Rada
Evropské unie

Brusel 7. října 2019
(OR. en)

12814/19

LIMITE

PE-QE 110

ODPOVĚĎ NA OTÁZKU PARLAMENTU

Odesílatel:	Pracovní skupina pro obecné záležitosti
Příjemce:	Výbor stálých zástupců / Rada
Předmět:	NÁVRH ODPOVĚDI NA OTÁZKU K PÍSEMNÉMU ZODPOVĚZENÍ E-001323/2019 - Dita Charanzová (ALDE) "Útvar EU pro kybernetickou obranu"

1. Delegace naleznou v příloze:

   – znění výše uvedené otázky k písemnému zodpovězení;

   – návrh odpovědi připravený Pracovní skupinou pro obecné záležitosti na zasedání dne 3. října 2019.

2. Tento návrh odpovědi se předkládá ke schválení Výboru stálých zástupců (část I) a Radě.

Otázka k písemnému zodpovězení E-001323/2019
Radě
článek 130 jednacího řádu
Dita Charanzová (ALDE)

Předmět: Útvar EU pro kybernetickou obranu

Vedení války kybernetickými prostředky v podobě dezinformačních kampaní, průmyslové špionáže a útoků na životně důležitou infrastrukturu nabývá na intenzitě s tím, jak je čím dál více zařízení a systémů připojených k internetu.

Všechny členské státy přijaly na vnitrostátní úrovni strategie pro boj s tímto nebezpečím, avšak útoky mají často přeshraniční povahu a míří na cíle v několika zemích.

Jakou činnost Rada vyvíjí, aby tato vnitrostátní obranná opatření koordinovala s cílem posílit jejich účinnost a zajistit, aby v ochraně EU nezůstávaly mezery?

Jaké nástroje jsou k dispozici k tomu, aby pomohly členskému státu nebo v něm usazeným společnostem v případě útoku, včetně protiopatření sdílených s dalšími členskými státy, a aby se vyměňovaly informace o možné hrozbě?

Když odhlédneme od Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), podporuje Rada vytvoření útvaru EU pro kybernetickou obranu v rámci společné bezpečnostní a obranné politiky (SBOP) či jiná mezivládní opatření?

CS
Č. E-001323/2019
Odpověď

Závěry o kybernetické diplomacii přijaté Radou dne 11. února 2015 daly EU a jejím členským státům ambiciózní mandát k prosazování svobody, bezpečnosti a prosperity v kyberprostoru: to zahrnuje mimo jiné prosazování a ochranu lidských práv, uplatňování mezinárodního práva a norem odpovědného chování státu, správu internetu, boj proti kyberkriminalitě, ochranu sítí a systémů vlády a kritické infrastruktury, mezinárodní spolupráci, budování kapacit, konkurenceschopnost na digitálním trhu, strategickou spolupráci s klíčovými partnery.

Dne 20. listopadu 2017 zdůraznila Rada potřebu řešit kybernetickou bezpečnost soudržným způsobem na vnitrostátní, unijní i celosvětové úrovni[1]. Tato výzva znovu zazněla v závěrech Rady a členských států ze dne 19. února 2019[2]. Dále Rada dne 26. června 2018 přijala závěry o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[3], v nichž vyzvala EU a její členské státy, aby společně pracovaly na rozvoji evropské spolupráce v případě kybernetické bezpečnostní krize. Na základě této spolupráce by byla zavedena praktická operacionalizace a dokumentace všech příslušných aktérů, procesů a postupů v rámci stávajících mechanismů EU pro řešení krizí, zejména opatření pro integrovanou politickou reakci na krize.

Unie již učinila významné kroky směrem k zajištění kybernetické bezpečnosti, když například dne 6. července 2016 přijala směrnici Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[4]. Tato směrnice stanoví vytvoření sítě bezpečnostních týmů typu CSIRT (Computer Security Incident Response Team), v jejímž rámci mohou její členové spolupracovat, vyměňovat si informace a budovat vzájemnou důvěru. Členové sítě tak budou mít možnost zlepšit řešení přeshraničních incidentů, a dokonce projednat způsob koordinované reakce v případě konkrétních incidentů.

1 Dokument 14435/17.
2 Dokument 6573/1/19 REV 1.
3 Dokument 10086/18.
4 Úř. věst. L 194, 19.7.2016, s. 1.

Nedávno také Rada přijala nařízení známé jako akt EU o kybernetické bezpečnosti[5], jímž se posiluje mandát Agentury Evropské unie pro kybernetickou bezpečnost (ENISA). Tento obnovený a trvalý mandát umožní agentuře ENISA hrát významnou úlohu při zlepšování odolnosti EU vůči kybernetickým útokům, zejména budováním kapacit, ale také výměnou informací a poskytováním analýz.

Agentura ENISA bude navíc na žádost jednoho nebo více členských států pomáhat členským státům při posuzování incidentů s významným dopadem, a to poskytováním odborných znalostí a usnadňováním technického řešení takových incidentů. Může také poskytovat podporu ve vztahu k následným technickým řešením incidentů. Agentura ENISA navíc funguje jako sekretariát sítě týmů CSIRT.

Kybernetické útoky často vykazují vnější rozměr a Rada v této souvislosti odkazuje na své závěry ze dne 19. června 2017 o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“). Soubor nástrojů pro diplomacii v oblasti kybernetiky stanoví opatření zahrnující i omezující opatření, která je možné použít v rámci prevence nepřátelské činnosti v kyberprostoru a reakce na ni. Evropská rada ve svých závěrech ze dne 28. června 2018 požádala orgány i členské státy, aby zavedly opatření uvedená ve společném sdělení o zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb[6], včetně práce na určování původců kybernetických útoků a praktického využívání souboru nástrojů pro diplomacii v oblasti kybernetiky[7].

---

5 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (Úř. věst. L 151, 7.6.2019, s. 15).

6 Dokument JOIN(2018) 16 final.

7 Dokument EUCO 9/18.

Dne 18. října 2018 přijala Evropská rada závěry, ve kterých vyzvala k tomu, aby se pokročilo v práci věnované schopnosti odrazovat od kybernetických útoků a reagovat na ně prostřednictvím omezujících opatření EU[8]. V návaznosti na to přijala Rada dne 17. května 2019 potřebné právní akty, jimiž se stanoví rámec[9] pro cílená omezující opatření pro odrazování od kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, a pro reakci na ně. Tam, kde je to považováno za nezbytné k dosažení cílů SZBP uvedených v příslušných ustanoveních článku 21 Smlouvy o Evropské unii, tyto akty umožňují, aby byla omezující opatření použita v rámci reakce na kybernetické útoky s významným dopadem na třetí země nebo mezinárodní organizace.

---

8 Dokument EUCO 13/18.

9 Nařízení Rady (EU) 2019/796 (Úř. věst. L 129I, 17.5.2019, s. 1) a rozhodnutí Rady (SZBP) 2019/797 (Úř. věst. L 129I, 17.5.2019, s. 13) ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy.