulação das forças de defesa neozelandesas agiu de forma profissional e de acordo com o direito internacional e os procedimentos da aviação civil em vigor na região. *“A NZDF examinou as rotas percorridas e todas as informações disponíveis. Não dispomos de dados que indiquem que eles perturbaram a aviação civil.”* As forças de defesa declararam que a Nova Zelândia adota uma abordagem aberta e transparente no âmbito destas operações. *“Neste contexto, ocorreu um diálogo entre os responsáveis neozelandeses e chineses, e deixamos claro que se trata de um desdobramento de longa data que visa fazer cumprir as sanções impostas pela ONU à Coreia do Norte.”* O porta-voz declarou que as forças de defesa neozelandesas não fariam mais comentários sobre os detalhes destas discussões, nem sobre os detalhes das operações.

*(Rádio Nova Zelândia, 18-04-2026)*

## **... ATUALIDADE DO MERCADO DE ARMAS ...**

### **PAÍSES DO GOLFO REDUZIRIAM DEPENDÊNCIA DE ARMAS DOS EUA VOLTANDO-SE PARA A COREIA DO SUL**

Segundo o *Wall Street Journal* de ontem, os países do Golfo estão tentando reduzir sua dependência dos EUA em matéria de armamento e voltando-se para a Coreia do Sul, o Reino Unido e a Ucrânia, a fim de prevenir um possível vazio nas suas capacidades de defesa aérea. Assim, a Arábia Saudita teria pedido às empresas sul coreanas Hanwha e LIG Nex 1 que antecipassem, se possível, a data de entrega do sistema de mísseis terra-ar Cheongung II (M-SAM), capaz de interceptar drones, mísseis balísticos e aviões. Por sua vez, os Emirados Árabes Unidos, que já utilizaram o Cheongung II face aos ataques iranianos, lhes teriam pedido que fornecessem mísseis interceptadores adicionais, com seus estoques de munições sendo rapidamente esgotados após as últimas seis semanas de ataques aéreos. Segundo o jornal americano, esses países, bem como o Catar, estão examinando várias formas de adquirir armamentos, como drones interceptadores ucranianos, metralhadoras tradicionais americanas ou mísseis de baixo custo desenvolvidos por uma *startup* inglesa. Este passo é interpretado como um desejo de estabelecer uma defesa aérea multicamadas

combinando não apenas sistemas de interceptação de médio alcance, mas também drones interceptadores, equipamentos de guerra eletrônica e meios de defesa aproximada.

(KBS World Radio, 13-04-2026)

### PAÍSES DA OTAN PRESTES A EXPANDIR COOPERAÇÃO COM INDÚSTRIAS SUL-COREANAS DE ARMAMENTO

Uma delegação dos representantes permanentes na Organização do Tratado do Atlântico Norte (OTAN) de 30 países foi recebida ontem em Seul pelo Ministro das Relações Exteriores da Coreia do Sul, Cho Hyun, para discutir a cooperação na indústria de armamento e trocar ideias sobre a situação regional, incluindo a questão da península coreana. As duas partes partilharam a necessidade de expandir a sua cooperação para além dos domínios existentes, particularmente em direção ao espaço e às tecnologias inovadoras, e concordaram em continuar a procurar medidas concretas a este respeito. Além disso, a delegação visitou locais industriais do setor da defesa a fim de observar as competências tecnológicas de ponta das empresas sul coreanas e de compreender melhor o potencial da Coreia do Sul neste domínio. O Ministério estimou que esta visita deverá contribuir para alargar o âmbito da colaboração entre Seul e a OTAN, ao mesmo tempo em que reforça as bases para a entrada de empresas sul-coreanas de defesa nos mercados europeus e transatlânticos.

(KBS World Radio, 15-04-2026)

### ... CIBERESPAÇO ...

#### HACKERS NORTE-COREANOS NÃO PARAM DE APERFEIÇOAR TÉCNICAS UTILIZANDO A INTELIGÊNCIA ARTIFICIAL

Os grupos de hackers apoiados pela Coreia do Norte continuam a aperfeiçoar as suas técnicas de ataque cibernético, adotando uma guerra psicológica sofisticada através das redes sociais ou falsificando suas identidades para serem contratados, com a ajuda da inteligência artificial (IA). De acordo com a análise do Genians Security Center, o grupo APT37 estabelece laços de amizade com os seus alvos, aos quais distribui *software* malicioso. O grupo contacta-os no *Facebook* através de contas que se fazem passar por norte-coreanos, antes de continuar o contato no *Telegram*. Promete lhes enviar documentos criptografados sobre armas militares, para que instalem um falso leitor de PDF. Essa tática é chamada de “*pretexting*”, que consiste em enganar a vítima usando um cenário fictício. Por sua vez, o Group IB identificou casos de contratação onde norte-coreanos geraram uma identidade e um currículo usando IA generativa. Descobriu também um ecossistema de organizações de falsos desenvolvedores operando em várias plataformas, como o GitHub. Estas atividades ilegais começaram já em 2012 e continuaram até março passado. Um funcionário do Group IB sublinhou que estas ameaças vão além do simples âmbito dos problemas de segurança informática. Ele acrescentou que as empresas que empregam involuntariamente trabalhadores ligados a Pyongyang correm o risco de uma pesada responsabilidade legal.

(KBS World Radio, 13-04-2026)

#### NA COREIA DO SUL, MULTIPLICAM-SE ATAQUES CIBERNÉTICOS DESDE INÍCIO DOS ATAQUES CONTRA O IRÃ

Com a guerra no Oriente Médio, o número de alertas de ataques cibernéticos aumentou 2,5 vezes em março. Segundo as autoridades financeiras, estes alertas foram emitidos através do sistema integrado de vigilância do país, denominado FIRST. No entanto, o seu número exato não foi divulgado por razões de segurança. Este aumento é atribuído a fraquezas no *software* da Microsoft ou da Oracle, reveladas durante os ataques cibernéticos apoiados pelo Irã contra os EUA e Israel. Os relatos de tentativas de *hackers* contra instituições financeiras sul-coreanas por meio de plataformas como o *Telegram* também estão aumentando. Um ataque de negação de serviço distribuído (DDoS) contra uma empresa de cartão de crédito sul coreana foi detectado em meados do mês passado. Colocado em serviço no final de fevereiro, o sistema FIRST, gerido pelo Serviço de Supervisão Financeira (FSS), difunde em tempo real às instituições financeiras sul-coreanas os fatores de risco relacionados com vulnerabilidades de *software*, tendências de ataques cibernéticos ou transações eletrônicas fraudulentas. O FSS expandiu a equipe responsável por responder a incidentes de segurança digital, criando duas subequipes responsáveis respectivamente pela análise de risco e pelo monitoramento

de ameaças. Também se comprometeu a reforçar o sistema de prevenção através do compartilhamento de casos de pirataria e de um monitoramento permanente.

(KBS World Radio, 13-04-2026)

### SIDERÚRGICAS ÁRABES INTERROMPEM ATIVIDADES APÓS SEREM VÍTIMAS DE ATAQUES CIBERNÉTICOS

Em um comunicado divulgado na segunda-feira, 13 de abril, *hackers* do grupo pró resistência Handala afirmaram ter infiltrado os sistemas de TI de dois gigantes siderúrgicos árabes, causando uma interrupção total das suas operações. O Handala declarou que seus *hackers* realizaram uma operação cibernética “*sem precedentes e em grande escala*” para infiltrar os sistemas usados pela Sulb, na Arábia Saudita, e pela Foulath, no Bahrein. Este ataque cibernético paralisou estas duas empresas, que produzem coletivamente dois milhões de toneladas métricas de aço por ano, no valor de cinco bilhões de dólares, ainda segundo o mesmo comunicado, no qual Handala afirmou que esta operação as obrigou a suspender suas atividades industriais. O grupo especificou que esta operação constitui uma resposta aos recentes ataques americano-israelenses contra empresas siderúrgicas nos países da Frente de Resistência, especificamente no Irã. “*Nenhum lugar no território inimigo está fora do alcance da ação decisiva do Handala*”, continuou o grupo, que já tinha conseguido penetrar sistemas de TI e bases de dados sensíveis nos EUA e territórios palestinos ocupados.

(Press TV, 14-04-2026)

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](http://velhogeneral.com.br)

[Assine o Velho General](#)