FIESP | DEPARTAMENTO DA INDÚSTRIA DE DEFESA

CLIPPING

19 de dezembro de 2016

- **OTAN quer se manter como pilar em defesa ante planos de UE e Trump***
- **LAAD 2017 terá cluster de Cyber***
- **Por que há uma nova corrida espacial pela conquista da Lua, como na Guerra Fria***
- **Path Forward For Army's Modernization Priorities Takes Shape***

OTAN quer se manter como pilar em defesa ante planos de UE e Trump*

A Organização do Tratado do Atlântico Norte (OTAN) encerra 2016 com a mensagem de que se manterá como a "pedra fundamental" da segurança na Europa diante dos planos da União Europeia (UE) de ganhar autonomia militar e da vitória eleitoral nos Estados Unidos de Donald Trump, que não deu como certa a continuidade de seu país na organização sem mais investimentos europeus.

Em um ano em que o leste da Europa se reforçou ante as ameaças da Rússia e no sul de seu território pelo auge do terrorismo jihadista e a instabilidade que causam as ondas migratórias, a aliança enfrenta agora os desafios de encaixar a vontade da UE de crescer

como potência em defesa e a retórica que, ao menos durante sua campanha eleitoral, Trump usou sobre a organização.

Além de para dar sinal verde ao envio de seis batalhões aos países bálticos e Polônia e reforçar posições no Mar Negro e no Mediterrâneo oriental, a cúpula da OTAN realizada em julho em Varsóvia serviu para que o presidente americano, Barack Obama, corroborasse a solidez do vínculo transatlântico e para assinar com a União Europeia uma declaração para estreitar a cooperação.

A UE está atualmente imersa em um processo interno para fazer efetiva a estratégia global de segurança apresentada em junho pela alta representante comunitária para a Política Externa, Federica Mogherini, que pede mais compromisso dos países frente a "ameaças" desde o exterior.

A saída da UE do Reino Unido, um país tradicionalmente reticente a fortalecer a Política de defesa e Segurança Comum, poderia representar um atrativo a mais para avançar nessa área.

Em uma conferência em novembro, Mogherini insistiu que a UE quer se transformar em "um forte fornecedor de segurança em nossa região e fora dela".

"A UE aumentar suas capacidades de defesa, seria algo necessário de qualquer maneira", disse à Agência EFE o diretor sênior de Política Externa do Centro de Estudos para a Cooperação Transatlântica German Marshall Fund, Ian Lesser.

Na sua opinião, a criação de um Exército europeu -algo que Mogherini já descartou- não é realista, mas sim que os países da UE cooperem mais entre eles e com a OTAN, "simplesmente porque é mais rentável".

A UE e a OTAN, ambas com 28 Estados-membros, compartilham 22 deles.

A diretora do escritório de Bruxelas do Centro de Estudos Bertelsmann Stiftung, Stefani Weiss, disse que o impulso da UE "não é novo", mas acrescentou que "dada a insegurança sobre a direção que os EUA tomará com Trump", a Europa finalmente "pensará seriamente sobre sua segurança e o reforço de capacidades".

"Sem dúvida a eleição de Trump criou novas dúvidas entre os europeus sobre a confiabilidade dos EUA como parceiro da UE e sobre o futuro da Aliança como pedra fundamental da segurança europeia, e global, desde a Segunda Guerra Mundial", indicou à EFE.

Afirmações de Trump durante a campanha como que a Aliança está "obsoleta" porque não aborda de maneira apropriada o terrorismo e porque muitos países europeus não investem o ideal de 2% do PIB em defesa, "parecem fazer condicional o apoio dos EUA à OTAN" no que se refere à defesa coletiva, que é a razão de ser da organização.

Lesser pediu cautela e não dar por feitas as declarações da campanha. "Provavelmente vai haver certo tipo de valorização na Administração de Trump com relação à linguagem", disse.

Em tal sentido afirmou que, "no final, EUA seguirão sendo um aliado de confiança dentro da OTAN".

Segundo dados da OTAN, a despesa em defesa dos países europeus e Canadá subiu 0,6% em 2015 e, neste ano, 1,5% (US$ 3 bilhões a mais) após anos em declínio.

Fonte: Defesanet
Data da publicação: 19 de dezembro
Link: http://www.defesanet.com.br/otan/noticia/24370/OTAN-quer-se-manter-como-pilar-em-defesa-ante-planos-de-UE-e-Trump/

LAAD 2017 terá cluster de Cyber*

Assim como na LAAD Security 2016 (foto), o setor de Defesa e Segurança Cibernética terá destaque na edição de 2017 da LAAD Defence & Security através de uma área dedicada no Pavilhão 4.

O espaço irá reunir empresas que apresentarão soluções e tecnologias como sistemas de segurança da informação, programas de detecção de intrusão, hardware para a composição de laboratórios, simuladores de defesa e guerra cibernética, além de estímulo à produção de software nacional, como antivírus, entre outros.

As 7 previsões para o cibercrime em 2017[1]
The Next Tier – 8 Security Predictions for 2017" é um relatório que está sendo divulgado pela Trend Micro que revela algumas previsões de segurança para o próximo ano.

Nele, a empresa define quais serão as principais ameaças tanto para companhias quanto para usuários finais — e já fique sabendo que o diagnóstico não é bom: "Os ataques serão mais amplos e diferenciados para atingirem novas camadas de vulnerabilidade". "Em 2017, a indústria de segurança cibernética vai aterrissar em um território completamente novo, tendo em vista que o cenário de ameaças digitais de 2016 abriu novas portas que poderão ser exploradas para uma série de ataques.

O aumento de casos de ransomware em dispositivos móveis e a propaganda cibernética influenciando a opinião pública também estarão presentes", diz Raimund Genes, diretor de Tecnologia da Trend Micro.

Vale lembrar que as ações de cibercriminosos têm se tornado cada vez mais refinadas. Em 2016, o maior ataque DDoS da história foi registrado: ele veio em ondas, e o primeiro atingiu um pico de 1.1 Tbps, com uma sequência de 901 Gbps.

Ataques seguintes continuaram com números similares (variando entre 800 Gbps e 900 Gbps), e o CTO da OVH, Octave Klaba, ainda comentou que o botnet DDoS tinha a capacidade de bombardear 1.5 Tbps. Para realizar esse ataque, os hackers usaram câmeras de segurança, por exemplo; ou seja, gadget de IoT (Internet das Coisas).

Segundo a TrendMicro, sobre ataques em softwares em 2016, foram mapeadas 46 vulnerabilidades da Apple, 96 bugs da Adobe e 69 brechas afetando a Microsoft. Provavelmente em 2017, essas ameaças vão persistir por meio do ataque de Exploit Kits. Então, está na hora de melhorar o seu jogo. Se você tem uma companhia ou é usuário final, acompanhe sempre a nossa página dedicada ao assunto para ficar ligado em notícias e dicas sobre segurança. Agora, acompanhe as sete previsões para 2017.

Ransomware não cresce, mas será refinado

Exatamente, o malware mais assustador de que temos conhecimento hoje talvez não cresça em número de ataques, segundo a TrendMicro. Por outro lado, eles ficarão mais refinados. Isso acontece porque, no mesmo compasso que a segurança melhora e as pessoas começam a ficar mais atentas, os cibercriminosos precisam encontrar novas maneiras de invadir e trancar computadores.

Caso você não saiba, o ransomware invade um computador e criptografa todos arquivos, praticamente sequestrando um gadget. Dessa maneira, o cibercriminoso pede um valor X, normalmente em Bitcoins, para liberar os arquivos.

Com a implementação mais massiva da IoT, novos gadgets estão suscetíveis aos ataques — e os gadgets de IoT não costumam ter uma segurança tão robusta quanto desktops,

notebooks e, talvez, smartphones. Em 2017, os ataques de ransomware devem se concentrar também em sistemas de ponto de venda (PoS).

IoT protagonista

Como citamos, a IoT já foi o canal para crackers realizarem o maior ataque DDoS da história em 2016. A tendência é a Internet das Coisas continuar sendo esse canal.

"Com o crescente uso de dispositivos móveis, a tendência é o aumento da exploração de vulnerabilidades nos sistemas de segurança das empresas e também em ambientes industriais, representando ameaças para as organizações. Webcams, roteadores, sistemas de transporte público, ar-condicionado, aquecedores domésticos, carros conectados à internet: todos esses sistemas sofreram ataques remotos de cibercriminosos no ano de 2016", diz o estudo.

A IoT industrial já registrou uma diversidade, segundo a Trend Micro: "Conhecido como BlackEnergy – cavalo de Troia projetado para lançar ataques de negação de serviço –, existe uma grande chance de grupos de espionagem se aproveitarem de empresas distribuidoras de energia, visando ao roubo de dados bancários.

O aumento significativo no número de vulnerabilidades do sistema SCADA (30% do número total de vulnerabilidades encontradas pela TippingPoint em 2016) vai introduzir perigos e riscos sem precedentes para organizações e consumidores".

Mais vazamentos e exposeds

Tanto cibercriminosos quanto células hackers tiveram um 2016 agitado: milhões de bancos de dados e contas foram expostos na internet. Seja por ativismo político ou para causar danos em algum serviço, milhares de companhias sangraram neste ano.

Segundo a Trend Micro, o Comprometimento de E-mails Corporativos (BEC) e o Comprometimento de Processos Corporativos (BPC) continuarão a crescer, tendo em vista que são formas eficazes e relativamente simples de extorsão, levando um funcionário desprevenido a transferir dinheiro para a conta de um criminoso, podendo render até a US$ 140 mil (R$ 470 mil).

De forma alternativa, hackear diretamente um sistema de transação financeira, apesar de ser mais trabalhoso, pode render muito mais para os cibercriminosos — chegando até a US$ 81 milhões (R$ 275 mi). O foco em 2017 está voltado para os CEOs de empresas. "O golpe é fácil e rentável, não exigindo tanto em termos de infraestrutura.

Em dois anos, a perda total estimada por meio do golpe BEC foi de US$ 3 bilhões. Segundo pesquisas da Trend Micro, atacantes foram capazes de extorquir US$ 75 milhões em apenas seis meses".

BEC ganha força

A Trend Micro também nota que em 2017 o "Business Process Compromise (BPC) ganhará força entre os cibercriminosos que buscam atingir o setor financeiro. Possíveis cenários incluem o hacking de sistemas online de compra, para que os criminosos cibernéticos possam receber pagamentos destinados a vendedores reais ou a transferências não autorizadas de fundos".

Adobe e Apple sofrerão mais ataques

Adobe e Apple ultrapassarão a Microsoft em termos de descobertas de vulnerabilidades. A Adobe ultrapassou a Microsoft pela primeira vez em 2016 em termos de descobertas de vulnerabilidades. Entre as vulnerabilidades divulgadas pela Iniciativa Zero-Day (ZDI), até agora em 2016, havia 135 vulnerabilidades nos produtos

Adobe e 76 na Microsoft. "A descoberta de vulnerabilidades da Adobe invariavelmente levará ao desenvolvimento de malwares que podem ser integrados em exploit-kits.

A Trend Micro aconselha aos usuários de produtos Apple e Adobe que protejam os terminais e dispositivos móveis contra malwares que explorem essas vulnerabilidades".

Ciberpropaganda

Cerca de metade da população mundial tem acesso à internet, formando 46% do globo. Ou seja, isso significa um maior alcance dos indivíduos ao fácil e rápido acesso às informações independente da credibilidade que elas contenham.

A Trend Micro mapeou o vazamento de informações em plataformas como o WikiLeaks — usadas para propaganda — com materiais altamente comprometedores a apenas uma semana das eleições nos EUA. "No monitoramento contínuo do cenário underground, foram observados também alguns anúncios dos ganhos de US$ 20 por mês, resultantes da disseminação de propagandas fake sobre candidatos eleitorais.

Foram encontrados também grupos de agentes cibernéticos dedicados a publicar materiais de propaganda em sites de mídias sociais como Facebook e LinkedIn".

A empresa também cita que, em países onde uma eleição está próxima, como França e Alemanha, além de movimentos subsequentes à retirada do Reino Unido da União Europeia (UE), também conhecida como Brexit, serão todos influenciados pelo que é compartilhado e feito por meio da utilização de meios eletrônicos. "Entidades capazes de navegar na opinião pública usando a cyberpropaganda de uma forma estratégica serão capazes de produzir resultados que as favoreçam; 2017 terá um uso muito mais abusivo de informações duvidosas propagadas pelas mídias sociais", define.

Novos alvos com táticas também novas

"Novos movimentos e métodos que vão atacar diferentes empresas, ampliando o número de alvos desviando-se de sistemas antievasivos. Os hackers começarão a fazer uma detecção mais deliberada de sandbox para checar se a rede aceita arquivos desconhecidos", explica a Trend Micro. "Soluções de segurança que utilizam machine learning poderão ser usadas para se proteger de ameaças conhecidas, enquanto tecnologias sandboxing customizadas são capazes prevenir novas versões de ameaças. A tecnologia multicamada pode também auxiliar em uma resposta proativa contra ataques direcionados e será extremamente importante na luta contra esses tipos de campanhas".

Fonte: Defesanet
Data da publicação: 19 de dezembro
Link: http://www.defesanet.com.br/laad2017/noticia/24369/LAAD-2017-tera-cluster-de-Cyber/

Por que há uma nova corrida espacial pela conquista da Lua, como na Guerra Fria*

décadas existe a promessa de uma base na Lua. Colocamos um pé lá, e parou por aí - nossa presença no satélite natural da Terra se resume a pegadas.
Ao mesmo tempo, nos tornamos especialistas em orbitar a Terra a bordo da Estação Espacial Internacional.
No entanto, estão surgindo cada vez mais iniciativas públicas e privadas que não só anunciam um retorno à Lua, mas ambiciosos planos de colonização.

A China já revelou que pretende pousar no lado oculto da Lua (que não pode ser visto da Terra) em 2018, enquanto a Rússia prepara o pouso de sua primeira nave tripulada para 2031.

Os Estados Unidos não se manifestaram como governo, mas em julho deste ano deram permissão para a empresa privada Moon Express ir à Lua. E a NASA convocou recentemente companhias do setor privado a enviarem sugestões de experimentos que podem ser feitos por lá.

A que se deve tanto interesse?

Para o especialista em aeromecânica Leon Vanstone, da Universidade do Texas, o principal motivo é o mesmo da Guerra Fria: poder.

"Devemos lembrar que foram os russos (então União Soviética) os primeiros a enviar um homem ao espaço - eles queriam militarizar o espaço - e os Estados Unidos se apressaram então em colocar um homem na Lua", disse Vanstone à BBC mundo.

Essa demonstração de poder custou centenas de milhões de dólares e, segundo Vanstone, as então potências perceberam que o melhor para todos era realizar iniciativas conjuntas em que os gastos e responsabilidades são compartilhados (como acontece agora na Estação Espacial Internacional).

Mas o tabuleiro do xadrez geopolítico mudou.

A China está crescendo como uma potência espacial, e os Estados Unidos já não têm o mesmo status - dependem dos russos para avançar com seu programa espacial. E, conforme lembra a especialista em Direito Espacial Jill Stuart, da London School of Economics, "há muita tensão entre os Estados Unidos e a Rússia ".

"Então, há sempre uma política complicada por trás", afirmou Stuart à BBC.

Além disso, diferentemente da maioria das agências espaciais do mundo - como a NASA (EUA), ESA (Europa) ou Roscosmos (Rússia) -, o programa espacial chinês é dirigido por militares.

Essa seria a diferença entre o governo chinês e americano.

"Os Estados Unidos não querem dizer que o seu programa é estatal. Na sua política capitalista, preferem dizer 'vamos deixar nossas empresas privadas à frente do programa espacial'", esclarece Stuart.

Para Naveen Jain, um dos fundadores da Moon Express, as possibilidades de negócios na Lua são ilimitadas. Uma licença de uso e exploração permitiria a ele dar início a atividades de mineração, oferecer pacotes turísticos ou vender pedaços de rochas lunares como pedras preciosas.

Stuart e Vanstone deixam claro, no entanto, que essas empresas não são de todo privadas, uma vez que são financiadas com dinheiro do Estado e devem operar sob a tutela da NASA.

Por que agora?

Uma outra razão para a retomada do interesse pela Lula é a tecnologia mais barata.

"A primeira vez que o homem foi à Lua precisou de foguetes gigantes que custaram centenas de milhões de dólares", conta Jain à BBC.

Os avanços na tecnologia permitem que os foguetes sejam menores, mais leves, eficientes e econômicos.

"Estamos usando um foguete menor impresso em 3D que custa menos de US$ 5 milhões", acrescenta o empresário, que planeja enviar no ano que vem uma sonda avaliada em outros US$ 5 milhões para a Lua.

E o avanço tecnológico nos leva à terceira razão para essa "febre" pela Lua: recursos minerais e naturais.

O desenvolvimento de dispositivos inteligentes é possível graças aos raros recursos minerais da Terra, como tântalo ou tungstênio, supercondutores que fazem com que a tecnologia seja rápida, minimalista e econômica.

Jain não esconde que esse é o seu principal interesse no satélite.

"A Lua é extremamente rica em recursos. Tudo pelo que brigamos na Terra está em abundância no espaço", afirma o empresário.

"Lutamos por terra, água e combustível, sem perceber que somos um pequeno ponto azul no espaço", completa.

Vanstone concorda que esse é um interesse comercial e geopolítico importante.

"Cada vez mais pessoas estão interessadas em metais raros, e esse é o interesse de fazer a mineração na Lua", diz.

A questão é que seria muito mais caro trazer esses minerais para a Terra do que continuar a explorar o que temos aqui.

Bases lunares?

O fato de que há muitos recursos na Lua leva a outra motivação: construir bases lunares.

Com o avanço da tecnologia e a capacidade de chegar cada vez mais longe, a Lua se torna apenas um pequeno passo para a exploração do espaço.

Mas, para que isso aconteça, é preciso resolver um problema antes: combustível para viajar. Afinal, a maior parte do peso das naves lançadas ao espaço é de combustível.

Assim que a meta não for mais o nosso satélite, será Marte. E, se um dia chegarmos lá, então o desafio vai além.

Para isso, a Lua poderia ser uma parada estratégica para abastecimento.

E não apenas os Estados Unidos acreditam nisso. A China também está de olho em Marte e anunciou, recentemente, que em 2020 pretende visitar o Planeta Vermelho.

"A Lua pode ser usada como uma base, já que é feita exatamente dos materiais que precisamos", diz Vanstone.

Mas as empresas privadas não a veem apenas como uma base para abastecimento.

"Parafraseando JFK (ex-presidente americano John Fitzgerald Kennedy) 'escolhemos ir à Lua não porque era fácil, mas porque era um bom negócio', e é disso que se trata, de fazer um bom negócio", diz o fundador da Moon Express, que vê a comercialização da Lua como um negócio "grandiosamente genial".

Leon Vanstone reconhece que há muito dinheiro envolvido no espaço.

"E os primeiros a fazer negócio serão aqueles que ganharão mais dinheiro", avalia.

Mas quem pode explorar a Lua?

Esse poderia ser o risco do investimento.

Segundo o tratado sobre a exploração e utilização do espaço, assinado por 103 países em 1967, "o espaço, incluindo a Lua e outros corpos celestes, não deve ser objeto de apropriação nacional por reivindicação de soberania, uso, ocupação ou de qualquer outra forma".

Como os governos poderiam então planejar operações na Lua e conceder concessões a empresas privadas se, a princípio, ninguém tem o poder de fazê-lo?

Embora o acordo internacional afirme que o espaço é um território neutro e ninguém pode se apropriar dos corpos celestes, há diversas interpretações.

"Primeiramente, o tratado especifica que nenhuma nação deve se apropriar de qualquer corpo celeste", diz a especialista Jill Stuart. "Mas há dúvidas se as entidades não-estatais poderiam fazer essas reivindicações."

Em segundo lugar, o fato de que você não pode reclamar a propriedade, não significa que não possa ocupar o espaço.

"É como a Antártida", diz a especialista. "Você pode ter uma base lá, contanto que diga que o que está sob seus pés não é seu", afirma Stuart.

Na Antártida não se pode declarar soberania de nada, mas é permitido ter bases. Será assim na Lua?

Sendo assim, Estados e empresas privadas estão à procura de brechas na legislação de quase 50 anos para abocanhar uma fatia do negócio no espaço.

O Departamento de Estado dos Estados Unidos explicou por escrito à BBC que a permissão dada à Moon Express está baseada no fato de que são "as atividades privadas que desbloqueiam novas investidas espaciais e permitem avançar nossa compreensão do sistema solar, o que, sob vigilância adequada, pode beneficiar todos os países no longo prazo."

O governo dos EUA não ignora o tratado, pelo contrário, considera a responsabilidade de legislar sobre as atividades nacionais no espaço.

"A base para esta jurisdição é mais nacional do que territorial. Entre os objetivos do processo de autorização para atividades privadas no espaço está assegurar o cumprimento do tratado", afirmou.

Para Stuart, o que preocupa são outras iniciativas do governo americano para promover atividades espaciais.

Em novembro de 2015, os Estados Unidos aprovaram uma lei que permite aos cidadãos americanos explorar comercialmente e reivindicar a posse de recursos obtidos no espaço.

"Isso me perturba um pouco", admite Stuart.

"Essa lei tem o potencial de minar o acordo internacional que já está em vigor para o espaço", completa.

Na opinião de Sa'id Mosteshar, do Instituto de Direito e Política Espacial de Londres, essa legislação não cumpre os tratados internacionais.

"Parece que os Estados Unidos estão concedendo a seus cidadãos um direito que o próprio país não tem", disse Sa'id Mosteshar à BBC.

"Você não pode dar um direito nacional que não pode exercer".

Em 1979, antecipando uma futura exploração lunar, a ONU redigiu o Tratado da Lua, estipulando as condições para essa atividade.

A questão é que apenas 13 países assinaram o acordo - e nenhum deles tem recursos para participar de uma corrida espacial.

Para os especialistas, parte do problema é que essas leis foram escritas há muitos anos e não foram atualizadas.

Talvez a exploração da Lua seja inevitável. E a possibilidade de haver bases de diferentes países, como ocorre na Antártida, não está tão distante de acontecer.

Mas, para Jill Stuart, a pergunta que devemos fazer é: quem nós queremos que nos represente no espaço?

"Em breve teremos diferentes entidades pousando em corpos celestes, e acho que devemos nos perguntar quem a gente quer que vá para o espaço e nos represente".

"Eu não quero acordar daqui a 100 anos e descobrir que a Lua é da Coca-Cola", acrescenta.

Fonte: G1

Data da publicação: 18 de dezembro

Link: http://g1.globo.com/ciencia-e-saude/noticia/por-que-ha-uma-nova-corrida-espacial-pela-conquista-da-lua-como-na-guerra-fria.ghtml

Path Forward For Army’s Modernization Priorities Takes Shape*

WASHINGTON -- The Army this week took another step in articulating what types of investments it deems necessary to support operational ideas about future ground warfare.

The service earlier this year presented its “Big 8” initiatives, a list of modernization priorities designed to stay ahead of global threats and maintain overmatch against present and future adversaries. However, the service’s Training and Doctrine Command (TRADOC) has refined that list to the “Big 6+1” set of initiatives, with the “+1” referring to soldier and team performance and overmatch which cuts across all other capabilities listed.

According to a set of slides presented at the Army’s Capabilities Information Exchange with industry, which took place at Fort Eustis, Virginia, on Thursday, the service has carved out solid modernization objectives and the resources needed to meet capabilities in the near-, mid-, and far-term.

The Army will prioritize modernizing its aviation fleet, combat vehicles, cross domain fires, robotics and autonomous systems, advanced protection, and cyber and electromagnetic capabilities.

From 2018 through 2022, the Army will complete its aviation restructure initiative (ARI) that it began in 2013 when it decided to retire its OH-58 Kiowa Warrior armed reconnaissance helicopters and use AH-64 Apache attack helicopters paired with unmanned aircraft systems to fill the gap.

The service will also continue to modernize the AH-64 Echo-model, the UH-60 Mike- and Victor-model Black Hawk utility helicopters and the CH-47F Chinook cargo helicopter. And it will complete the Joint Multi-Role Technology Demonstration as the Army heads

toward its Future Vertical Lift program of record that will bring a next-generation family of helicopters online in the 2030s.

The Army will test fly both a Bell Helicopter- and Lockheed Martin-developed tiltrotor helicopter and a Boeing and Sikorsky-made helicopter with coaxial rotor blades in 2017 and 2018.

Further out, in the years 2023 through 2027, the Army will begin fielding its CH-47F Block II. Some of the planned changes in Block II will be upgrades to the electrical system, transmission and rotor system and will align the conventional Army Chinooks more closely with the MH-47s that Army specials operators fly.

The Army plans to field FVL helicopters in medium-lift and lighter-lift variants and field CH-47 Block III over a larger window of time -- between 2028 and 2050.

As for combat vehicles, the Army in the near-term will address shortfalls in mobility and lethality within the Infantry Brigade Combat Teams. This means bringing a Ground Mobility Vehicle online and using the Joint Light Tactical Vehicle as an interim Light Reconnaissance Vehicle until it can afford to buy something else.

The service will also improve Stryker lethality for the 2nd Cavalry Regiment, currently considered outgunned by its Russian counterparts. Outfitting the vehicle with a 30mm cannon on 81 of the infantry carriers is being fast-tracked with plans to start fielding in 2018.

The Armored Multi-Purpose Vehicle (AMPV) will enter into low-rate production, beginning to replace the obsolete M113 armored personnel carriers first fielded in 1960. BAE Systems presented its first general-purpose AMPV variant to the Army Thursday in a ceremony at its York, Pennsylvania, facility.

Future Fighting Vehicle (FFV) synthetic and physical prototyping, modeling and simulation will take place in the next few years as well. The Army will also focus on developing next-generation power trains that will provide a 50 percent increase in power and will also work on a durable light weight track with hopes of reducing weight and cost while not losing durability.

In the mid-term, the Army will improve limited Mobile Protected Firepower (MPF) capabilities for both IBCTs and Stryker BCTs through modifications to existing platforms and engineering change proposals. The Stryker will also see lethality upgrades in terms of weapons and optics.

The Army will develop a Future Fighting Vehicle to replace the Bradley Fighting Vehicle.

The service plans to incorporate some level of autonomous and remote-operated reconnaissance systems within the combat vehicle fleet in order to replace soldiers having to do “dull, dirty, dangerous tasks.”

In the out-years, the Army will focus on enhancing Armored BCTs capability to deploy, move around easily and bring more lethality to the battlefield. Also planned is bringing a new "direct-fire" system online, to include a main battle tank. The service will divest Bradleys and replace them with the FFV.

"Terrain-shaping" capabilities for cross-domain fires will be fielded at different levels in the near-, mid- and far-term.

More and more, the Army will incorporate robotics and autonomous systems into battlefield maneuvers. From 2018 to 2022, the Army will work on increasing operations at safer standoff distances for the force through robots and autonomous systems. As part of that, the service will develop Automated Ground Resupply through leader-follower robotics technology. Robots will also have the capability to conduct route

clearance and counter improvised explosive devices as well as improve situational awareness.

Between 2023 through 2027, the Army will bring in an unmanned air cargo delivery capability and increase the amount of supply both ground and air platforms can carry into the fight. The service will also introduce exoskeleton technology.

The Army will continue to enhance protection by speeding up the fielding of Active Protection Systems on combat vehicles in the near-term. At the same time, a science and technology effort will work on advanced protection for aircraft. The Common Missile Warning System and the Radar Warning Receiver on aircraft will be upgraded. And the Army will field the CMWS replacement, the Common Infrared Countermeasure, and also the Advanced Threat Detection System (ATDS).

By 2027, the Army will be in the thick of developing a vehicle protection suite to include adaptive armor, "hard-kill" and "soft-kill" capabilities to engage the enemy, and active blast techniques.

And farther afield the service will bring online more advanced aircraft survivability equipment for the legacy fleet and FVL.

While cyber and electromagnetic capability development is more vague, the Army wants freedom to act within space, cyberspace and use electronic warfare to its advantage in the near-term.

Later, the Army plans to employ “the full range of physical and virtual capabilities” and “deny, degrade, disrupt and destroy” enemy networks and weapons. The Army also wants position navigation and timing capability in a GPS-degraded or denied environment.

In the far future, the service will use offensive and defensive cyber and EW tools in formations and at all Army echelons.

The Army has laid out these plans in the hopes of better conveying to industry what problems and gaps it has, what it's looking for and when it wants to buy certain systems. Maj. Gen. Bo Dyess, the Army Capabilities Integration Center's deputy director, told reporters Friday the Army struggles to communicate to industry what it wants and to provide industry with a way to show what it has to address Army needs.

Additionally, the Army wants to find better ways to work with for small, innovative businesses.

The Capabilities Information Exchange (CIE) is an attempt to better interface with industry and to give industry an easier channel to bring capabilities forward for the Army to consider.

Fonte: Defense News
Data da publicação: 16 de dezembro
Link: http://www.defensenews.com/articles/path-forward-for-armys-modernization-priorities-takes-shape

* Não mencionado o autor no texto.