FIESP | DEPARTAMENTO DA INDÚSTRIA DE DEFESA

CLIPPING

17 de janeiro de 2016

Orçamento Geral da União para 2017 é publicado no Diário Oficial*

O Orçamento Geral da União de 2017 foi sancionado sem vetos pelo presidente da República em exercício, Rodrigo Maia, e publicado na edição desta quarta-feira (11) do Diário Oficial da União.

Esta é a primeira peça orçamentária sob vigência da Proposta de Emenda à Constituição nº 55 de 2016 (PEC 55/2016), a PEC do teto dos gastos, que estabelece limite para as despesas públicas pelos próximos 20 anos.

Maia sancionou a lei nesta terça-feira (10), durante viagem do presidente Michel Temer a Portugal, onde participou do funeral do ex-presidente português Mário Soares.

O Orçamento foi aprovado pelo Congresso Nacional em 15 de dezembro do ano passado, com previsão de R$ 3,5 trilhões de gastos federais e salário-mínimo de R$ 945,8.

Em 29 de dezembro, no entanto, o governo corrigiu o cálculo do salário-mínimo e anunciou, por decreto, o valor de R$ 937, em vigor desde 1º de janeiro.

Para 2017, o Orçamento estima que o Produto Interno Bruto cresça 1,3% e a taxa básica de juros, a Selic, fique em 12,11%. A peça orçamentária também prevê 4,8% de inflação e projeta um câmbio de R$ 3,43 por dólar.

A lei prevê que as despesas com juros e amortização da dívida pública consumirão R$ 1,7 trilhão. Segundo o texto, R$ 306,9 bilhões serão destinados ao pagamento de pessoal na esfera federal, R$ 90 bilhões vão para investimentos das estatais e R$ 58,3 bilhões para investimentos com recursos do Orçamento Fiscal e da Seguridade Social.

Essa última dotação subiu R$ 19 bilhões em relação à proposta original. O aumento decorreu de emendas de deputados e senadores às despesas de 2017.

Fonte: Portal Brasil
Data da publicação: 11 de janeiro
Link: http://www.brasil.gov.br/governo/2017/01/Orcamento-Geral-da-Uniao-para-2017-e-publicado-no-Diario-Oficial

Boeing, LM e BAE Systems aumentam produção de armas guiadas*

A Boeing, Lockheed Martin e BAE Systems estão aumentando a produção de kits de orientação de precisão para bombas devido ao aumento dos ataques aéreos contra alvos do Estado Islâmico (ISIS ou EI).

O míssil Hellfire da Lockheed Martin, a bomba de pequeno diâmetro SDB e a bomba JDAM da Boeing estão em baixa nos estoques das forças americanas, de acordo com o Wall Street Journal.
A Força Aérea dos EUA já gastou US$ 2 bilhões em munições guiadas de precisão na campanha contra o ISIS. A Boeing atualmente produz 120 kits de orientação GPS para bombas JDAM por dia.

Fonte: Poder Aéreo
Data da publicação: 16 de janeiro
Link: http://www.aereo.jor.br/2017/01/16/boeing-lm-e-bae-systems-aumentam-producao-de-armas-guiadas/

Contra Informação Digital - Uma bomba invisível*

Por Bruno Ferrari

No meio da tumultuada entrevista coletiva dada na semana passada peio presidente eleito dos Estados Unidos, Donald Trump, recheada de frases fortes, uma ganhou destaque: "Acho que foi a Rússia", disse o republicano.

Trump reconhecia pela primeira vez a participação do governo de Vladimir Putin nos ataques de hackers ao Partido Democrata, de sua oponente Hillary Clinton, durante a campanha eleitoral. Naquele episódio, em setembro de 2016, invasores digitais acessaram os computadores do Comitê Nacional Democrata e de diversos líderes do partido, entre eles o chefe de campanha de Hillary, John Podesta.

Os documentos obtidos não eram especialmente comprometedores, mas foram entregues ao site WikiLeaks, tornaram-se públicos e causaram ainda mais dano à já desgastada campanha de Hillary. Segundo uma avaliação feita pela Central de Inteligência dos Estados Unidos, a CIA, os ataques foram perpetrados por hackers ligados ao governo russo.

A intenção na divulgação do material, segundo a CIA, era ajudar Trump a vencer a eleição. Ainda na coletiva, Trump afirmou não ter nenhum laço ou pendência que pudesse justificar uma preferência russa por ele. O governo russo nega as acusações e não há certezas sobre as intenções dos hackers. O episódio, porém, encaixa-se perfeitamente numa lista de evidências preocupantes sobre uma nova ameaça a democracias.

Nos últimos meses, diversos relatórios de empresas de segurança digital e agências governamentais apontam para ataques hackers e campanhas de desinformação como uma estratégia das agências de inteligência da Rússia.

Os relatos ocorrem em nações em que Putin tem interesses políticos e econômicos. O Instituto Sueco de Relações Exteriores, principal autoridade de política internacional do país, divulgou, em 5 de janeiro, um relatório de 44 páginas a respeito. O documento detalha a ação de grupos ligados ao governo da Rússia para influenciar a opinião pública sueca.

Enumera ações como distribuição de documentos forjados e notícias falsas, assim como o uso tático de sites fantoches em russo e em sueco, com o objetivo de manter a Suécia fora da Organização do Tratado do Atlântico Norte (Otan), aliança ocidental criada em 1949 para fazer frente à União Soviética. "A adesão da Suécia à Otan teria implicações militares e políticas que exigiram da Rússia uma retaliação", disse Maria Zakharova, ministra das Relações Exteriores da Rússia, em 2015.

Segundo os autores do estudo, reportagens mentirosas foram publicadas em veículos de origem russa e depois repercutidas pela versão sueca no Sputnik, veículo que defende os interesses da diplomacia russa. Depois, foram replicadas por sites suecos. "Estabelecemos as intenções das ações, as narrativas dominantes e os padrões comportamentais que têm estreita correlação entre a diplomacia russa, o que sugere que se trata de uma ação coordenada", concluiu o relatório. O documento lista também o uso, pelo governo Putin, de táticas "tradicionais" da geopolítica, como agentes infiltrados e ameaças militares.

Também na semana passada, autoridades na Alemanha disseram estar examinando a proliferação recente e sem precedentes de notícias falsas no país. O comunicado veio em meio a relatos da BfV, agência de inteligência alemã, sobre esforços russos para influenciar a eleição parlamentar na Alemanha, marcada para setembro. A BfV acusa a Rússia de usar ferramentas de propaganda e muito dinheiro numa campanha de desinformação para diminuir o poder do governo da atual primeira-ministra, Angela Merkel.

"Estamos lidando com um fenômeno de dimensão que nunca vimos antes", disse Steffen Seibert, porta-voz do governo alemão, a uma reportagem da agência Reuters publicada na semana passada. Segundo a Reuters, a BfV também confirmou a ocorrência de um ciberataque em dezembro contra a Organização pela Segurança e Cooperação na Europa (OSCE), O ataque usou as mesmas ferramentas vistas numa ação hacker de 2015 contra o Parlamento alemão, atribuída ao grupo de hackers russo APT28.

No fim de dezembro, o FBI, polícia federal dos Estados Unidos, divulgou um relatório de análise conjunta com a empresa de segurança FireEye, que afirma que o APT2S age em apoio aos interesses estratégicos de Putin, principalmente em questões de defesa e geopolítica. A cooperação do grupo hacker com o governo russo ocorre, segundo o relatório, desde 2007, mas intensificou-se nos últimos dois anos.

O estudo do FBI apresentado em dezembro descreve que um aparato de software para invasão de computadores e roubo de informações sugere o apoio do governo da Rússia, uma vez que 97% das amostras de malware (nome dado a programas maliciosos) foram compiladas durante os dias da semana em que há expediente, e 88% delas no período entre 8 e 18 horas no fuso horário de cidades como Moscou e São Petersburgo.

Outro governo que demonstra preocupação com as táticas de "ciberinfluência" russa é a França, que também terá eleições em 2017. O ministro da Defesa, Jean-Yves Le Drian, se pronunciou sobre os ataques de hackers na semana passada, afirmando que os serviços de inteligência do país estão aprendendo as lições com o caso das eleições americanas.

O ministro confirmou a preocupação de uma eventual interferência da Rússia nas eleições. Le Drian disse que o risco ficou ainda mais aparente quando hackers russos atacaram, no ano passado, o canal TV5 Monde, tirando-o do ar.

Nesse cenário, torna-se um exercício razoável, e não paranoico, imaginar qual seria o interesse de Putin na eleição de Montagem de Daniel Graf sobre Fotos de: AFP (3), Reuters e Thinkstock Trump e se o presidente russo teria alguma influência sobre o americano. Mal terminara a coletiva em que o presidente eleito dos Estados Unidos negara laços com a Rússia, reportagens surgiram na imprensa americana afirmando que ele não fora totalmente sincero. Motivos econômicos não faltam para Putin apoiar um governo de Trump.

Um dos primeiros movimentos do republicano ao ser eleito foi anunciar o empresário Rex Til lerson, presidente da petrolífera Exxon-Mobil, como secretário de Estado. Há cerca de três anos, Tillerson recebeu de Putin a Ordem da Amizade, uma honra por seu trabalho pelo "fortalecimento na cooperação no setor de energia" no país.

Em sua sabatina no Senado, na semana passada, Tillerson deu a resposta correta para alguém sob escrutínio: disse ser favorável a manter as sanções econômicas em vigor contra a Rússia, impostas pelos Estados Unidos e pela União Européia após Putin anexar a Crimeia, em 2014. Mas a ExxonMobil tem interesse na suspensão das sanções, para voltar a investir na extração de petróleo na Sibéria e no ártico russo. Trump já indicou que tende a reconhecer a Crimeia como russa e a não confrontar Putin na defesa do ditador Bashar al Assad na Guerra Civil da Síria.

O presidente eleito tem também interesses empresariais na Rússia. Lançou o concurso Miss Universo em Moscou, em 2013, e planejou a construção de uma Trump Tower na capital russa. De acordo com o jornal russo Kommmersant, Donald Trump Jr., filho do presidente eleito, disse a investidores que o grupo planejava construir imóveis em Moscou, São Petersburgo e Sochi.

O herdeiro afirmou em 2008, segundo a imprensa americana, que seus negócios "veem muito dinheiro vindo da Rússia". Na guerra de versões, boatos e desinformação, a munição se torna cada vez mais pesada. Segundo uma reportagem da rede de TV americana CNN, um ex-agente do serviço secreto britânico preparou uin dossiê durante a corrida eleitoral americana a pedido do Partido Democrata.

De acordo com o dossiê mencionado na reportagem, agentes russos têm imagens comprometedoras de Trump participando de uma orgia em Moscou, o que dá a Putin uma ferramenta para chantagear o presidente americano. Trump e o governo russo negaram a existência de tais vídeos.

O ciberespaço é considerado campo de batalha há anos, mas os governos das democracias mais ricas não estavam preparados para esse tipo de confronto. "A Rússia mostrou-se capaz de lançar inovações tecnológicas recentes em ataques, como usar conexões de satélite para infiltrar códigos maliciosos em redes de países", afirma o americano Ben Buchanan, pós-doutorando em cíbersegurança pela Universidade Harvard. "Eles também estão evoluindo suas táticas quando não apenas coletam informações sigilosas, mas criam uma estrutura para divulgá-las à imprensa e às redes sociais de acordo com seus interesses."

Mesmo com as acusações vindas de diversas potências políticas mundiais, pode-se dizer que os russos, pelo menos por enquanto, estão numa posição confortável. Ainda que surjam evidências, como as apontadas no relatório do FBI, é muito difícil comprovar objetivamente a participação do governo Putin nos ataques e manobras de desinformação.

Uma hipótese é que hackers de outros países trabalhem durante o fuso horário russo justamente para criar evidências contra aquele país. E a Rússia está longe de ser a única nação a defender agressivamente seus interesses. Os Estados Unidos agiram fortemente para tentar influenciar os britânicos e levá-los a permanecer na União Européia, no plebiscito do ano passado. "Se usamos táticas cibernéticas para influenciar governos e resultados de eleições em outros países, é mais que natural que também sejamos alvos de estratégias similares" diz Joseph Steinberg, presidente da empresa de segurança SecureMySodal. "O que devemos fazer é nos preparar para reagir a esses ataques. Os eventos recentes mostram que não estamos preparados", diz.

Fonte: Defesanet
Data da publicação: 16 de janeiro
Link: http://www.defesanet.com.br/cyberwar/noticia/24535/Contra-Informacao-Digital----Uma-bomba-invisivel/

O voo internacional da Embraer na área de defesa*

A agenda do executivo Jackson Schneider, presidente da Embraer Defesa & Segurança, sempre esteve lotada de compromissos internacionais. Mas a previsão é que esteja ainda mais cheia de viagens internacionais em 2017. Nos próximos meses, Schneider vai percorrer os quatro cantos do mundo com o objetivo de deixar ainda mais internacional a área de defesa da fabricante brasileira de aviões.

A esperança para alcançar o objetivo reside em um avião com cumprimento de 35,2 metros, altura de 11,8 metros e que pesa, quando carregado, 74 toneladas. É o KC-390, o maior avião militar já fabricado no Brasil. Trata-se de uma aeronave para transporte tático/logístico e para reabastecimento em voo, desenvolvido pela Embraer Defesa & Segurança. “Ele será fundamental para avançarmos internacionalmente”, afirmou Schneider.

Hoje, 8% das receitas da Embraer, que inclui ainda as áreas de aviação comercial e executiva, vêm de contratos no Brasil. No caso da divisão de defesa é o contrário. O País responde por grande parte de seu faturamento, que representou 14,2% do total faturado pela Embraer no terceiro trimestre de 2016.

As primeiras unidades do KC-390 serão entregues no primeiro semestre de 2018, com um ano de atraso. O cliente é a Força Área Brasileira (FAB), que comprou 28 aeronaves por R$ 7,2 bilhões, sendo que o valor também inclui um pacote de suporte logístico inicial.

O atraso na entrega do cargueiro se deve à falta de pagamentos do governo brasileiro, o que obrigou a Embraer a replanejar as etapas de desenvolvimento de sua aeronave. Hoje, o montante a receber do governo federal na área de defesa é da ordem de US$ 296 milhões, o que deve ser acertado ao fim do contrato.

Além do pedido da FAB, a Embraer conta com cartas de intenções dos governos de Portugal, República Tcheca, Argentina, Colômbia e Chile. A Embraer estima que há um potencial global para vender 700 aeronaves deste tipo nos próximos 20 anos.

Para ganhar clientes, a empresa conta com apoio de seus escritórios internacionais. Está presente em Cingapura, Estados Unidos e Holanda. Agora, está reabrindo seu espaço em Abu Dhabi, no Oriente Médio, região que pode ter grande apelo para as vendas do KC-390.

Fonte: Tecnodefesa
Data da publicação: 16 de janeiro
Link: http://tecnodefesa.com.br/o-voo-internacional-da-embraer-na-area-de-defesa/

Testes de aviões antissubmarino russos Il-38 são realizados no Extremo Oriente*

As aeronaves partiram da área militar da Rússia, localizada no mar do Japão. Eles também treinaram simulação de ataque contra submarino inimigo, identificando-o e monitorando-o com ajuda de radares de localização via rádio e dispositivos hidroacústicos durante difíceis condições climáticas.

O Il-38 é a versão atualizada do caça Il-18. Além de detectar e destruir submarinos, a aeronave realiza missões de reunião de informações. O caça é equipado com elementos

de navegação, radares e sistema de pontaria, capaz de detectar navios e submarinos militares.

Fonte: Sputinik News
Data da publicação: 17 de janeiro
Link: https://br.sputniknews.com/defesa/201701177447262-aviacao-militar-da-russia-video/

Enter the Fifth Domain*

As foreign nationals – from independent hackers to criminal organizations to nation-states – continue to test and breach U.S. networks, it is fast becoming clear that the cyberwar is here and is happening on a global scale.

While civilian and defense agencies within the federal government are racing to get up to speed on security and offensive strategies in cyberspace, these discussions are happening independently and often without coordination with others in government, let alone the private sector.

As was seen with the Sony hack – reportedly done by North Korea – the breach of Office of Personnel Management networks – tied to the Chinese government – and attacks on U.S. critical infrastructure – like the dam hacks attributed to Iranian actors – foreign attackers will not be solely targeting our military networks. Unlike traditional domains of warfare, in cyberspace, civilian assets are the prime targets.

With that in mind, Sightline Media Group is proud to announce our newest brand: Fifth Domain, a news and information resource that brings civilian, defense, industry, private

sector and critical infrastructure stakeholders together in one place for a holistic discussion on cybersecurity, both defense and offense.

The website is anchored by breaking and in-depth news from the trusted journalists currently reporting on these issues for C4ISRNET, Defense News and Federal Times, supplemented with original reporting, industry thought-leadership and the data and resources cyber pros need to stay ahead of the adversary.

Fonte: fifthdomain
Data da publicação: 1 de janeiro
Link: http://fifthdomain.com/2017/01/16/enter-the-fifth-domain/

* Não mencionado o autor no texto.