Abstract

Securitatea cibernetică constituie cel mai complex segment din domeniul Tehnologiei Informației și Comunicațiilor (IT&C). Înglobează toate subdomeniile acestuia, obligând specialiștii care activează în această zonă să le cunoască și să le înțeleagă în profunzime.

Luând în considerare anvergura atacurilor cibernetice recente și înmulțirea armelor cibernetice, care ar putea aduce atingere vieților omenești prin sabotarea sistemelor de comandă și control ale unor utilități cum ar fi alimentarea cu apă, energie electrică sau administrare trafic, NATO a decis să considere spațiul cibernetic drept cel de al patrulea domeniu strategic al său. Prin această reacție firească la complexitatea proceselor care se desfășoară în sfera cibernetică, NATO permite unui stat membru ca în urma unui atac de tip ”Denial of Service” (DoS) să invoce cel de-al cincilea articol al tratatului Atlanticului de Nord care face referire la apărarea colectivă. Această măsură permite ca un ”banal” atac DoS să constituie începutul unui nou război mondial.

În cadrul tezei se analizează contextul cibernetic actual cu accent pe atacurile la nivel statal și cele la nivel organizațional pentru a determina nivelul de sofisticare la care s-a ajuns. De asemenea, sunt trecute în revistă toate aspectele legale cu privire la conflictele cibernetice atât la nivel statal precum și la nivel organizațional pentru o determinare corectă a nivelului de la care un incident cibernetic poate determina un răspuns armat din partea unui stat membru. Mai mult, sunt propuse câteva măsuri pentru modificări ale cadrului legal în vederea eficientizării analizei care reglementează conflictele cibernetice.

Teza descrie implementarea unor principii biologice aplicate unor procese executate pentru asigurarea securității cibernetice, alături de câteva primitive de inteligență artificială pentru automatizarea triajului evenimentelor de securitate prin calcularea riscului asociat. În egală măsură, se propun o platformă de apărare cibernetică a infrastructurilor critice bazată pe o rețea definită software (SDN) și o platformă automată de analiză malware pentru a proteja împotriva vulnerabilităților de tip ”0-day” și a amenințărilor remanente avansate (APT) care au ca sursă ”Dark Web-ul” sau folosesc protocoale de anonimizare de tipul ”Tor”. Mai mult, se propune o modificare a protocolului ”Structured Threat Information Expression (STIX)” care constă în introducerea noțiunilor de pericol asociat și de marcare a datelor pentru export în vederea eficientizării și securizării schimbului de evenimente de securitate cu alte organizații partenere. În plus, pentru a ușura efortul angajaților dispeceratelor sau punctelor de comandă s-a dezvoltat un modul pentru prezentarea într-o manieră cognitivă a informațiilor de securitate ale unei organizații, în vederea măririi vitezei de reacție a acestora pentru soluționarea unui eveniment de securitate.

Pentru fiecare platformă propusă și implementată sunt prezentate studii de caz și rezultate experimentale validate prin publicații în jurnale și volume ale unor conferințe indexate ISI, IEEE sau DBLP.