Protezione delle Infrastrutture Critiche: la sfida del 21º secolo

Author : Roberto Di Pietro

Date : 6 Febbraio 2020

Le infrastrutture critiche garantiscono il benessere economico e sociale dei cittadini. Un qualsiasi danno a queste strutture avrebbe un impatto significativo per qualsiasi Paese.

Ad oggi, **sistemi informatici completamente automatizzati** gestiscono e monitorano le infrastrutture critiche civili e militari, compresi aeroporti, porti, ferrovie, impianti di trattamento delle acque, centrali elettriche, reti elettriche e siti di estrazione di petrolio e gas [1]. Inoltre, la pervasività delle tecnologie mobili, dei dispositivi intelligenti, e in generale della persistente connettività alla rete Internet sta facilitando la diffusione di soluzioni operative (OT) efficienti e affidabili, ideali per essere integrate in scenari in cui possibili guasti del sistema possano condurre a conseguenze catastrofiche.

Se però da un lato la crescente integrazione delle tecnologie dell'informazione e della comunicazione ha indubbiamente migliorato l'efficienza delle infrastrutture critiche, la **trasformazione digitale** e l'avvento dell'**Industria 4.0** fanno sì che le pratiche di sicurezza per le infrastrutture critiche diventino sempre più complesse e vulnerabili, in ragione dell'evanescenza del perimetro di sicurezza, della velocità della diffusione di eventuali contagi, e della pervasività dei possibili punti di attacco (si pensi ai dispositivi IoT). Un esempio corrente è dato dall'interruzione dell'erogazione di servizi a causa di attacchi di tipo *ransomware*.

Una dimensione altrettanto importante relativa alla sicurezza delle infrastrutture critiche riguarda la minaccia relativa agli Unmanned Aerial Vehicles (UAVs), ovvero i **droni**, che costituiscono un classico esempio di tecnologia a uso duale, come descritto nel seguito.

Laddove le attività di monitoraggio e manutenzione per le infrastrutture critiche risultano essere di difficile esecuzione per via di difficoltà all'accesso (si pensi a *pipeline* che attraversano deserti) o altamente complesse, gli Unmanned Aerial Vehicles (UAVs), o veicoli aerei senza pilota, costituiscono uno dei trend tecnologici emergenti ed efficaci per rispondere a tali esigenze e garantire una maggiore tempestività di intervento. L'adozione degli UAVs in questi scenari sta crescendo in maniera esponenziale sul mercato, grazie ai loro costi sempre più contenuti e a una vasta gamma di avanzate di funzionalità. Tra le varie **applicazioni in ambito civile e militare**, i droni sono già stati adottati per missioni di monitoraggio ambientale e zone ostili, ispezione di gasdotti, controllo perimetrale, sorveglianza a distanza e situazioni contingenti [2]. I droni, pur offrendo grandi benefici, potrebbero però anche essere adottati per scopi illeciti, come ad esempio scattare foto/video violando la **privacy** dell'individuo, violare aree ad accesso limitato, o come vettori d'attacco (ad es. per il trasporto e rilascio di esplosivi o materiali radioattivi) verso bersagli selezionati, come ha dimostrato il recente attacco ai pozzi petroliferi Sauditi.

L’attacco alle piattaforme petrolifere dell’Arabia Saudita ha infatti evidenziato come l’utilizzo di droni coordinati tra loro ha costituito una **minaccia rilevante** contro le più costose e sofisticate tecnologie di difesa adottate dai Sauditi. Ad esempio, un drone fatto volare a bassa quota invece di uno che sorvola ad alta quota consente di eludere i sistemi di intercettazione adottati per l’identificazione di tali minacce (ad esempio il RADAR). Questa criticità ha portato quindi a un rialzo sia nei costi di produzione che dei prezzi del petrolio sul mercato internazionale, oltre ad allarmare l’intero settore industriale.

Spostandoci dal Middle East verso l’Europa, **un esempio significativo** è stato l’attacco all’aeroporto londinese di Gatwick mediante un numero non ben precisato di velivoli a guida autonoma. La mancanza di un *Intrusion Detection and Prevention System* all’interno dell’aeroporto ha costretto circa 140.000 passeggeri a subire disagi nelle partenze con circa la cancellazione di 800 voli. Si stima infatti che le perdite derivanti da tale attacco si aggirano intorno ai 25 milioni di dollari. Ad aprile 2019, invece, sono stati dirottati circa quattro voli all’aeroporto di Milano-Malpensa a causa della presenza di un drone non autorizzato, costringendo l’infrastruttura ad adottare misure di prevenzione per la salvaguardia delle persone. Infine, lo scorso 9 maggio 2019 anche l’aeroporto di Francoforte in Germania è stato vittima di analoghe problematiche dovute all’intrusione di droni, comportando disagi significativi per i passeggeri.

L’intrusione di tali velivoli non autorizzati ha messo in risalto come gli **attuali sistemi di difesa** adottati nelle infrastrutture critiche non siano ancora in grado di individuare e contrastare tali minacce.

In sintesi, la facile reperibilità e la difficile tracciabilità di droni e mini-droni stanno consentendo a criminali e terroristi di ricorrere a strategie di attacco dai costi estremamente ridotti senza avvalersi di tecnologie estremamente sofisticate e dispendiose per portar a termine un attacco.

A tal proposito, la progettazione e realizzazione di metodi e soluzioni volte al **miglioramento della resilienza, prevenzione e protezione delle infrastrutture critiche** contro minacce e attacchi cyber-fisici, con particolare riferimento ai droni, diventano cruciali.

In questo contesto il gruppo di ricerca afferente al Cybersecurity Security and Innovation Lab (https://cri-lab.net) presso il College of Science and Engineering dell'Hamad Bin Khalifa University, Doha (Qatar), guidato dal Prof. Roberto Di Pietro, sta mirando a sviluppare e implementare diverse **contromisure** (come ad esempio un framework per l'identificazione dei velivoli sospetti, sistemi di navigazione di emergenza per UAV, e lo sviluppo di tecniche avanzate di jamming e anti-jamming) per ridurre al minimo gli attacchi ed i rischi implicati dai droni [3],[4].

Il framework messo a punto per l'identificazione dei droni consente di analizzare direttamente il traffico di rete "*cifrato*" scambiato tra un controller remoto e il drone in diversi scenari eterogenei, consentendo all'infrastruttura critica di:
(i) discriminare i movimenti del drone;
(ii) discernere se è in volo o fermo.

A questo passo fanno seguito l'applicazione di tecniche innovative di ***jamming* selettivo** che consentono di inibire il drone, in un contesto in cui le comunicazioni amiche possono continuare e che consentono di essere impiegate in concomitanza con soluzioni di ***anti-spoofing*** (per i sistemi amici) del Global Positioning System (GPS).

Infine, il CRI-LAB sta sviluppando soluzioni ICT di frontiera per protocolli e applicazioni sicure su diversi temi ricerca tra cui l'Internet of Things [5], l'Industrial Internet of Things, comunicazioni in ambito marittimo e avionico e soluzioni di sicurezza basate su blockchain.

Bibliografia

[1] Cazorla, Lorena, Alcaraz, Cristina and Lopez, Javier, *Cyber stealth attacks in critical information infrastructures*, IEEE Systems Journal 12.2 (2016).

[2] Altawy, Riham and Amr, M. Youssef, *Security, privacy, and safety aspects of civilian drones: A survey*, ACM Transactions on Cyber-Physical Systems 1.2 (2017).

[3] Tedeschi, Pietro, Gabriele Oligeri, and Roberto Di Pietro, *Leveraging Jamming to Help Drones Complete Their Mission*, IEEE Access (2019).

[4] Sciancalepore, Savio, Ibrahim, Omar Adel, Oligeri, Gabriele, and Di Pietro, Roberto (2019), *PiNcH: an Effective, Efficient, and Robust Solution to Drone Detection via Network Traffic Analysis*, Computer Networks, 2020.

[5] Tedeschi, Pietro, Savio Sciancalepore, Areej Eliyan and Roberto Di Pietro, *LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications*, IEEE Internet of Things Journal

(2019).

Articolo a cura di **Roberto Di Pietro** e **Pietro Tedeschi**