# Vulnerabilidade dos Sistemas Globais de Navegação por Satélite

Capitão de Mar e Guerra (RM1) Carlos Norberto S. Bento

Em um ambiente tenso gerado pelas atuais crises geopolíticas na Ucrânia, em Israel, no Iêmen, em Twain e entre as duas Coréias, onde se tem evidenciado a importância da guerra cibernética nos conflitos modernos, o Ocidente aparenta viver em uma situação de tranquilidade e segurança ilusórias em relação à resiliência de seus sistemas vitais, principalmente os de fornecimento de energia elétrica, de troca de dados, e de informações transmitidas por satélites.

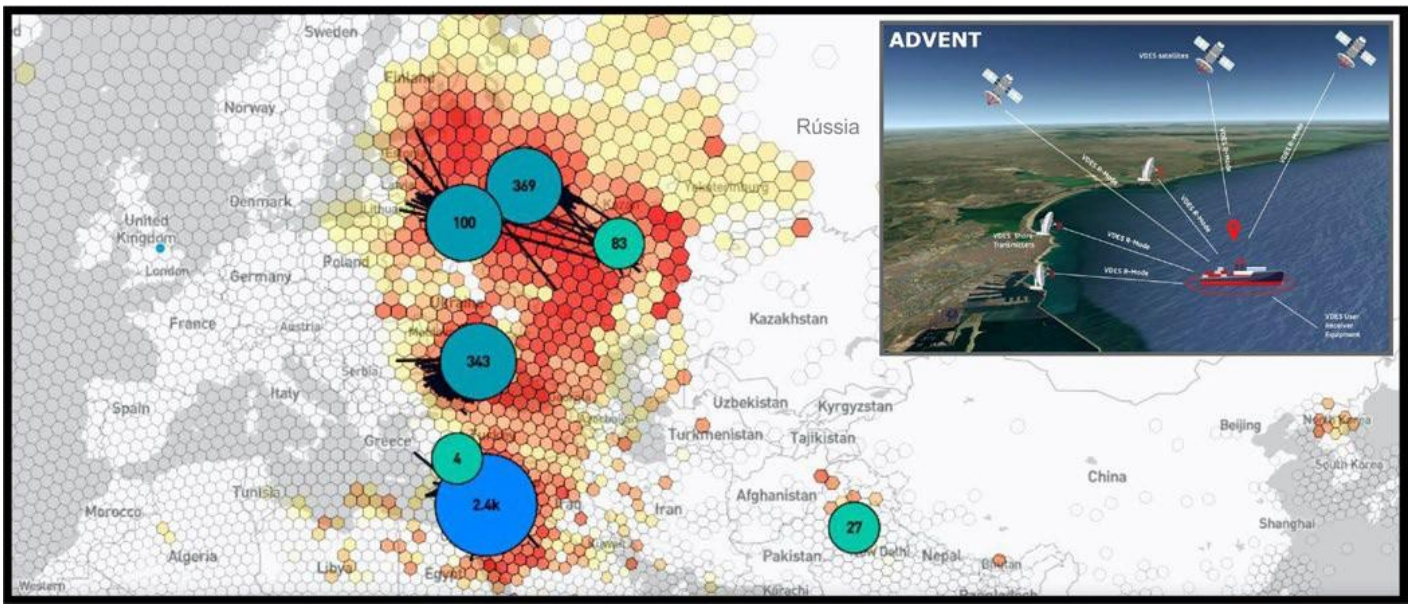
Em paralelo à possibilidade de ataques cibernéticos a sistemas em terra e ataques físicos a cabos submarinos, que conduzem cerca de 90% das informações da Internet, causarem muita apreensão, os Sistemas Globais de Navegação por Satélite (GNSS) como o GPS estadunidense, o Galileo europeu, o GLONASS russo e o BeiDou chinês, apesar de menos vulneráveis a tais ataques, podem ter o sinal de seus satélites negados pelos próprios operadores e estão sujeitos a bloqueios e falsificações desses sinais, podendo afetar todos os sistemas que dependem de Posição, Navegação e Tempo (PNT) e criar grandes desafios e riscos para a aviação, o transporte marítimo e outros serviços essenciais em todo o mundo.

Hoje, as pessoas dificilmente percebem o quão dependentes suas vidas cotidianas são de medições de tempo precisas e confiáveis. Sistemas de infraestrutura crítica operando nos setores financeiro, de telecomunicações, energia, saúde e transporte não podem funcionar adequadamente sem sinais de tempo precisos, cuja falha pode ter consequências sérias, com implicações potenciais incluindo perda econômica, segurança reduzida e perda de vidas humanas. No Ocidente, as principais fontes de sincronização de tempo desses sistemas são sinais transmitidos por satélites GPS, o que compreensivelmente levou a preocupações sobre nossa dependência desse sistema, que continua se expandindo e não dispondo de serviço de PNT alternativo implementado, fazendo a sua confiabilidade diminuir em face do aumento das ameaças e interferências reais. Sem o serviço de PNT prestado pelo GPS, grande parte da vida moderna seria gravemente afetada com o comprometimento de diversos sistemas críticos e de segurança, cortes de energia prolongados, nenhum sinal de celular, usuários sem WhatsApp, UBER, GoogleMaps, Waze etc.

Os sinais do GPS estão sendo bloqueados (jamming) em todo o planeta, mais especialmente perto de zonas de conflito.

O número de ocorrências de interferências intencionais no sinal do GPS tem aumentado consideravelmente nos últimos anos. Ataques de falsificação de sinais (spoofing), que enviam dados enganosos que fazem os receptores de GPS calcularem que estão em outro lugar, e que podem fazer os pilotos e marítimos avaliarem que estão em uma posição ou altitude segura, quando não estão.

Essas interferências vem sendo conduzidas por militares nas últimas duas décadas para defender locais sensíveis contra os ataques de drones e mísseis ou mascarar suas próprias atividades. Os países bálticos acusam a Rússia de bloquear os seus espaços aéreos e o Oriente Médio




*Bloqueio (vermelho) e Falsificação (preto) do sinal GPS (20JUL2024).*
*Fontes: https://spoofing.skai-data-services.com e https://gpsjam.org*
*Solução Advent para PNT alternativo VDES no detalhe.*

tornou-se região focal de interferências. Pesquisadores da Universidade do Texas descobriram que uma das principais fontes de falsificação de sinais é uma base aérea israelense, que em paralelo à sua tarefa de bloquear os sinais para os foguetes do Hamas, acabam afetando os vôos comerciais na região. Enquanto os aviões de carreira têm sistemas de segurança de backup,

no ano passado uma falsificação de sinal quase enviou um jato executivo para o espaço aéreo controlado pelo Irã. A figura acima ilustra a situação.

Enquanto o Galileo, o GLONASS e o BeiDou se modernizam, o GPS não tem um sistema de apoio civil e os EUA estão ficando para trás nessa nova competição no espaço, com os satélites GPS ficando desatualizados, muitos excedendo a vida útil projetada de 8 a 15 anos, e com um lento processo de substituição.Novas tecnologias estadunidenses estão em desenvolvimento, mas pode demorar anos até que sejam amplamente adotadas.A Fundação para Navegação e Tempo Resilientes dos EUA (Resilient Navigation and Timing Foundation - https://rntfnd.org) há anos vem alertando para a gravidade do problema.

O Galileo possui a capacidade de autenticar seus sinais, garantindo que eles sejam reais, e o BeiDou tem o maior número de satélites, com a China construindo uma infraestrutura terrestre para expandir sua cobertura, com estações associadas a 12.000 milhas de cabos de fibra ótica, que transmitem sinais cobrindo todo o país e fornecem serviço de PNT sem satélites.
Na Ucrânia, muitas munições guiadas por satélite fabricadas nos EUA não resistiram à tecnologia de interferência russa, levando Kiev a parar de empregar certos tipos de armamentos fornecidos pelo Ocidente depois que as suas taxas de eficácia despencaram, de acordo com oficiais ucranianos de alto escalão e avaliações internas confidenciais obtidas pelo The Washington Post. A capacidade da Rússia de neutralizar essas armas de alta tecnologia tem sérias implicações para a Ucrânia e seus apoiadores ocidentais, potencialmente fornecendo um modelo para adversários como China e Irã.

A vulnerabilidade dos GNSS fica ainda mais alarmante quando constatamos um aumento da ocorrência de interferências não intencionais ao redor do mundo e a capacidade dos EUA, Rússia e China de destruir satélites no espaço, como fizeram com alguns de seus próprios satélites.

Apesar de existirem receptores híbridos que podem operar com vários GNSS, aumentando a sua resiliência, eles não estão imunes ao bloqueio e falsificação de seus sinais.

O Reino Unido vem conduzindo uma série de estudos e demonstrações sobre o seu sistema de PNT alternativo eLoran, baseado em estações em terra. A Coréia do Sul, usuária do GPS, está pronta para aprimorar sua navegação e confiabilidade de serviço com esse sistema totalmente operacional e estabelecido. Espera-se que tal sistema garanta que os navios possam navegar com segurança mesmo durante interrupções de sinal de GPS em larga escala, como as que o país experimentou recentemente, e para aprimorar a confiabilidade dos serviços dos seus setores público e privado, incluindo transmissão, telecomunicações e finanças.

Apesar de os EUA já terem desenvolvido equipamentos para interferir nos sinais dos GNSS BeiDou e GLONASS, os sistemas eLoran estão atualmente operacionais na China, e a Rússia possui um sistema semelhante (Chayka).

No setor marítimo, além de alternativas baseadas em Sistemas de Referência Inercial (IRS), Bússolas Quânticas e R-Mode, o sistema de troca de dados VHF (VDES - VHFData Exchange System), uma evolução do AIS, também está sendo estudado como uma fonte de alternativa de PNT (A-PNT), particularmente por meio de sua capacidade de longo alcance, conhecida como VDES-R (ver detalhe da figura).

Atualmente, os EUA estão tão dependentes dos sinais de GPS, que a mera ameaça de interrupção dos seus serviços pode ser suficiente para impactar a sua segurança nacional e política externa. O Brasil, como tantos outros países usuários do GPS nos mais variados campos de atividade, provavelmente tenderá a acompanhar alguma solução adotada pelos EUA.

INFORMATIVO OUT/24 nº.16 COMPLETO DISPONÍVEL EM:

https://cembra.org.br/sites/default/files/2024-09/Infocembra16-digital-26set.pdf