PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAŢILOR

HOTĂRÂRE

privind adoptarea opiniei referitoare la

Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator

COM (2016) 410

În temeiul prevederilor art. 67 şi ale art. 148 din Constituţia României, republicată, ale Legii nr. 373/2013 privind cooperarea dintre Parlament şi Guvern în domeniul afacerilor europene şi ale art. 160 - 185 din Regulamentul Camerei Deputaţilor, republicat,

Camera Deputaţilor adoptă prezenta hotărâre.

Articol unic. – Luând în considerare opinia nr. 4c-19/1101, adoptată de Comisia pentru afaceri europene, în şedinţa din 27 septembrie 2016, Camera Deputaţilor:

1. Salută obiectivul declarat de Comisia Europeană de a sprijini acoperirea geografică echilibrată pe piaţa Uniunii cu oferte de produse și servicii de securitate în sectorul tehnologiei informaţiilor şi comunicaţiilor.

2. Salută intenţia Comisiei Europene de a examina posibilitatea dezvoltării, împreună cu statele membre şi regiunile interesate, a unei platforme de specializare inteligentă în materie de securitate cibernetică.

3. Salută intenţia Comisiei Europene de a sprijini securitatea cibernetică prin integrarea acesteia în politicile sectoriale ale Uniunii şi recomandă ca integrarea vizată să ţină cont de repartizarea geografică a vulnerabilităţilor, pentru a sprijini în special statele membre care se confruntă cu riscuri şi sarcini administrative sporite din acest punct de vedere.

4. Îşi manifestă îngrijorarea cu privire la perspectivele limitate de creştere pentru societăţile comerciale cu activitate în sectorul securităţii cibernetice în interiorul pieţei unice, care conduc la o multitudine de fuziuni şi achiziţii de către investitori din afara Europei şi invită Comisia Europeană să ia măsurile necesare pentru a stimula capacitatea de inovare a antreprenorilor europeni din domeniul securităţii cibernetice şi pentru a fructifica disponibilul de finanţare al investitorilor europeni; consideră că riscul pierderii de *know-how* şi expertiză europeană în acest domeniu prin exodul de creiere ar trebui să se afle prioritar pe agenda de lucru a Comisiei Europene.

5. Consideră că potenţialul întreprinzătorilor europeni în domeniul serviciilor referitoare la securitatea cibernetică, în special a celor tineri, ar trebui sprijinit cu mai multă insistenţă la nivelul Uniunii, prin măsuri de protecţie a afacerilor aflate la început şi a microîntreprinderilor, în special în statele membre care se confruntă cu un şomaj ridicat în rândul tinerilor.

6. Atrage atenţia asupra faptului că măsurile de sprijinire a certificării unitare la nivelul Uniunii joacă un rol important în ceea ce priveşte creşterea securităţii produselor şi a serviciilor precum şi a încrederii; această certificare ar trebui limitată la ceea ce este necesar, realizată cu participarea industriilor din domeniu şi prevăzută cu suficientă flexibilitate pentru a permite modificarea operativă ca urmare a progresului tehnic foarte rapid.

7. Sprijină eforturile Comisiei Europene în materie de standardizare şi reglementare a internetului obiectelor, a tehnologiilor 5G, a celor de tip *cloud computing* şi a celor de date şi atrage atenţia asupra necesităţii de a contracara eficient şi din timp fenomenele de tip *malware* care ar putea cunoaşte o extindere masivă odată cu noile tehnologii, pentru unele dintre acestea cum ar fi *ransomware* fiind necesare măsuri coordonate la nivelul Uniunii, inclusiv de tip poliţienesc.

8. Recomandă o acţiune hotărâta la nivelul Uniunii pentru a scădea dependenţa de oligopolurile furnizorilor de sisteme de operare şi programe de calculator, deoarece omogenitatea utilizatorilor astfel generată favorizează criminalitatea cibernetică, pe lângă efectele negative asupra pieţei libere şi asupra cheltuielilor administraţiei publice; propune completarea cu acest obiectiv a strategiei privind securitatea cibernetică.

9. Recomandă sprijinirea educaţiei cetăţenilor cu privire la dezvoltarea unui comportament preventiv pe internet, prin metode active şi fără a se limita la posibilităţile oferite de instruirea *online*, având în vedere că vulnerabilitatea acestora generează riscuri privind securitatea reţelelor pe scară largă în urma utilizării calculatoarelor personale pentru atacuri de tip *botnet*.

10. Recomandă dezvoltarea şi completarea bazei de date privind securitatea cibernetică prevăzute la nivelul Uniunii, pentru a include atât informaţii relevante privind combaterea criminalităţii cât şi rezultate ale cercetării ştiinţifice în domeniu, ca parte a *cloud*-ului ştiinţei deschise, astfel încât aspectele privind securitatea cibernetică să poată fi incluse în proiectarea şi dezvoltarea noilor produse şi tehnologii încă din faza emergentă de laborator sau de pilot.

11. Îşi manifestă îngrijorarea cu privire la subraportarea incidentelor de securitate cibernetică şi cheamă la o acţiune la nivelul Uniunii pentru a crea un sistem facil de raportare a acestor incidente, spre exemplu prin intermediul unui modul al platformei *online*, care să fie accesibil tuturor cetăţenilor europeni, în scopul reducerii riscului generat de cunoaşterea incompletă a naturii şi modalităţii de acţiune în domeniul criminalităţii cibernetice şi pentru a pune la dispoziţia IMM-urilor sau a întreprinderilor preocupate de confidenţialitatea datelor lor un instrument de colectare de informaţii minimale.

12. Atrage atenţia asupra gradului scăzut de conştientizare a riscurilor de securitate cibernetică reprezentat de evoluţia rapidă a domoticii, internetului lucrurilor şi *cloud-computing*-ului şi recomandă introducerea unui sistem voluntar de atenţionare a utilizatorilor de către fabricanţii şi vânzătorii de produse şi servicii în aceste domenii, sistem armonizat pe planul Uniunii pentru a facilita libera circulaţie şi care ar putea fi elaborate ca o dezvoltare a sistemului de etichetare prevăzut de comunicare.

13. Atrage atenţia asupra conexiunilor dintre securitatea cibernetică, atacurile asupra conturilor bancare şi finanţarea terorismului şi invită Comisia Europeană să desfăşoare acţiuni concrete şi hotărâte pentru a reduce riscurile de creştere a atacurilor cibernetice şi de sporire a impactului lor distructiv.

14. Salută modul coerent şi complet în care a fost elaborată comunicarea, cu identificarea corespunzătoare a nevoii intensificării cooperării pentru pregătirea răspunsului la incidentele cibernetice la nivelul Uniunii, atât între instituţiile europene şi autorităţile naţionale, cât şi la nivelul parteneriatului public-privat.

15. Atrage atenţia asupra faptului că prostituţia infantilă şi tratamentul violent al copiilor, ca parte a pornografiei infantile pe internet, necesită o abordare distinctă şi cuprinzătoare în ce priveşte combaterea criminalităţii cibernetice şi invită Comisia Europeană să sprijine o cooperare strânsă a agenţiilor europene cu rol în asigurarea securităţii informatice cu Agenţia Europeană pentru Drepturi Fundamentale şi cu alte organisme internaţionale care au ca obiect protecţia copilului; recomandă formarea de expertiză specifică pentru prevenirea şi combaterea infracţiunilor cibernetice în care copiii sunt victime.

16. Remarcă rolul esenţial pe care trebuie să îl joace atât Comisia Europeană cât şi agenţiile de profil ale Uniunii, prin iniţiative concrete de impulsionare a eforturilor în domeniul securităţii cibernetice, cum ar fi: instituirea unor canale fiabile pentru raportarea voluntară a incidentelor cibernetice, crearea unei platforme de formare în materie de securitate cibernetică şi un posibil cadru european de certificare de securitate în domeniul tehnologiei informaţiei şi comunicaţiilor.

17. Atrage atenţia asupra posibilităţii de extindere a criminalităţii favorizate de internet, inclusiv a procurării de arme în scop terorist şi cheamă la acţiune fermă în acest sens, prin însoţirea măsurilor specifice mediului *online* de acţiuni poliţieneşti în teren, prin cooperare între statele membre şi prin măsuri preventive pe plan social şi educativ la nivelul Uniunii.

18. Atrage atenţia că deşi concluziile comunicării sunt fundamentate, acestea sunt totuşi sumare iar utilitatea lor ar fi fost mult sporită dacă ar fi fost însoţite de o propunere de foaie de parcurs sau de o descriere sintetică a domeniilor strategice sectoriale cu care se urmăreşte coordonarea strategiei privind securitatea cibernetică.

19. Atrage atenţia că securitatea cibernetică nu poate fi realizată cu succes doar prin reglementarea legislativă şi efortul instituţiilor publice, implicarea sectorului privat şi dezvoltarea unui dialog public-privat real este esenţială, aceasta având rolul de a viza eliminarea vulnerabilităţilor pe care noile evoluţii tehnologice sau conceptuale le pot crea din perspectiva securităţii cibernetice.

20. Consideră că pentru atingerea unui nivel ridicat al securităţii cibernetice este necesar un parteneriat solid între mediul universitar, structurile guvernamentale şi mediul privat, care să se manifeste în domeniile economic, de securitate şi de apărare.

21. Consideră că este necesară educarea publicului, efort menit să conducă la dezvoltarea unei culturi de securitate în domeniul cibernetic, inclusiv prin implicarea mediului academic şi educaţional, ca şi a mass-mediei şi societăţii civile.

22. Consideră oportună introducerea noţiunilor privind securitatea cibernetică încă din şcoală, de exemplu prin explicarea normelor de securitate şi etică în spaţiul virtual, a conduitei pentru prevenirea infracţiunilor în domeniul cibernetic, în mod special a comportamentului agresiv întâlnit pe reţelele sociale şi nu numai.

23. Consideră că eforturile legislative în statele membre au un rol important în asigurarea securităţii cibernetice, în special prin formarea unei atitudini favorabile pentru măsurile necesare, aşa cum a demonstrat iniţierea de către Comisia pentru afaceri europene din Camera Deputaţilor a demersurilor privind introducerea în programa şcolară a unei *curricule* de securitate cibernetică.

24. Atrage atenţia că atacurile cibernetice coordonate şi sponsorizate de state prezintă tendinţa de a evolua de la utilizarea abuzivă a spaţiului cibernetic în relaţiile interstatale spre acţiuni militare, războiul convenţional şi electronic fiind însoţite din ce în ce mai des de atacuri cibernetice, inclusiv prin integrarea acestora în acţiuni specifice războiului psihologic cum ar fi propaganda, provocările sau dezinformarea.

25. Consideră că este necesară impunerea unor cerinţe minime de securitate pentru protecţia infrastructurilor cibernetice pentru deţinătorul infrastructurii, inclusiv a obligaţiei de a elabora şi pune în aplicare planuri şi politici de securitate, precum şi de a raporta cu titlu anonim incidentele majore.

26. Atrage atenţia asupra riscului prezentat de cunoaşterea incompletă a originii atacurilor cibernetice, a modalităţii prin care acestea se materializează, precum şi a repartiţiei geografice a ţintelor atacurilor cibernetice şi propune derularea unor analize în acest sens.

27. Consideră oportun ca statele membre să dispună de libertatea de a desemna centre specializate din cadrul unei autorităţi publice care să îndeplinească funcţia de echipe de intervenţie în caz de incidente informatice (CSIRT).

28. Apreciază ca utilă partajarea informaţiilor cu autorităţile relevante din statele membre, în conformitate cu legislaţia naţională şi europeană, în contextul abordării interdependenţelor intersectoriale şi a rezilienţei infrastructurii reţelelor publice majore.

29. Ia act de sugestia Comisiei Europene, conform căreia autorităţile naţionale de reglementare ar putea utiliza capacităţile CSIRT pentru a efectua examinări periodice ale infrastructurilor reţelelor publice şi consideră că şi utilizarea centrelor specializate cu rol de CSIRT ar veni în sprijinul autorităţilor naţionale din statele membre.

30. Subliniază necesitatea adaptării continue a legislaţiei existente în domeniu, atât la nivelul Uniunii, cât şi la nivelul statelor membre, în funcţie de evoluţia contextului general de securitate şi a combaterii în mod eficient a ameninţărilor şi vulnerabilităţilor specifice, provenite din spaţiul virtual.

31. Apreciază ca semnificativ, în acest context, exemplul activităţii desfăşurate de instituţiile abilitate în domeniu din România şi susţine importanţa alocată dezvoltării securităţii cibernetice, atât în ceea ce priveşte activitatea la nivel naţional, cât şi în planul cooperării cu instituţiile UE şi din ale statelor membre.

Această hotărâre a fost adoptată de către Camera Deputaţilor în şedinţa din 4 octombrie 2016, cu respectarea prevederilor art. 76 alin. (2) din Constituţia României, republicată.

PREŞEDINTELE

CAMEREI DEPUTAŢILOR

Florin IORDACHE

Bucureşti, 4 octombrie 2016

Nr. 90.