REZUMATUL TEZEI DE DOCTORAT

„**INTERNET OF THINGS – Securitate și Aplicații Militare**”

Autor: Cpt.ing. **Marius-Ștefăniță PREDA**
Email: marius.preda@mta.ro, tel.: +40785257440
Conducător de doctorat: Prof. univ. emerit dr. ing. **Victor-Valeriu PATRICIU**

Tema acestei teze explorează potențialul revoluționar al Internetului Lucrurilor (IoT) în remodelarea războiului modern, un context în care tehnologiile emergente și disruptive, cum ar fi IoT, devin din ce în ce mai pertinente. Cercetarea se concentrează pe capacitatea aplicațiilor IoT militare de a influența semnificativ tactica și strategia militară, evidențiată de conflictele recente, precum invazia Ucrainei de către Federația Rusă. Acest context a demonstrat nu doar relevanța aplicațiilor militare IoT, dar și necesitatea urgentă de adaptare a strategiilor militare pentru a integra noile capabilități tehnologice.

IoT introduce complexități semnificative pentru securitatea cibernetică, având în vedere natura sa omniprezentă și convergența elementelor fizice cu cele virtuale. Aceasta rezultă într-un mediu plin de incertitudini, unde amenințările cibernetice pot migra rapid între mediile fizic și virtual. Caracteristicile definitorii ale IoT, precum eterogenitatea și volumul mare de date, accentuează aceste provocări, necesitând soluții de securitate inovatoare și eficiente.

Un risc important la adresa securității naționale, discutat în această teză, este utilizarea tehnologiilor IoT de către actori statali și non-statali pentru a iniția atacuri în spațiul cibernetic, cu consecințe directe asupra securității naționale. Teza avansează analizând modul în care dispozitivele IoT sunt integrate în infrastructurile critice, cum ar fi cele din domeniile energetic și de transport, subliniind riscurile asociate cu perturbările acestora. În contextul războiului hibrid, utilizarea combinată a operațiilor cinetice și cibernetice devine tot mai frecventă, demonstrată de atacurile cibernetice coordonate înainte de acțiuni militare convenționale.

Astfel, problema securității cibernetice a tehnologiilor IoT cu potențial ridicat de aplicare în medii operaționale militare este tratată în această teză punând accent pe trei direcții principale de cercetare. Prima direcție se concentrează pe securitatea rețelelor de senzori IoT, analizând protocolul RPL și tehnologia 6LoWPAN, identificând vulnerabilitățile și metodele de exploatare. Cea de a doua direcție abordează analiza securității traficului de rețea IoT, aplicând tehnici de analiză a datelor pentru a detecta atacuri cibernetice și stabilirea comportamentului normal al rețelei. Cea de a treia direcție revizuiește soluțiile IDS existente pentru IoT, propunând apoi o soluție inovatoare de detectare a anomaliilor bazată pe învățare automată profundă, evidențiind progresele și provocările din acest domeniu. Rezultatele obținute în urma efortului de cercetare contribuie semnificativ la îmbunătățirea securității IoT, oferind soluții inovative și eficiente pentru diverse scenarii operaționale, inclusiv militare.

În final, lucrarea abordează necesitatea integrării IoT cu alte tehnologii emergente și disruptive, cum ar fi inteligența artificială, 5G și Big Data, subliniind cum această fuziune poate spori capacitatea de răspuns și de adaptare a forțelor militare în scenarii de conflict. Acest amestec de tehnologii facilitează o transformare profundă în cadrul operațiilor militare, evidențiind importanța adaptării continue a strategiilor de securitate la evoluțiile tehnologice.

Această teză oferă o perspectivă detaliată și bine documentată asupra rolului crucial al IoT în contextul războiului modern, oferind totodată o analiză complexă a provocărilor și oportunităților prezentate de această tehnologie emergentă din perspectiva securității cibernetice. Prin explorarea interacțiunii dintre tehnologie și strategie militară, lucrarea contribuie substanțial la literatura existentă, propunând noi direcții pentru dezvoltarea și implementarea tehnologiilor IoT în scopuri defensive și ofensive.