Cîmpean (DNSC): Operatiunile cibernetice împotriva statelor membre UE cresc în frecventa, complexitate si magnitudine

Operatiunile cibernetice împotriva statelor membre ale Uniunii Europene sau împotriva aliatilor cresc în frecventa, complexitate si magnitudine, a declarat, marti, directorul general al Directoratului National de Securitate Cibernetica (DNSC), Dan Cîmpean, într-o conferinta internationala de specialitate.

"Dupa cum probabil stiti, Directoratul National de Securitate Cibernetica (DNSC) este o autoritate nationala civila în materie de securitate cibernetica, precum si punct unic de contact pentru celelalte agentii civile nationale cibernetice. Asadar, o prima reflectie pe care o avem se refera la ceea ce se întâmpla în jurul nostru, la ceea ce se întâmpla în Europa si la nivel international. Este un fapt ca operatiunile cibernetice împotriva statelor membre ale Uniunii Europene sau împotriva aliatilor nostri (unele dintre aceste operatiuni fiind sponsorizate de stat) cresc în frecventa, complexitate si magnitudine. Acest lucru submineaza în mod evident stabilitatea infrastructurilor nationale, a economiei, chiar si a pietei unice digitale europene - prin intermediul spionajului cibernetic, al scanarii vulnerabilitatii infrastructurii critice, al DDoS, al ransomware-ului si al tuturor tipurilor de atacuri disruptive, pe care le observam - în special în contextul geopolitic actual. Pe de o parte, institutiile europene iau masuri pentru a proteja piata unica digitala, în timp ce, pe de alta parte, statele membre îsi exercita prerogativele nationale, în special în cazul în care atacurile cibernetice ameninta securitatea nationala sau afecteaza operatorii de servicii esentiale, astfel cum sunt definite în Directiva NIS sau în legislatia locala", a spus Cîmpean.

În viziunea sefului DNSC, tendintele amenintarilor la adresa securitatii digitale, cum ar fi transformarea digitala rapida, proliferarea dispozitivelor Internet of Things (IoT) si cresterea vulnerabilitatilor raportate, au fost însotite de o serie de tendinte politice si strategice profund îngrijoratoare. Astfel, Cîmpean a mentionat faptul ca statele militarizeaza în mod activ spatiul cibernetic, ca acestea continua sa reprezinte cel mai mare potential de vatamare în spatiul cibernetic, coroborat cu faptul ca toate capacitatile cibernetice ofensive sunt din ce în ce mai raspândite în contextul a doua tendinte mai largi în materie de conflicte si de razboi, precum operatiunile hibride si utilizarea surogatelor.

De asemenea, alta tendinta evidentiaza faptul ca civilii si companiile sunt victime din ce în ce mai vulnerabile ale atacurilor cibernetice, în timp ce eforturile de a aplica norme de constrângere a comportamentului statului au scazut.

"Cu toate acestea, capacitatea actuala de aparare cibernetica a UE este extrem de limitata. UE continua sa joace un rol consultativ în mare masura, lasând în mâinile statelor membre realitatile strategice si operationale ale apararii cibernetice. Capacitatile existente sunt fragmentate si izolate în cadrul diferitelor institutii, agentii si initiative, ceea ce submineaza, prin urmare, coordonarea si cooperarea. Resursele, atât în ceea ce priveste finantarea, cât si personalul, lipsesc. Însa, indiferent daca luam în considerare utilizarea anumitor mijloace din setul de instrumente ale diplomatiei cibernetice a UE (fie acest regim de sanctiuni cibernetice orizontale autonome sau atribuirea coordonata de UE) sau ca luam în considerare furnizarea unui raspuns tehnic autorilor, exista întotdeauna o nevoie comuna: avem nevoie de capacitate sporita, avem nevoie de cunostinte, trebuie sa dispunem de o rezerva mai mare de resurse pentru a descuraja infractorii de la activitatea lor cibernetica, avem nevoie de capacitati si instrumente diferite si noi pentru a nega beneficiile acestor atacuri cibernetice si pentru a mobiliza în mod corespunzator toti actorii-cheie si resursele împotriva acestora si avem nevoie de responsabilitati suplimentare, mai clare si specifice - activitati de baza - care includ, dar nu se limiteaza la dezvoltarea capacitatii de detectare, capabilitati tehnice de atribuire si capacitatii de raspuns în situatii de criza", a explicat directorul general al DNSC.

Acesta a adaugat ca, în acest moment, atât Uniunea Europeana, cât si România au anumite lacune în ceea ce priveste capabilitatile de securitate cibernetica.

"Pentru a elimina aceste lacune, avem nevoie de o mai mare implicare si o cooperare mai strânsa cu UE, cu organismele guvernamentale nationale, cu operatorii de servicii esentiale, cu mediul academic si cu sectorul privat, în general. În România, de exemplu, avem nevoie si de un actor civil mai bun, mai agil si mai capabil, care sa sustina un nivel înalt de cooperare nationala si internationala si sa transmita mesajul adecvat în acest sens. S-ar putea sa stiti deja, acest actor este noul Directorat National de Securitate Cibernetica care a înlocuit CERT-RO. Aceasta va fi o modalitate institutionala adecvata de a elimina lacunele actuale în ceea ce priveste asteptarile legate de capabilitati si de a permite autoritatilor române sa transmita un semnal diplomatic, dar puternic, ca exista consecinte pentru încalcarea normelor comportamentului responsabil în spatiul cibernetic", a mentionat Cîmpean.

Institutul National de Cercetare-Dezvoltare în Informatica (ICI Bucuresti) a organizat, marti, conferinta internationala intitulata "Constructia digitalizarii globale: crearea de încredere, descurajare si coordonare a politicilor prin diplomatia cibernetica".