PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

HOTĂRÂRE
privind adoptarea opiniei referitoare la Comunicarea comună către Parlamentul European şi Consiliu - Rezilienţă, prevenire şi apărare: construirea unei securităţi cibernetice puternice pentru UE
JOIN(2017)450

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, aprobat prin Hotărârea Camerei Deputaţilor nr. 8/1994, republicat, cu modificările şi completările ulterioare,

Camera Deputaţilor adoptă prezenta hotărâre.

Articol unic. – Luând în considerare opinia nr. 4c-19/461 adoptată de Comisia pentru afaceri europene, în şedinţa din 15 noiembrie 2017, Camera Deputaţilor:

1. Apreciază şi consideră benefică atitudinea Comisiei şi a celorlalte instituţii europene cu privire la măsurile necesare în domeniul securităţii cibernetice, cu atât mai mult luând în considerare magnitudinea pachetului de măsuri şi a comunicărilor propuse. Consideră că acest ritm trebuie menţinut şi dezvoltat în continuare, inclusiv prin măsuri specifice adoptate la nivel naţional de către statele membre.
2. Susţine poziţia Guvernului României, conform căreia România sprijină pachetul de propuneri în domeniul securităţii cibernetice, pe care îl consideră oportun şi necesar, în condiţiile dinamicii deosebite a ameninţărilor cibernetice şi, mai ales, a consecinţelor pe care astfel de atacuri le pot avea asupra sistemelor informatice, economiilor statelor membre, dar şi asupra stabilităţii sistemelor democratice şi a valorilor europene.
3. Subliniază interesul României privind o implicare activă în instituirea unei reţele de consolidare a capacităţii cibernetice a Uniunii, care să reunească Serviciul European de Acţiune Externă, autorităţile din domeniul cibernetic ale statelor membre, serviciile Comisiei, mediul academic şi societatea civilă, în acord cu strategia globală.
4. Subliniază poziţia României de a sprijini o abordare constructivă în negocierile asupra propunerilor legislative, dar şi în discuţiile vizând punerea în aplicare a celorlalte iniţiative ale Comisiei, dată fiind importanţa acordată de ţara noastră securităţii cibernetice, problematică de interes major la nivel naţional, inclusiv în perspectiva Preşedinţiei române a Consiliului UE, în primul semestru al anului 2019.
5. Reliefează susţinerea României faţă de focalizarea demersurilor comune ale statelor membre pe cele trei dimensiuni – rezilienţă, descurajare şi apărare cibernetică, ca premisă pentru un răspuns eficient şi coordonat la nivel european faţă de ameninţările de această natură.

6. În mod particular, subliniază poziţia Guvernului României, conform căreia interesul României vizează propunerile legate de pregătirea în vederea unei reacţii rapide la atacurile cibernetice, creşterea conştientizării efectelor acestora, dezvoltarea competenţelor, implicit a educaţiei, în domeniul securităţii cibernetice, precum şi susţinerea eforturilor de îmbunătăţire a capabilităţilor în domeniu ale statelor terţe din politica de vecinătate a UE.

7. Evidenţiază eforturile României pentru sporirea nivelului de securitate cibernetică şi prin transpunerea exigenţelor Uniunii Europene în materie de securitate cibernetică, sens în care România a iniţiat transpunerea în plan naţional legislativ a prevederilor Directivei Parlamentului European şi a Consiliului privind măsuri pentru un nivel comun de securitate a reţelelor şi a sistemelor informatice în Uniunea Europeană (Directiva NIS).

8. Sprijină poziţia Guvernului României, conform căreia România susţine importanţa consolidării cooperării cu statele membre şi cu Agenţia Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (ENISA), mai ales în contextul propunerilor de extindere a competenţelor agenţiei, în privinţa conţinutului rapoartelor situaţionale, incluzând cauzele tehnice şi impactul incidentelor de securitate cibernetică, în vederea unei mai bune cooperări tehnice şi operaţionale în situaţii de criză.

9. În ceea ce priveşte partea din regulament referitoare la cadrul de certificare a securităţii cibernetice, subliniază că poziţia României este de susţinere a obiectivului principal de a atesta faptul că produsele şi serviciile în domeniul tehnologiei informaţiilor şi comunicaţiei, care au fost certificate în conformitate cu o astfel de schemă, respectă cerinţele specifice privind securitatea informatică. Consideră, în acest sens, că se impune o analiză aprofundată a măsurilor privind certificarea în domeniul securităţii cibernetice, în strânsă legătură cu actorii pieţei.

10. Apreciază că o atenţie particulară trebuie acordată măsurilor care trebuie adoptate la nivel naţional pentru crearea cadrului legal de identificare a autorităţii naţionale de supraveghere a certificării care să participe în Grupul european pentru certificarea de securitate cibernetică.

11. În ceea ce priveşte pilonul apărării cibernetice din prezenta comunicare, atrage atenţia asupra aspectelor referitoare la controlul exporturilor tehnologiilor critice cibernetice de supraveghere, deoarece acestea ar trebui aduse la cunoştinţa Grupului de lucru pentru produse cu dublă utilizare (WPDU), pentru a evita formulări inexacte în documentul final. Consideră ca posibilă măsură la nivel european incriminarea corespunzătoare a infracţiunilor de orice fel în mediul cibernetic şi introducerea sancţiunilor penale pentru acestea atât în planul UE, cât şi la nivelul statelor membre.

12. Consideră că este necesară abordarea modului în care instrumente cibernetice au putut sau pot influenţa procesele din interiorul unui stat, inclusiv procesele democratice la nivel intern, în cadrul unei comunicări specifice care să includă o evaluare a modalităţilor prin care un actor a putut sau poate face acest lucru.

13. Apreciază iniţiativa unei reforme a Agenţiei Uniunii Europene pentru Securitatea Reţelelor şi a Informaţiilor (ENISA), însă consideră necesară o consultare aprofundată a statelor membre şi instituirea unor mecanisme la nivelul Agenţiei pentru colaborarea cu instituţiile specifice din statele membre, care să cuprindă un cadru mai larg şi care să includă dar să nu se limiteze la un schimb de informaţii permanent.

14. Consideră pozitivă ideea unui schimb de informaţii prin implicarea organismelor şi agenţiilor UE, a statelor membre, precum şi a structurilor însărcinate în acest domeniu ale statelor membre, însă consideră că o abordare cuprinzătoare ar trebui să includă un schimb de informaţii şi expertiză cu mediul privat şi sectorul neguvernamental.

15. Atrage atenţia asupra necesităţii unei abordări prioritare, în continuarea demersurilor efectuate până acum, a verificării şi controlului impactului pe care relaţia Uniunii Europene sau a statelor membre cu actori terţi, deopotrivă în ce priveşte relaţia comercială, îl poate avea asupra infrastructurii critice, inclusiv a celei din domediul cibernetic.

16. Apreciază că ar fi benefică analizarea aprofundată a dovezilor privind implicarea unor anumite state sau a altor actori în procese democratice interne ale unui alt stat, folosindu-se de mediul cibernetic şi de mijloacele puse la dispoziţie de acesta.

17. Recomandă dezvoltarea, la nivel european, a cooperării cu mediul privat activ în domeniu, atât în ceea ce privește marile companii prezente la nivel internațional, cât și întreprinderile mici și mijlocii, cu privire la schimbul de informații și expertiză, precum și privind dezvoltarea și aprofundarea unor mecanisme de control, în mediul cibernetic, a mijloacelor care pot provoca infracțiuni în mediul online, inclusiv cu privire la implicarea unor actori terți în procesele interne ale unor state membre. În același timp, atrage atenția asupra necesității respectării, în toate aceste procese, a drepturilor și libertăților fundamentale și a procedeelor democratice, cu precădere a intimității și vieții private a consumatorilor.

18. Apreciază plus-valoarea pe care Directiva NIS o aduce în planul rezilienței cibernetice la nivel european și susține punerea acesteia în aplicare, însă atrage atenția asupra necesității unor măsuri complementare cu aceasta, care să includă crearea unor legături între statele membre și între acestea și instituțiile europene, cu precădere în ceea ce privește structurile interne sau cele europene abilitate în domeniul securității cibernetice.

19. Ia notă de opțiunea Comisiei Europene privitoare la examinarea posibilității de a lansa un fond de răspuns la situații de urgență legate de securitatea cibernetică și recomandă declanșarea cât mai rapidă a procesului de consultare a statelor membre cu privire la această inițiativă.

20. În continuarea inițiativei Comisiei de creare a unei rețele de centre de competențe în materie de securitate cibernetică și a unui centru european de competențe și de cercetare în materie de securitate cibernetică, recomandă realizarea unei stratificări la nivelul acesteia care să cuprindă rețele aferente mediului public, privat, academic și societății civile.

21. Consideră că investițiile de orice fel în cercetare și dezvoltare de capabilități în domeniul securității cibernetice necesită asigurări și protecții împotriva eventualelor scurgeri de informații sau utilizări ale acestora de către terți în scopuri proprii, inclusiv în ce privește criptarea și recomandă detalierea unor astfel de măsuri în viziunea Comisiei.

22. Susține eforturile Comisiei în ce privește promovarea conștientizării și a „igienei" cibernetice în rândul cetățenilor, sens în care consideră benefică ideea organizării unor cursuri speciale în mediul educațional și a unor campanii de informare și publicitate periodice în spațiul public, dedicate securității cibernetice.

23. Recomandă instituirea unor mijloace prin care să fie studiate în amănunt atacurile cibernetice majore de până acum, ca punct de pornire în adoptarea unei conduite preventive bazate pe lecții învățate și în identificarea și aplicarea unor eventuale soluții pentru combaterea unor astfel de atacuri.

24. Crede că, pentru a putea investiga și identifica soluții privind accesul la „Darknet" (internetul întunecat), o posibilă cale ar putea fi identificarea și cooptarea, după caz, a unor utilizatori care au avut sau au acces la mijloacele „Darknet" și utilizarea experienței acestora ca punct de pornire în investigații.

25. În vederea intensificării răspunsului politic, consideră că ar fi necesară o campanie de conștientizare și, eventual, perfecționare, desfășurată în rândul oamenilor politici din statele membre ale Uniunii Europene, cu privire la securitatea cibernetică și la toate fenomenele adiacente.

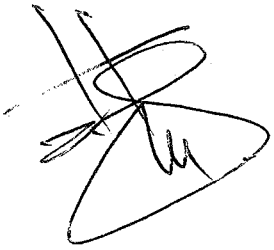
26. Apreciază propunerea Comisiei cu privire la „intensificarea sprijinului financiar pentru proiectele naționale și transnaționale care urmăresc îmbunătățirea justiției penale în spațiul cibernetic", însă atrage atenția asupra necesității unui control al acestor proiecte și al rezultatelor lor, pentru a evita o eventuală obținere de avantaje de către terți implicați în aceste proiecte, avantaje care ar putea fi folosite în detrimentul Uniunii sau al statelor membre și al cetățenilor acestora.

27. Consideră prioritară îmbunătățirea perpetuă a relației dintre UE și NATO în domeniul securității cibernetice și încurajează Comisia să susțină cadrul regional ca mijloc de cooperare între statele membre în acest domeniu.

Această hotărâre a fost adoptată de către Camera Deputaţilor în şedinţa din 21 noiembrie 2017, cu respectarea prevederilor art. 76 alin. (2) din Constituţia României, republicată.

p. PREŞEDINTELE
CAMEREI DEPUTAŢILOR

Petru - Gabriel VLASE



Bucureşti, 21 noiembrie 2017
Nr. 87.

Departamentul legislativ,
Şef departament, Georgică Tobă