La quinta generazione mobile è anche un problema di sicurezza

LINK: https://www.airpressonline.it/36408/36408/

La quinta generazione mobile è anche un problema di sicurezza Secondo una direttiva europea, i satelliti per telecomunicazioni di prossima generazione dovranno essere integrati con il 5G (quinta generazione mobile), dal momento che la quarta generazione non sarà in grado di soddisfare la domanda di dati già nel 2021. A livello industriale se ne discute e già sono pronti i requisiti delle nuove architetture di sistema, che vogliono piattaforme flessibili e riconfigurabili in orbita e maggiore integrazione tra orbite Geo e Leo, nonché tra micro e nano satelliti di prossima progettazione. A questo scopo, nel 2019 l'Agenzia spaziale europea (Esa), a seguito di un accordo con 16 aziende europee, firmato nel 2017, per una rete 5G basata sui satelliti, manderà in orbita un prototipo. Dapprima, per questioni di latenza, lo 'space cloud', che include oltre ai satelliti Geo, HAPS, micro e macro satelliti (in banda Ka per il civile e EHF per il militare) servirà il mercato verticale: trasporti, media, intrattenimento. Come spiegato ieri da Giovanni Nicolai, presidente commissione aerospazio, in occasione del convegno 'Space Cybersecurity: la protezione delle infrastrutture strategiche', organizzato dalla commissione sicurezza informatica dell'ordine degli ingegneri di Roma. L'iniziativa guarda ad un mercato che nel 2020 varrà il 23% in più dei 3 miliardi attuali e al quale l'industria mondiale guarda con particolare attenzione. Dovendo gestire una grande mole di dati, si alza di conseguenza il rischio di attacchi, con bug non prevedibili, che rendono sempre più centrale la protezione da attacchi cyber di tutte le componenti del sistema spaziale, comprese le strutture a terra, che si traduce poi nella sicurezza dell'architettura satellitare complessiva, preposta anche alla protezione di infrastrutture critiche. A livello politico si discuterà di questo a breve, per arrivare ad un regolamento, atteso per dicembre, che prevede un budget di circa 36 miliardi di euro per l'intero settore dello spazio e della difesa. 'Il problema in Europa - osserva Giuseppe Viriglio, senior advisor di Telespazio - è la frammentazione sulla questione di una cyber agenzia. Serve una policy comune per creare tutto l'apparato necessario, un'agenzia di vigilanza unica per dire che siamo in presenza di un attacco e hardware e software adeguati a resistere agli attacchi. Inoltre in Europa manca ancora il set minimo di requisiti per la protezione dei satelliti dagli attacchi cyber'. La questione è in divenire a livello politico europeo, ma l'industria, come detto, si sta portando avanti, mettendo a punto soluzioni atte allo scopo dopo aver identificato rischi e impatti. Telespazio (Leonardo 67%, Thales 33%) in particolare, sta lavorando - come spiegato da Marco Brancati, chief technology officer dell'azienda -, per rendere i suoi centri di controllo, da cui vengono erogati servizi a terzi, sempre più robusti agli attacchi cyber. 'Ci stiamo concentrando nel segmento 'cyber4space' per minimizzare i rischi derivanti da potenziali attacchi ai segnali Satcom e Satnav, con particolare attenzione al filone droni e RPAS (diverse le sperimentazioni già avviate, ndr), dove in tempi rapidi la tematica cyber deve trovare la giusta trattazione'. Nel campo dei velivoli a pilotaggio remoto, settore in grande sviluppo, le sorgenti di attacco cibernetico sono

molteplici, compreso lo spoofing del segnale GNSS. 'Un attacco malevolo ad una o più infrastrutture genera un danno a molti, basti pensare ai trasporti'. Sottolinea Walter Matta, director of strategy, innovation & government di Vitrociset. 'Due anni fa la Commissione europea ha promosso la creazione di una task force per la cyber security, composta da istituzioni e industrie per innalzare il livello di attenzione e creare una capacità di protezione incentrata su centri di competenza nazionali, collegati ad un unico centro europeo, che funga da hub centrale'. 'A livello nazionale serve dunque un test bed per la cyber security, dove fare in ambiente reale e simulato sperimentazione nel dominio spazio, abilitante per tutti gli altri (terrestre, marittimo e aereo, ndr)'. In questo momento c'è un ragionamento aperto su Grottaglie, a seguito di un accordo per 'clusterizzare' le infrastrutture, dove certificare soluzioni e sviluppare tecnologia. 'La tecnologia - conclude Massimo Crisci, a capo della divisione radio frequency system dell'Esa-Estec - non è la parte facile, ma sicuramente la più controllabile'. 'I sistemi spaziali sono distribuiti e vanno protetti globalmente, sia a livello di tutti gli asset che li compongono, sia a livello di dati (per questo si usa la crittografia)". Servirà una combinazione di tecnologie da sviluppare, necessariamente low cost (questo è uno dei problemi principali per Esa, ndr), per le quali gli standard già sono stati fissati. Il tutto - su questo concordano tutti - da implementare sin dall'inizio.