Středa, 13. června 2018

P8_TA(2018)0258

Kybernetická obrana

Usnesení Evropského parlamentu ze dne 13. června 2018 o kybernetické obraně (2018/2004(INI))

(2020/C 28/06)

Evropský parlament,

— s ohledem na Smlouvu o Evropské unii (SEU) a Smlouvu o fungování Evropské unie (SFEU),

— s ohledem na dokument nazvaný „Sdílená vize, společný postup: silnější Evropa – globální strategie pro zahraniční a bezpečnostní politiku Evropské unie“, který dne 28. června 2016 představila místopředsedkyně Komise, vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku,

— s ohledem na závěry Rady ze dne 20. prosince 2013, 26. června 2015, 15. prosince 2016, 9. března 2017, 22. června 2017, 20. listopadu 2017 a 15. prosince 2017,

— s ohledem na sdělení Komise ze dne 7. června 2017 nazvané „Diskusní dokument o budoucnosti evropské obrany“ (COM(2017)0315),

— s ohledem na sdělení Komise ze dne 7. června 2017 nazvané „Vznik Evropského obranného fondu“ (COM(2017)0295),

— s ohledem na sdělení Komise ze dne 30. listopadu 2016 o Evropském obranném akčním plánu (COM(2016)0950),

— s ohledem na společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 7. února 2013 nazvané „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“ (JOIN(2013)0001), které bylo předloženo Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů,

— s ohledem na pracovní dokument útvarů Komise ze dne 13. září 2017 s názvem „Posouzení strategie EU v oblasti kybernetické bezpečnosti za rok 2013“ (SWD(2017)0295),

— s ohledem na politický rámec EU pro kybernetickou obranu ze dne 18. listopadu 2014,

— s ohledem na závěry Rady ze dne 10. února 2015 o diplomacii v oblasti kybernetiky,

— s ohledem na závěry Rady ze dne 19. června 2017 o rámci pro společnou diplomatickou reakci EU na nepřátelskou činnost v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“),

— s ohledem na společné prohlášení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 13. září 2017 Evropskému parlamentu a Radě s názvem „Odolnost, odrazující opatření a obrana: budování silné kybernetické bezpečnosti pro EU“ (JOIN(2017)0450),

Středa, 13. června 2018

— s ohledem na „Tallinnskou příručku 2.0 o mezinárodním právu platném pro kybernetické operace“ (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) ([1]),

— s ohledem na směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii ([2]),

— s ohledem na činnost Globální komise pro stabilitu kybernetického prostoru,

— s ohledem na sdělení Komise ze dne 28. dubna 2015 nazvané „Evropský program pro bezpečnost“ (COM(2015)0185),

— s ohledem na společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 6. dubna 2016 s názvem „Společný rámec pro boj proti hybridním hrozbám – Reakce Evropské unie“ (JOIN(2016)0018) adresované Evropskému parlamentu a Radě,

— s ohledem na své usnesení ze dne 3. října 2017 o boji proti kyberkriminalitě ([3]),

— s ohledem na společné prohlášení předsedy Evropské rady, předsedy Komise a generálního tajemníka Severoatlantické aliance (NATO) ze dne 8. července 2016, na společné soubory návrhů na uplatňování společného prohlášení schválené Radou EU a Severoatlantickou radou dne 6. prosince 2016 a 5. prosince 2017 a na zprávy o pokroku při jejich provádění přijaté dne 14. června, resp. 5. prosince 2017,

— s ohledem na své usnesení ze dne 22. listopadu 2012 o kybernetické bezpečnosti a ochraně ([4]),

— s ohledem na své usnesení ze dne 22. listopadu 2016 o evropské obranné unii ([5]),

— s ohledem na návrh nařízení Evropského parlamentu a Rady ze dne 13. září 2017 o agentuře ENISA, „Agentuře EU pro kybernetickou bezpečnost“, zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“), který předložila Komise (COM(2017)0477),

— s ohledem na své usnesení ze dne 13. prosince 2017 o výroční zprávě o provádění společné zahraniční a bezpečnostní politiky (SZBP) ([6]),

— s ohledem na své usnesení ze dne 13. prosince 2017 o výroční zprávě o provádění společné bezpečnostní a obranné politiky (SBOP) ([7]),

— s ohledem na článek 52 jednacího řádu,

— s ohledem na zprávu Výboru pro zahraniční věci (A8-0189/2018),

A. vzhledem k tomu, že kybernetické a hybridní výzvy, hrozby a útoky představují největší hrozbu pro bezpečnost, obranu, stabilitu a konkurenceschopnost EU, její členské státy a občany; vzhledem k tomu, že je jasné, že součástí kybernetické obrany je jak vojenský, tak civilní rozměr;

([1]) Cambridge University Press, únor 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) Úř. věst. L 194, 19.7.2016, s. 1.
([3]) Přijaté texty, P8_TA(2017)0366.
([4]) Úř. věst. C 419, 16.12.2015, s. 145.
([5]) Přijaté texty, P8_TA(2016)0435.
([6]) Přijaté texty, P8_TA(2017)0493.
([7]) Přijaté texty, P8_TA(2017)0492.

B. vzhledem k tomu, že EU a její členské státy čelí dříve neznámé hrozbě v podobě politicky motivovaných a státem financovaných kybernetických útoků, jakož i kybernetické trestné činnosti a terorismu;

C. vzhledem k tomu, že armáda všeobecně uznává kybernetický prostor jako pátý operační okruh, který umožňuje rozvoj schopností v oblasti kybernetické bezpečnosti; vzhledem k tomu, že se diskutuje o tom, zda kybernetický prostor uznat jako pátý válečný okruh;

D. vzhledem k tomu, že v ustanovení o vzájemné obraně v čl. 42 odst. 7 SEU je stanoveno, že v případě, že dojde k ozbrojenému napadení na území určitého členského státu, mají členské státy EU vzájemnou povinnost poskytnout pomoc a podporu všemi prostředky, které jsou v jejich moci; vzhledem k tomu, že tím není dotčena zvláštní povaha bezpečnostní a obranné politiky některých členských států; vzhledem k tomu, že doložka o solidaritě v článku 222 SFEU doplňuje ustanovení o vzájemné obraně tím, že je v ní stanoveno, že členské státy EU jsou povinny jednat společně, pokud je některý členský stát EU cílem teroristického útoku nebo obětí přírodní nebo člověkem způsobené pohromy; vzhledem k tomu, že doložka o solidaritě znamená využití jak civilních, tak vojenských struktur;

E. vzhledem k tomu, že zatímco kybernetická obrana je i nadále především v kompetenci členských států, hraje EU zásadní úlohu při poskytování platformy pro evropskou spolupráci a zajišťování úzké koordinace těchto nových snah na mezinárodní úrovni i v rámci transatlantického bezpečnostního uskupení od samého počátku, aby se zabránilo neefektivnosti, kterou se vyznačuje celá řada tradičních opatření v oblasti obrany; vzhledem k tomu, že musíme učinit více, než jen prohloubit naši spolupráci a koordinaci; vzhledem k tomu, že musíme zajistit účinnou prevenci tím, že rozšíříme schopnosti EU odhalovat kybernetické útoky, bránit se jim a odrazovat od nich; vzhledem k tomu, že aby bylo v EU dosaženo účinné kybernetické bezpečnosti a zajištěno, aby byly členské státy vybaveny alespoň k tomu, aby se nestaly snadným cílem kybernetických útoků, je nutné vytvořit důvěryhodnou kybernetickou obranu a systém odrazování, a dále vzhledem k tomu, že nezbytnou součástí společné bezpečnostní a obranné politiky a vytvoření evropské obranné unie by měly být rozsáhlé kapacity v oblasti kybernetické obrany; vzhledem k tomu, že čelíme stálému nedostatku vysoce kvalifikovaných odborníků na kybernetickou obranu; vzhledem k tomu, že nezbytnou součástí vytvoření účinné SBOP je úzká koordinace v souvislosti s ochranou ozbrojených sil vůči kybernetickým útokům;

F. vzhledem k tomu, že členské státy EU jsou často předmětem kybernetických útoků ze strany nepřátelských a nebezpečných státních i nestátních subjektů na civilní nebo vojenské cíle; vzhledem k tomu, že stávající ohrožení je především výsledkem roztříštěné strategie a kapacit EU v oblasti obrany, což cizím zpravodajským agenturám opakovaně umožňuje využívat bezpečnostních slabin systémů a sítí IT, které mají pro evropskou bezpečnost zásadní význam; vzhledem k tomu, že se vládám členských států se často nedaří informovat příslušné zúčastněné strany včas, aby jim umožnily odstranit slabé stránky jejich výrobků a služeb; vzhledem k tomu, že tyto útoky vyžadují urychlené posílení obrany a rozvoj evropských ofenzivních i defenzivních kapacit v civilní a vojenské oblasti, aby bylo možné zabránit případnému přeshraničnímu dopadu kybernetických incidentů na hospodářství a společnost;

G. vzhledem k tomu, že se hranice mezi civilním a vojenským vměšováním v kybernetickém prostoru rozostřují;

H. vzhledem k tomu, že k řadě kybernetických útoků dochází z důvodu nedostatečné odolnosti a robustnosti soukromé a veřejné síťové infrastruktury, nedostatečně chráněných či zabezpečených databází a dalších nedostatků v důležité informační infrastruktuře; vzhledem k tomu, že pouze malý počet členských států považuje ochranu své sítě a informačních systémů a souvisejících údajů za součást své povinnosti náležité péče, což vysvětluje nedostatek investic do odborné přípravy, nejmodernějších zabezpečovacích technologií a vydávání vhodných pokynů;

I. vzhledem k tomu, že právo na soukromí a ochranu údajů je stanoveno v Listině základních práv EU a článku 16 SFEU a upraveno obecným nařízením EU o ochraně osobních údajů, které vstoupilo v platnost 25. května 2018;

J. vzhledem k tomu, že o aktivní a účinné kybernetické politice lze hovořit, pokud umožňuje odrazovat nepřátele a narušovat kapacity, přičemž předchází útoku a snižuje schopnost zaútočit;

K. vzhledem k tomu, že řada teroristických skupin a organizací využívá kybernetický prostor jako levný nástroj sloužící k náboru členů, radikalizaci a šíření teroristické propagandy; vzhledem k tomu, že teroristické skupiny, nestátní subjekty a nadnárodní zločinecké sítě využívají kybernetické operace k anonymnímu získávání finančních prostředků, shromažďování informací a vývoji kybernetických zbraní za účelem vedení kybernetických teroristických kampaní, k narušování, poškozování nebo ničení důležité infrastruktury, k útokům na finanční systémy a k provozování další nelegální činnosti, což má významný dopad na bezpečnost evropských občanů;

L. vzhledem k tomu, že v rámci diskuzí o modernizaci obrany, společných evropských obranných snahách, budoucím rozvoji ozbrojených sil a jejich operací a o zlepšení strategické autonomie Evropské unie je jednou ze zásadních otázek odrazování a kybernetická obrana evropských ozbrojených sil a životně důležité infrastruktury;

M. vzhledem k tomu, že zatímco některé členské státy investovaly značné prostředky do vytvoření řádně personálně zajištěných velitelství pro kybernetickou obranu, která mají řešit tyto nové výzvy a zlepšit svou kybernetickou odolnost, zbývá ještě mnoho práce, neboť je stále obtížnější čelit kybernetickým útokům na úrovni členských států; vzhledem k tomu, že velitelství členských států pro kybernetickou obranu se od sebe liší, pokud jde o ofenzivní a defenzivní mandát; vzhledem k tomu, že struktura kybernetické obrany je stále roztříštěná a v jednotlivých členských státech se značně liší; vzhledem k tomu, že odrazování a kybernetická obrana představuje činnost, kterou lze nejlépe vyvíjet ve spolupráci na evropské úrovni a s našimi partnery a spojenci, jelikož její operační okruh nezná ani státní, ani organizační hranice; vzhledem k tomu, že vojenská a civilní kybernetická bezpečnost je úzce propojena, a že je proto nutné zajistit větší součinnost mezi civilními a vojenskými odborníky; vzhledem k tomu, že soukromé společnosti mají v dané oblasti velké množství odborných zkušeností, což vede ke vzniku základních otázek ohledně správy a bezpečnosti a schopnosti států bránit své občany;

N. vzhledem k tomu, že z důvodu nedostatečné včasné reakce na měnící se prostředí kybernetické bezpečnosti je naléhavě nutné rozšířit schopnosti v oblasti kybernetické obrany; vzhledem k tomu, že klíčovými prvky při zajišťování bezpečnosti v této oblasti je rychlá reakce a odpovídající připravenost;

O. vzhledem k tomu, že stálá strukturovaná spolupráce (PESCO) a Evropský obranný fond (EDF) jsou nové iniciativy, jejichž prostřednictvím by bylo možné podpořit ekosystém, který může zajistit příležitosti pro malé a střední podniky a začínající podniky, podporovat společné projekty v oblasti kybernetické obrany a přispět k vytváření regulačního a institucionálního rámce;

P. vzhledem k tomu, že se členské státy účastnící se stálé strukturované spolupráce zavázaly k tomu, že zajistí, aby došlo k rozšíření spolupráce v oblasti kybernetické obrany, jako je výměna informací, odborná příprava a operační podpora;

Q. vzhledem k tomu, že ze sedmnácti projektů vybraných jako projekty stálé strukturované spolupráce se dva týkají oblasti kybernetické obrany;

R. vzhledem k tomu, že Evropský obranný fond musí podpořit globální konkurenceschopnost a inovativnost evropského obranného průmyslu tím, že bude investovat do digitálních a kybernetických technologií a nabídne malým a středním podnikům a začínajícím podnikům příležitost se také zapojit s cílem usnadnit rozvoj inteligentních řešení;

S. vzhledem k tomu, že s cílem zajistit potřeby členských států týkající se rozšiřování jejich kapacit v oblasti kybernetické obrany zahájila Evropská obranná agentura (EDA) řadu projektů, mj. v oblasti vzdělávání a odborné přípravy, jako je platforma pro koordinaci odborné přípravy a výcviku v oblasti kybernetické obrany (CD TEXP), sdružování žádostí o podporu odborné přípravy a výcviku v oblasti kybernetické obrany ze strany soukromého sektoru (DePoCyTE) a projekt v oblasti kybernetických polygonů;

T. vzhledem k tomu, že probíhají další projekty EU v oblasti informovanosti o dané situaci, odhalování škodlivého softwaru a výměny informací (platforma Malware Information Sharing Platform (MISP) a systém Multi-Agent System For Advanced persistent threat Detection (MASFAD));

U. vzhledem ke značné potřebě budování kapacit a odborné přípravy v oblasti kybernetické obrany, která dále roste, a vzhledem k tomu, že ji lze neúčinněji zajistit ve spolupráci v rámci EU a NATO;

V. vzhledem k tomu, že mise a operace SBOP jsou stejně jako všechny moderní organizace velmi závislé na fungujících systémech IT; vzhledem k tomu, že kybernetické hrozby ohrožující mise a operace SBOP mohou existovat na různých rovinách, které sahají od taktické roviny (mise a operace SBOP) přes provozní rovinu (sítě EU) až k obecnější globální rovině, jejíž součástí je infrastruktura IT;

W. vzhledem k tomu, že velitelské a kontrolní systémy, výměna informací a logistika spoléhají na utajovanou i neutajovanou infrastrukturu v oblasti IT, zejména pokud jde o taktickou a operační úroveň; vzhledem k tomu, že tyto systémy představují přitažlivý cíl pro nepřátelské subjekty, které se snaží útočit na mise; vzhledem k tomu, že kybernetické útoky mohou mít citelný dopad na infrastrukturu v Evropské unii; vzhledem k tomu, že kybernetické útoky zejména na energetickou infrastrukturu Evropské unie by mohly mít závažné důsledky, a proto je nutné ji obzvláště chránit;

X. vzhledem k tomu, že kybernetická obrana je samozřejmě důležitým faktorem ve všech fázích plánování mísí a operací SBOP a je třeba ji neustále sledovat, a vzhledem k tomu, že aby ji bylo možné plně začlenit do plánování misí a zajistit jí nepřetržitou životně důležitou podporu, je nutné vytvořit příslušné kapacity;

Y. vzhledem k tomu, že síť Evropské bezpečnostní a obranné školy (EBOŠ) je jediným evropským zařízením, které zajišťuje odborné vzdělávání pro struktury, mise a operace SBOP; vzhledem k tomu, že v současné době se v kybernetické oblasti plánuje podstatné rozšíření její úlohy při sjednocování evropských vzdělávacích kapacit;

Z. vzhledem k tomu, že Varšavská deklarace ze summitu NATO konaného v roce 2016 uznala kyberprostor jako operační okruh, ve kterém se musí NATO bránit tak účinně, jako se brání ve vzduchu, na zemi a na moři;

AA. vzhledem k tomu, že EU a NATO přispívají k rozšíření kapacit členských států v oblasti kybernetické obrany, a to prostřednictvím výzkumu v oblasti technologií dvojího užití a projektů koordinovaných Evropskou obrannou agenturou (EDA) a NATO, a ke zlepšení kybernetické odolnosti členských států pomocí podpory poskytované Agenturou Evropské unie pro bezpečnost sítí a informací (ENISA);

AB. vzhledem k tomu, že NATO v roce 2014 učinila kybernetickou bezpečnost součástí své kolektivní obrany a v roce 2016 uznala kybernetický prostor za operační oblast vedle země, vzduchu a moře; vzhledem k tomu, že EU a NATO jsou partnery, kteří se při budování své kybernetické odolnosti doplňují; vzhledem k tomu, že kybernetická bezpečnost a obrana je již jedním z nejsilnějších pilířů spolupráce mezi těmito dvěma subjekty a rozhodující oblastí, ve které mají oba jedinečné kapacity; vzhledem k tomu, že se EU a NATO ve svém společném prohlášení ze dne 8. července 2016 dohodly na širokém programu spolupráce; vzhledem k tomu, že čtyři ze čtyřiceti dvou návrhů užší spolupráce se týkají kybernetické bezpečnosti a obrany, přičemž další návrhy se zaměřují obecněji na hybridní hrozby; vzhledem k tomu, že tyto návrhy doplňuje další návrh týkající se kybernetické bezpečnosti a obrany, který byl předložen dne 5. prosince 2017;

AC. vzhledem k tomu, že skupina vládních odborníků na oblast informační bezpečnosti fungující při OSN (UNGGE) uzavřela poslední kolo jednání; vzhledem k tomu, že ačkoli tentokrát nebyla schopna dospět ke konsenzu ohledně zprávy, zůstávají v platnosti dohody z roku 2017, 2015 a 2013, včetně toho, že pro oblast zachování míru a stability a prosazování otevřeného, bezpečného, mírumilovného a přístupného prostředí IKT platí stávající mezinárodní právo, zejména Charta OSN, která má v tomto ohledu zásadní význam;

AD. vzhledem k tomu, že nedávno vytvořený rámec pro společnou diplomatickou reakci EU na nepřátelskou kybernetickou činnost – soubor nástrojů pro diplomacii v oblasti kybernetiky –, jehož cílem je vybudovat kapacity EU a členských států, tak aby bylo možné ovlivňovat chování potenciálních agresorů, předpokládá používání přiměřených opatření v rámci SZBP, včetně restriktivních opatření;

AE. vzhledem k tomu, že do nepřátelské činnosti za účelem dosažení politických, ekonomických nebo bezpečnostních cílů, mezi něž patří útoky na životně důležitou infrastrukturu, kybernetická špionáž, hromadné sledování občanů EU, dezinformační kampaně, šíření škodlivého softwaru (Wanncry a NotPetya apod.) a omezování přístupu k internetu a fungování systémů IT, jsou zapojeny nejrůznější státy – Rusko, Čína a Severní Korea, ale také nestátní aktéři (včetně organizovaných zločineckých skupin), které ponoukají k činnosti, najímají nebo sponzorují státy, bezpečnostní agentury či soukromé společnosti; vzhledem k tomu, že tato činnost představuje nedodržování a porušování mezinárodního práva, lidských práv a základních práv EU a ohrožuje demokracii, bezpečnost, veřejný pořádek a strategickou autonomii, a měla by proto vést ke společné reakci EU, jako je uplatňování rámce pro společnou diplomatickou reakci EU, včetně restriktivních opatření, které jsou součástí souboru nástrojů pro diplomacii v oblasti kybernetiky, jako jsou např. pokuty a omezení přístupu na vnitřní trh v případě soukromých společností;

AF. vzhledem k tomu, že k takovým rozsáhlým útokům proti IKT došlo v minulosti několikrát, mimo jiné vůči Estonsku v roce 2007, Gruzii v roce 2008 a v současnosti se používají téměř denně vůči Ukrajině; vzhledem k tomu, že ofenzivní kapacity v kybernetické oblasti se v nebývalé míře používají také vůči členským státům EU a NATO;

AG. vzhledem k tomu, že v případě technologií pro kybernetickou bezpečnost, které jsou důležité jak pro vojenskou, tak i civilní oblast, se jedná o tzv. technologie dvojího užití, které nabízejí mnoho příležitostí k vytvoření součinnosti mezi civilními a vojenskými subjekty v řadě oblastí, jako jsou nástroje v oblasti šifrování, bezpečnosti a řízení zranitelnosti a systémy detekce případů narušování a jejich prevence;

AH. vzhledem k tomu, že vývoj kybernetických technologií během příštích let bude mít dopad na nové oblasti, jako je umělá inteligence, internet věcí, robotika a mobilní zařízení, a všechny tyto prvky by mohly mít také různé důsledky z hlediska bezpečnosti v oblasti obrany;

AI. vzhledem k tomu, že velení v oblasti kybernetické obrany zřízené některými členskými státy může významně přispět k ochraně životně důležité civilní infrastruktury, a dále vzhledem k tomu, že znalosti týkající se kybernetické obrany jsou často stejně užitečné v civilní oblasti;

Budování kapacit k zajištění kybernetické obrany a odrazování

1. zdůrazňuje, že jedním ze základních prvků rozvoje evropské obranné unie by měla být společná politika a rozsáhlé kapacity v oblasti kybernetické obrany;

2. vítá iniciativu Evropské komise týkající se balíčku opatření v oblasti kybernetické bezpečnosti na podporu kybernetické odolnosti, odrazování a obrany EU;

3. připomíná, že kybernetická obrana má vojenský i civilní rozměr, a vyžaduje proto vytvoření integrovaného politického přístupu a úzkou spolupráci mezi vojenskými a civilními zúčastněnými stranami;

4. vyzývá k důslednému rozvoji kybernetických kapacit ve všech orgánech a institucích EU a také v členských státech a k vytvoření nezbytných politických a praktických řešení k překonání zbývajících politických, legislativních a organizačních překážek, které brání spolupráci v oblasti kybernetické obrany; považuje pravidelnou širší výměnu informací a prohloubenou spolupráci mezi příslušnými veřejnými subjekty v oblasti kybernetické obrany na úrovni EU i členských států za zásadní;

5. důrazně poukazuje na to, že k zajištění maximální účinnosti je od samého počátku nutné zapojit do nově vznikající evropské obranné unie v co nejširším rozsahu kapacity členských států v oblasti kybernetické obrany; proto členské státy naléhavě vybízí, aby v zájmu většího zefektivnění struktur v oblasti kybernetické obrany ve všech členských státech, neodkladného uplatňování dostupných krátkodobých opatření a prosazování výměny odborných zkušeností zajistily na základě jasného plánu úzkou spolupráci při budování svých příslušných velitelství pro oblast kybernetické obrany, čímž by přispěly k procesu koordinovanému Komisí, Evropskou službou pro vnější činnost (ESVČ) a Evropskou obrannou agenturou; domnívá se, že bychom měli vytvořit evropskou bezpečnou síť pro důležité informace a infrastrukturu; je si vědom toho, že jedním ze základních prvků účinné kybernetické obrany a odrazování je rozsáhlá schopnost připisovat kybernetické útoky jejich původci a že má-li být dosaženo účinné prevence, je nutné získat další významné technické zkušenosti; naléhavě vyzývá členské státy, aby s cílem zlepšit připisování kybernetických útoků pachatelům navýšily finanční a lidské zdroje, zejména odborníky z oblasti počítačové forenzní vědy; zdůrazňuje, že taková spolupráce by měla být zavedena také na základě rozšíření činnosti Agentury Evropské unie pro bezpečnost sítí a informací (ENISA);

6. je si vědom toho, že řada členských států se domnívá, že hlavní součástí jejich státní bezpečnostní strategie a nezbytnou součástí jejich státní suverenity je existence jejich vlastních kapacit v oblasti kybernetické obrany; zdůrazňuje však, že vzhledem k přeshraniční povaze kybernetického prostoru je rozsah a znalosti nutné k zajištění skutečně komplexních a účinných sil zaručujících dosažení strategické autonomie EU v kybernetickém prostoru mimo možnosti kteréhokoli členského státu jednajícího samostatně, a že je proto nutné ze strany všech členských států zajistit intenzivní koordinovanou reakci na úrovni EU; konstatuje v této souvislosti, že EU a její členské státy se nacházejí pod časovým tlakem, pokud jde o vytvoření takových sil, a musejí jednat okamžitě; podotýká, že z důvodu iniciativ EU, jako je jednotný digitální trh, má EU vhodné postavení pro to, aby se ujala vedoucí úlohy při rozvoji evropských strategií v oblasti kybernetické obrany; připomíná, že při rozvoji kybernetické obrany na evropské úrovni musí být podporována schopnost Unie bránit se; vítá v tomto ohledu navrhovaný trvalý mandát a posílenou úlohu agentury ENISA;

7. v této souvislosti naléhavě vybízí členské státy, aby při navrhování projektů spolupráce co nejlépe využily rámec, který jim poskytuje stálá strukturovaná spolupráce a Evropský obranný fond;

8. bere na vědomí intenzivní práci EU a jejích členských států v oblasti kybernetické obrany; bere na vědomí zejména projekty Evropské obranné agentury v oblasti kybernetických polygonů, program strategického výzkumu v oblasti kybernetické obrany a vypracovávání balíčků v oblasti informovanosti o dané kybernetické situaci, které by mohlo využívat velení;

9. vítá oba kybernetické projekty, které mají být zahájeny v rámci stálé strukturované spolupráce, totiž platformu pro výměnu informací v případě kybernetických incidentů a týmy rychlé kybernetické reakce a vzájemné pomoci v oblasti kybernetické bezpečnosti; zdůrazňuje, že tyto dva projekty se zaměřují na defenzivní kybernetickou politiku, jejímž cílem je vyměňovat si informace o kybernetických hrozbách pomocí propojené platformy členských států a týmů rychlé kybernetické reakce, které členským státům umožní navzájem si pomáhat, a zajistit tak vyšší úroveň kybernetické odolnosti a společně odhalovat, rozpoznávat a zmírňovat kybernetické hrozby; vyzývá Komisi a členské státy, aby navázaly na projekt PESCO pro vnitrostátní týmy rychlé kybernetické reakce a vzájemné pomoci v oblasti kybernetické bezpečnosti tím, že zřídí evropský tým rychlé kybernetické reakce, který by koordinoval a odhaloval společné kybernetické hrozby a bojovat proti nim a podpořil tak snahy zúčastněných členských států;

10. konstatuje, že schopnosti Unie v oblasti rozvoje projektů kybernetické obrany závisejí na dovedném ovládání technologií, zařízení, služeb a údajů i na zpracování údajů a že tyto schopnosti vyžadují možnost opřít se o vzájemnou důvěru průmyslových subjektů;

11. připomíná, že jedním z cílů v rámci úsilí vynaloženého na zajištění větší jednotnosti systémů velení je zajistit prostředky velení, které by byly interoperabilní se zeměmi Severoatlantické aliance, které nejsou členy EU, a s příležitostnými partnery, zajistit plynulou výměnu informací vedoucí k urychlení rozhodovacího procesu a zachovat kontrolu nad informacemi v souvislosti s kybernetickými riziky;

12. doporučuje, aby se našel způsob, jak doplnit projekty NATO v oblasti inteligentní obrany (např. nadnárodní budování kapacit v oblasti kybernetické obrany, platformu Malware Information Sharing Platform (MISP) a nadnárodního vzdělávání a odborné přípravy v oblasti kybernetické obrany (MNCDE&T));

13. uznává nový vývoj v oblastech, jako jsou nanotechnologie, umělá inteligence, data velkého objemu, odpadní elektrická a elektronická zařízení a vyspělá robotika; naléhavě žádá členské státy a EU, aby věnovaly zvláštní pozornost možnému zneužití těchto oblastí ze strany nepřátelských států a organizovaných zločineckých skupin; vyzývá k vytvoření odborné přípravy a rozvoji kapacit za účelem ochrany před vznikem sofistikovaných systémů trestné činnosti, jako jsou složité podvody založené na zneužití totožnosti a případy padělání zboží;

14. zdůrazňuje, že s cílem bojovat proti kybernetickým a hybridním hrozbám, odhalovat a odstraňovat extremistické a zločinecké ráje na internetu pomocí rozšíření a větší výměny informací mezi EU a jejími agenturami, jako jsou Europol, Eurojust, EDA a ENISA, je nezbytné upřesnit terminologii týkající se bezpečnosti v kybernetickém prostoru, zaujmout všeobecný jednotný přístup a vyvinout společné úsilí;

15. poukazuje na rostoucí úlohu umělé inteligence v oblasti kybernetické ofenzivy i defenzivy; naléhavě vyzývá EU a členské státy, aby této oblasti věnovaly zvláštní pozornost jak v rámci výzkumu, tak při praktickém rozvoji svých kapacit v oblasti kybernetické obrany;

16. klade zvláštní důraz na to, že se zavedením bezpilotních vzdušných prostředků, ať už ozbrojených nebo ne, by měla být přijata dodatečná opatření za účelem omezení jejich možných slabých stránek v kybernetické oblasti;

Kybernetická obrana misí a operací v rámci SBOP

17. zdůrazňuje, že kybernetická obrana by se měla považovat za operační úkol v rámci misí a operací SBOP a že by měla být začleněna do veškerého plánování v rámci této politiky, aby bylo zajištěno neustálé zohledňování kybernetické bezpečnosti během plánování, čímž by se omezily nedostatky v kybernetické oblasti;

18. je si vědom toho, že plánování úspěšné mise nebo operace v oblasti SBOP vyžaduje značné odborné zkušenosti v oblasti kybernetické obrany a zabezpečenou infrastrukturu a sítě IT, a to jak na úrovni operačního velení, tak i v rámci samotné mise, aby bylo možné hrozbu důkladně posoudit a poskytnout příslušnou ochranu v terénu; vyzývá ESVČ a členské státy zajišťující velení operací v rámci SBOP, aby prohloubily své odborné zkušenosti v oblasti kybernetické obrany pro mise a operace EU; konstatuje, že možnost správné přípravy mise SBOP za účelem ochrany před kybernetickými útoky má své omezení;

19. zdůrazňuje, že plánování veškerých misí a operací SBOP musí doprovázet důkladné posouzení situace, pokud jde o kybernetické hrozby; konstatuje, že taxonomie hrozeb, kterou vypracovala Agentura Evropské unie pro bezpečnost sítí a informací poskytuje pro toto posouzení vhodnou šablonu; doporučuje vytvořit kapacity pro posuzování kybernetické odolnosti při velitelství SBOP;

20. je si vědom zejména toho, že je důležité omezit kybernetickou stopu a prostor k útoku na mise a operace v rámci SBOP na nezbytné minimum; naléhavě vyzývá osoby, které se zabývají příslušným plánováním, aby k tomu přihlížely od začátku procesu plánování;

21. uznává analýzu potřeb agentury EDA týkajících se odborné přípravy, která poukázala na hlavní nedostatky v oblasti dovedností a schopností v oblasti kybernetické obrany mezi osobami s rozhodovací pravomocí nejen v členských státech, a vítá iniciativy této agentury v oblasti kurzů pro vedoucí osoby s rozhodovací pravomocí v členských státech na podporu plánování misí a operací SBOP;

Vzdělávání a odborná příprava v oblasti kybernetické obrany

22. konstatuje, že zefektivněné prostředí vzdělávání a odborné přípravy EU v oblasti kybernetické obrany by významně zmírnilo hrozby, a vyzývá EU a členské státy, aby posílily svou spolupráci v oblasti vzdělávání, odborné přípravy a výcviku;

23. jednoznačně podporuje program vojenský Erasmus a další společné iniciativy v oblasti odborné přípravy a vzdělávání mezi členskými státy, které jsou zaměřeny na zvýšení interoperability ozbrojených sil členských států a rozvoj společné strategické kultury na základě častějších výměnných pobytů mladého vojenského personálu, přičemž je třeba mít na paměti, že tato interoperabilita je mezi všemi členskými státy a spojenci NATO nezbytná; domnívá se však, že výměny týkající se odborné přípravy a vzdělávání v oblasti kybernetické obrany by měly přesahovat tuto iniciativu a měly by zahrnovat vojenský personál všech věkových kategorií a všech hodností a rovněž studenty ze všech akademických středisek se vzdělávacími programy v oblasti kybernetické bezpečnosti;

24. zdůrazňuje, že v oblasti kybernetické obrany jsou zapotřebí další odborníci; vyzývá členské státy, aby usnadnily spolupráci mezi civilními a vojenskými akademiemi s cílem odstranit tento nesoulad a vytvořit více možností v oblasti vzdělávání a odborné přípravy v oblasti kybernetické obrany, a aby vyčlenily více prostředků na specializovanou odbornou přípravu v oblasti kybernetických operací; vyzývá vojenské akademie, aby začlenily vzdělávání v oblasti kybernetické obrany do svých osnov a pomohly tak rozšířit skupinu talentů v kybernetické oblasti, která je k dispozici pro potřeby misí SBOP;

25. vyzývá všechny členské státy, aby dostatečně a aktivně informovaly podniky, školy a občany o kybernetické bezpečnosti a hlavních digitálních hrozbách a zvyšovaly jejich povědomí o těchto skutečnostech; vítá v tomto ohledu kybernetické příručky jako nástroj sloužící ke směrování občanů a organizací k lepší strategii v oblasti kybernetické bezpečnosti, ke zvýšení znalostí o kybernetické bezpečnosti a k celkovému zlepšení kybernetické odolnosti;

26. konstatuje, že vzhledem k tomu, že jsou zapotřebí více specializovaní zaměstnanci, měly by se členské státy zaměřit nejen na nábor schopných zaměstnanců ozbrojených sil, ale také na udržení potřebných specialistů;

27. vítá, že 11 členských států (Belgie, Estonsko, Finsko, Irsko, Lotyšsko, Německo, Nizozemsko, Portugalsko, Rakousko, Řecko a Švédsko) projektu „Cyber Ranges Federation" zahájilo realizaci prvního ze čtyř projektů v oblasti kybernetické obrany, které probíhají v rámci programu Evropské obranné agentury v oblasti sdružování a společného využívání kapacit; vyzývá ostatní členské státy, aby se k této iniciativě připojily; vyzývá členské státy, aby prosazovaly větší vzájemnou dostupnost virtuálního vzdělávání v oblasti kybernetické obrany a kybernetických polygonů; konstatuje v této souvislosti, že je třeba zvážit také úlohu agentury ENISA a její odborné znalosti;

28. domnívá se, že tyto iniciativy přispívají ke zlepšování kvality vzdělávání v oblasti kybernetické obrany na úrovni EU, zejména tím, že vytvářejí rozsáhlé technické platformy a dávají vzniknout komunitě odborníků EU; domnívá se, že evropské ozbrojené síly mohou zvýšit svou atraktivitu tím, že zajistí komplexní odbornou přípravu týkající se kybernetické obrany s cílem přilákat a udržet talenty v oblasti kybernetiky; zdůrazňuje, že je třeba určit slabá místa v počítačových systémech členských států i orgánů EU; uznává, že k nejčastěji zjištěným slabým místům v systémech kybernetické bezpečnosti patří lidská chyba, a proto vyzývá k pravidelné odborné přípravě vojenského i civilního personálu pracujícího v orgánech EU;

29. vyzývá Evropskou obrannou agenturu, aby co nejdříve zavedla platformu pro koordinaci vzdělávání, odborné přípravy a výcviku v oblasti kybernetické bezpečnosti (CD TEXP), která by měla podpořit program „Cyber Ranges Federation", se zaměřením na posílení spolupráce v oblasti harmonizovaných požadavků, podporu výzkumu a technologických inovací v oblasti kybernetické obrany a společnou pomoc třetím zemím při budování jejich kapacit za účelem vytvoření odolnosti, pokud jde o kybernetickou bezpečnost; vyzývá Komisi a členské státy, aby tyto iniciativy doplnily specializovaným evropským střediskem pro odbornou přípravu v oblasti kybernetické obrany s cílem zajistit odbornou přípravu pro nejnadějnější nové zaměstnance, která by podpořila odbornou přípravu zapojených členských států v kybernetické oblasti;

30. vítá skutečnost, že s cílem zvýšení úrovně vzdělávacích a výcvikových příležitostí v členských státech byla v rámci EBOP vytvořena platforma pro vzdělávání, odbornou přípravu, výcvik a hodnocení v oblasti kybernetické bezpečnosti (ETEE);

31. podporuje více výměn informací o dané situaci pomocí předložení nejlepšího kybernetického výcviku a koordinace příslušných snah o rozvoj kapacit za účelem dosažení větší interoperability a lepší prevence a reakce na budoucí útoky; vyzývá, aby tyto projekty byly prováděny se spojenci NATO, ozbrojenými silami členských států EU a dalšími partnery s rozsáhlými zkušenostmi v oblasti boje proti kybernetickým útokům s cílem vypracovat operační připravenost, společné postupy a normy, aby bylo možné komplexně čelit různým kybernetickým hrozbám; vítá v tomto ohledu zapojení EU do kybernetického výcviku, jako je CODE (Kybernetický ofenzivní a defenzivní výcvik);

32. připomíná, že odolný kybernetický prostor vyžaduje bezchybnou kybernetickou hygienu; vyzývá všechny veřejné a soukromé zúčastněné strany, aby prováděly pravidelná školení v oblasti kybernetické hygieny pro všechny své zaměstnance;

33. doporučuje zvýšit výměnu odborných znalostí a získaných poznatků mezi ozbrojenými silami, policejními silami a dalšími státními orgány členských států aktivně zapojenými do boje proti kybernetickým hrozbám;

Spolupráce mezi EU a NATO v oblasti kybernetické obrany

34. opakovaně zdůrazňuje, že EU a NATO mají na základě svých společných hodnot a strategických zájmů zvláštní odpovědnost a způsobilost řešit narůstající problémy v oblasti kybernetické bezpečnosti a kybernetické obrany účinněji a v úzké spolupráci, a to hledáním možné doplňkovosti, předcházením zdvojování úsilí a uznáváním svých příslušných povinností;

35. vyzývá Radu, aby ve spolupráci s dalšími příslušnými orgány a strukturami EU zvážila způsoby, jak co nejdříve, harmonizovaně a v úzké spolupráci s NATO zajistit podporu na úrovni Unie pro začlenění kybernetické oblasti do vojenských doktrín členských států;

36. vyzývá k provádění uvedených opatření, která již byla dohodnuta; vyzývá ke zvážení možnosti nových iniciativ na podporu spolupráce mezi EU a NATO, mj. s přihlédnutím k možnostem spolupráce v rámci specializovaného střediska NATO v oblasti kybernetické obrany (Cooperative Cyber Defence Centre of Excellence, CCD COE) a Akademie NATO pro komunikační a informační systémy, jejichž cílem je rozšířit kapacity týkající se odborné přípravy v oblasti IT a kybernetických systémů z hlediska softwaru i hardwaru, pokud jde o kybernetickou obranu; konstatuje, že by to mohlo zahrnovat dialog s NATO týkající se možnosti EU připojit se k CCD COE s cílem zvýšit doplňkovost a spolupráci; vítá nedávné vytvoření specializovaného Evropského střediska pro boj proti hybridním hrozbám; naléhavě vyzývá všechny příslušné orgány a spojence, aby pravidelně projednávali své činnosti s cílem zabránit překrývání a podpořit koordinovaný přístup ke kybernetické obraně; domnívá se, že je zásadní podnítit výměnu zpravodajských informací o kybernetických hrozbách mezi členskými státy a s NATO, a sice na základě vzájemné důvěry;

37. je přesvědčen, že rozšíření spolupráce mezi EU a NATO je v oblasti kybernetické obrany zásadní a užitečné, neboť je prostředkem k tomu, jak předcházet kybernetickým útokům, odhalovat je a odrazovat od nich; vyzývá proto obě tyto organizace, aby rozšířily svou operační spolupráci a koordinaci a zintenzivnily společnou snahu o vybudování kapacit, zejména v podobě společného cvičení a vzdělávání civilních a vojenských zaměstnanců v oblasti kybernetické obrany a díky účasti členských států na projektech NATO v oblasti inteligentní obrany; považuje za zásadní, aby EU a NATO zesílily výměnu informací s cílem umožnit oficiálně určovat pachatele kybernetických útoků a následně umožnit ukládat omezující sankce těm, kteří za tyto útoky odpovídají; naléhavě vyzývá obě organizace k užší spolupráci také ohledně kybernetických aspektů řešení krizí;

38. vítá výměnu koncepcí s cílem začlenit požadavky a normy týkající se kybernetické obrany do plánování a vedení misí a operací za účelem podpory interoperability a vyjadřuje naději, že na tuto výměnu naváže intenzivnější operační spolupráce ohledně zajištění kybernetické obrany příslušných misí a synchronizace operačních přístupů;

39. vítá dohodu mezi skupinou EU pro reakci na počítačové hrozby (CERT-EU) a skupinou NATO pro reakci na počítačové incidenty (NCIRC), která má usnadnit výměnu informací, logistickou podporu, sdílené posuzování hrozeb, získávání zaměstnanců a výměnu osvědčené praxe s cílem zajistit schopnost reagovat na hrozby v reálném čase; zdůrazňuje, že je důležité podporovat výměnu informací mezi týmy v rámci skupin CERT-EU a NCIRC a snažit se o vybudování větší důvěry; má za to, že existuje domněnka, že informace, které má k dispozici skupina CERT-EU, by mohl využít výzkum v oblasti kybernetické obrany a NATO a že tyto informace by se proto měly sdílet, pokud bude zajištěn plný soulad s právními předpisy EU v oblasti ochrany údajů;

40. vítá spolupráci mezi těmito dvěma organizacemi na cvičení v oblasti kybernetické obrany; bere na vědomí účast zástupců EU na každoročním koaličním cvičení v oblasti kybernetické obrany; je si vědom pokroku, který představuje účast EU na cvičení NATO v oblasti krizového řízení 17 prostřednictvím paralelních a koordinovaných cvičení (PACE), a vítá zejména to, že do tohoto cvičení byla začleněna také oblast kybernetické obrany; vyzývá obě organizace k zintenzivnění tohoto úsilí;

41. naléhavě vyzývá EU a NATO, aby organizovaly pravidelná cvičení na strategické úrovni s účastí nejvyšších politických představitelů z obou organizací; vítá v této souvislosti estonské cvičení EU CYBRID 2017, během něhož se generální tajemník NATO poprvé zúčastnil cvičení EU;

42. podotýká, že existuje značný prostor pro ještě náročnější a konkrétnější program v oblasti kybernetické obrany, který by v rámci konkrétních operací přesahoval koncepční rámec spolupráce; naléhavě vyzývá obě organizace, aby zavedly již existující agendu do praxe a účinně ji provedly a aby předložily ambicióznější návrhy týkající se příštího přehodnocení uplatňování společného prohlášení;

43. vítá průmyslové kybernetické partnerství NATO (NATO Industry Cyber Partnership, NICP) uzavřené v roce 2014 a vyzývá k zapojení EU do společných snah NICP s cílem propojit úsilí v oblasti spolupráce mezi NATO a EU s úsilím vedoucích průmyslových subjektů specializovaných na kybernetické technologie s cílem pokročit v oblasti kybernetické bezpečnosti pomocí trvalé spolupráce zaměřené zejména na: odbornou přípravu, výcvik a vzdělávání zástupců NATO, EU a průmyslu; začlenění EU a průmyslu do projektů NATO v oblasti inteligentní obrany; společné sdílení informací a osvědčených postupů v zájmu připravenosti a obnovy mezi NATO, EU a průmyslem; úsilí o společně budované kapacity pro kybernetickou obranu; a ve vhodných případech zajištění společné reakce na kybernetické incidenty;

44. bere na vědomí pokračující práci na návrhu nařízení, kterým se mění nařízení o agentuře ENISA ((EU) č. 526/2013) a kterým se stanoví evropský rámec pro certifikaci a označování bezpečnosti IKT; vyzývá agenturu ENISA, aby podepsala dohodu s NATO s cílem zvýšit jejich praktickou spolupráci, včetně výměny informací a účasti na výcviku v oblasti kybernetické obrany;

Mezinárodní normy platné pro oblast kybernetického prostoru

45. vyzývá k začlenění kapacity v oblasti kybernetické obrany do SZBP a začlenění vnější činnosti EU a jejích členských států jako průřezového úkolu a vyzývá k užší spolupráci mezi členskými státy, orgány EU, NATO, OSN, Spojenými státy a dalšími strategickými partnery, zejména pokud jde o pravidla, normy a opatření pro jejich vymáhání v kyberprostoru;

46. s politováním konstatuje, že skupina vládních odborníků OSN (UNGGE) pro období 2016-2017 nebyla ani po několika měsících jednání schopna dosáhnout nové společné dohody ohledně příslušné zprávy; připomíná, že jak uvádí zpráva z roku 2013 je v kyberprostoru uplatňováno a mělo by být prosazováno zejména platné mezinárodní právo a Charta Organizace spojených národů, která zakazuje hrozbu silou nebo použití síly vůči politické nezávislosti jakéhokoli státu, včetně škodlivých kybernetických operací určených k narušení technické infrastruktury nezbytné pro provádění oficiálních participativních postupů v jiném státě, včetně voleb; připomíná, že zpráva vládních odborníků na oblast informační bezpečnosti fungující při OSN z roku 2015 uvádí soubor norem odpovědného chování států, který zahrnuje zákaz toho, aby státy prováděly kybernetickou činnost v rozporu se svými závazky podle mezinárodních předpisů nebo aby tuto činnost vědomě podporovaly; vyzývá EU, aby zaujala vedoucí postavení v probíhajících a budoucích diskusích o mezinárodních normách v kybernetickém prostoru a jejich provádění;

47. poukazuje na význam Tallinské příručky 2.0, která představuje základ pro diskuzi a analýzu toho, jak lze stávající mezinárodní právo uplatnit na kybernetický prostor; vyzývá členské státy, aby zahájily analýzu zjištění, která odborníci v Tallinské příručce uvedli, a začaly je uplatňovat a aby se dohodly na dalších dobrovolných normách pro mezinárodní chování; konstatuje zejména, že veškeré ofenzivní využití kybernetických kapacit by mělo být založeno na mezinárodním právu;

48. potvrzuje, že je zcela oddán myšlence otevřeného, svobodného, stabilního a bezpečného kybernetického prostoru, v jehož rámci by se dodržovaly základní hodnoty demokracie, lidská práva a zásady právního státu a kde by se mezinárodní spory řešily mírovými prostředky na základě Charty OSN a zásad mezinárodního práva; vyzývá členské státy, aby podporovaly další uplatňování společného komplexního postoje EU k diplomacii a stávajícím normám v kybernetické oblasti a aby spolu s NATO vypracovaly kritéria a definice na úrovni EU týkající se toho, co představuje kybernetický útok, aby se zlepšila schopnost EU rychle se dohodnout na společném postoji v případě mezinárodně nesprávného jednání v podobě kybernetického útoku; plně podporuje provádění dobrovolných, nezávislých norem odpovědného chování států v kybernetickém prostoru, které by zahrnovaly respektování soukromí a dodržování základních práv občanů, vyplývajících ze zprávy vládních odborníků na oblast informační bezpečnosti fungující při OSN z roku 2015, a vytvoření regionálních opatření na budování důvěry; podporuje v této souvislosti činnost Globální komise pro stabilitu kybernetického prostoru za účelem vypracování návrhů norem a politik, které zlepší mezinárodní bezpečnost a stabilitu a poskytnou návod pro odpovědné chování států a nestátních subjektů v kybernetickém prostoru; podporuje návrh, že by státní a nestátní subjekty neměly provádět nebo vědomě umožňovat činnost, která úmyslně a podstatně poškozuje obecnou dostupnost nebo integritu veřejné podstaty internetu a tím i stabilitu kybernetického prostoru;

49. uznává, že většinu technologické infrastruktury vlastní nebo provozuje soukromý sektor, a že jsou tedy úzká spolupráce, konzultace a začlenění soukromého sektoru a skupin občanské společnosti pomocí dialogu s mnoha zúčastněnými stranami nezbytné k zajištění otevřeného, svobodného, stabilního a bezpečného kybernetického prostoru;

50. je si vědom toho, že vzhledem ke svému obtížnému prosazování nepřinášejí dvoustranné dohody mezi státy vždy očekávané výsledky; domnívá se proto, že účinným způsobem, jak by bylo možné doplnit snahy více zúčastněných stran, je vytváření koalic v rámci podobně smýšlejících skupin zemí, které se chtějí dohodnout na konsenzu; zdůrazňuje významnou úlohu místních orgánů v procesu technologických inovací a sdílení údajů, pokud jde o posílení boje proti trestné činnosti a teroristickým činnostem;

51. vítá skutečnost, že Rada přijala rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru, tzv. soubor nástrojů EU pro diplomacii v oblasti kybernetiky; podporuje možnost, aby EU přijala restriktivní opatření vůči nepřátelům napadajícím její členské státy v kybernetickém prostoru, včetně ukládání sankcí;

52. požaduje rovněž jasný aktivní přístup ke kybernetické bezpečnosti a kybernetické obraně a vyzývá k posílení diplomacie EU v kybernetické oblasti coby průřezového úkolu v zahraniční politice EU a její kapacity a všech nástrojů, tak aby mohly účinně posílit normy a hodnoty EU a vést k dosažení konsenzu o pravidlech, normách a opatřeních pro jejich prosazování v kybernetickém prostoru na celém světě; konstatuje, že budování kybernetické odolnosti ve třetích zemích přispívá k mezinárodnímu míru a bezpečnosti, což nakonec zvyšuje bezpečnost evropských občanů;

53. domnívá se, že kybernetické útoky, jako je NotPetya a WannaCry, jsou buď řízené státem, nebo k nim dochází s vědomím státu a jeho souhlasem; konstatuje, že tyto kybernetické útoky, které způsobují závažnou a trvalou hospodářskou škodu a ohrožují život, jsou jasným porušením mezinárodního práva a právních norem; domnívá se tedy, že NotPetya a WannaCry představují porušení mezinárodního práva, jimiž se provinily Ruská federace a Severní Korea, a že tyto dva státy by měly čelit úměrné a náležité reakci ze strany EU a NATO;

54. vyzývá Evropské centrum Europolu pro boj proti kyberkriminalitě, aby se stal ústředním místem pro divizi pro prosazování práva a vládní agentury věnované kyberkriminalitě, jejichž hlavní odpovědností by bylo řídit obranu jak domény eu, tak důležité infrastruktury sítí EU během útoku; zdůrazňuje, že toto ústřední místo by rovněž mělo být pověřeno výměnou informací a mělo by poskytovat pomoc členským státům;

55. zdůrazňuje, že je důležité vypracovat normy ohledně soukromí a bezpečnosti, šifrování, nenávistných výroků, dezinformací a teroristických hrozeb;

56. doporučuje, aby každý členský stát EU přijal povinnost pomáhat ostatním členským státům napadeným kybernetickým útokem a zajistit vnitrostátní odpovědnost v kybernetické oblasti v úzké spolupráci s NATO;

Civilně-vojenská spolupráce

57. vyzývá všechny zúčastněné strany, aby rozšířily partnerství v oblasti předávání poznatků, uplatňovaly vhodné obchodní modely a budovaly důvěru mezi podniky a koncovými uživateli z oblasti obrany a civilními uživateli a dále aby zlepšily transformaci akademických poznatků v praktická řešení, tak aby bylo možné zajistit jejich synergické působení a převádění řešení mezi civilním a vojenským trhem, který z hlediska kybernetické bezpečnosti a produktů kybernetické bezpečnosti v podstatě tvoří jeden trh, a to na základě transparentních postupů a za dodržování práva EU a mezinárodního práva s cílem zachovat a posílit strategickou autonomii EU; bere na vědomí ústřední úlohu, kterou soukromé firmy v oblasti kybernetické bezpečnosti hrají při včasném varování a připisování kybernetických útoků;

58. klade důraz na zásadní význam výzkumu a vývoje, zejména vzhledem k vysokým požadavkům na bezpečnost na obranném trhu; naléhavě vyzývá EU a členské státy, aby evropským podnikům v oblasti kybernetické bezpečnosti a dalším příslušným hospodářským subjektům, zejména malým a středním podnikům a začínajícím podnikům (které jsou hlavním zdrojem inovativních řešení v oblasti kybernetické obrany) poskytovaly větší praktickou podporu a snížily byrokratickou zátěž a aby prosazovaly užší spolupráci s vysokoškolskými výzkumnými organizacemi a významnými aktéry, tak aby došlo k omezení závislosti na produktech v oblasti kybernetické bezpečnosti z vnějších zdrojů a k vytvoření strategického dodavatelského řetězce v rámci EU s cílem posílit její strategickou nezávislost; v této souvislosti poukazuje na cenný příspěvek, který by mohl zajistit Evropský obranný fond a další nástroje v rámci víceletého finančního rámce (VFR);

59. vybízí Komisi, aby začlenila prvky kybernetické obrany do sítě Evropských výzkumných a odborných středisek pro kybernetickou bezpečnost mimo jiné s cílem zajistit v příštím VFR dostatečné zdroje pro kybernetické kapacity a technologie v oblasti dvojího užití;

60. konstatuje, že ochrana životně důležité veřejné a jiné civilní infrastruktury, zejména informačních systémů a souvisejících údajů, je jedním z významných úkolů pro členské státy, zejména pro orgány pověřené ochranou informačních systémů, a že by měla spadat buď do působnosti vnitrostátních struktur kybernetické obrany, nebo do působnosti těchto orgánů; zdůrazňuje, že to si vyžádá určitou míru důvěry a co nejužší spolupráci mezi vojenskými složkami, agenturami pro kybernetickou obranu a jinými příslušnými orgány v této oblasti a příslušnými průmyslovými odvětvími, které lze dosáhnout pouze pomocí jasného vymezení úkolů, rolí a povinností civilních a vojenských subjektů, a naléhavě vyzývá všechny zúčastněné strany, aby k tomu v rámci svého plánování přihlédly; naléhavě vyzývá k větší přeshraniční spolupráci, pokud jde o prosazování práva v souvislosti s odstraňováním nepřátelské činnosti v kybernetické oblasti za současného dodržování právních předpisů EU v oblasti ochrany údajů;

61. vyzývá všechny členské státy, aby soustředily své vnitrostátní strategie kybernetické bezpečnosti na ochranu informačních systémů a souvisejících údajů a považovaly ochranu této kritické infrastruktury za součást svých vlastních povinností náležité péče; naléhavě vyzývá členské státy, aby přijaly a provedly strategie, pokyny a nástroje, které zajistí přiměřenou úroveň ochrany proti hrozbám na identifikovatelné úrovni a jejichž náklady a zátěž na ochranu budou úměrné pravděpodobnému poškození, které hrozí dotčeným stranám; žádá členské státy, aby přijaly náležitá opatření, která uloží právnickým osobám spadajícím do jejich pravomoci povinnost chránit osobní údaje, jež mají na starosti;

62. uznává, že kvůli měnícímu se prostředí kybernetických hrozeb by mohla být vhodná silnější a strukturovanější spolupráce s příslušníky policie, zejména v některých kritických oblastech, např. při sledování hrozeb v oblastech jako je kybernetický džihád, kybernetický terorismus, on-line radikalizace a financování extremistických či radikálních organizací;

63. vybízí k úzké spolupráci mezi agenturami EU, jako je EDA, ENISA, Evropské centrum pro boj proti kyberkriminalitě, v rámci přístupu jdoucího napříč odvětvími s cílem prosazovat synergické působení a zabránit překrývání;

64. vyzývá Komisi, aby vypracovala plán pro koordinovaný přístup k evropské kybernetické obraně, který by zahrnoval aktualizaci politického rámce EU v oblasti kybernetické obrany, aby bylo zajištěno, že tento rámec jakožto příslušný politický mechanismus pro dosahování cílů EU v této oblasti stále plní svůj účel, a to v úzké spolupráci s členskými státy, agenturou EDA, Parlamentem a ESVČ; konstatuje, že tento proces musí být součástí širšího strategického přístupu k SZBP;

65. vzhledem k tomu, že v nadcházejících letech se zejména v rozvojových zemích objeví miliony nových uživatelů Internetu, vyzývá k budování kapacit v oblasti kybernetické bezpečnosti na základě rozvojové spolupráce a k trvalému vzdělávání a odborné přípravě v oblasti kybernetické informovanosti, čímž dojde k posílení odolnosti zemí a společností vůči kybernetickým a hybridním hrozbám;

66. požaduje mezinárodní spolupráci a vícestranné iniciativy s cílem vybudovat přísné rámce v oblasti kybernetické obrany a kybernetické bezpečnosti za účelem boje proti zmocňování se státu pomocí korupce, finančních podvodů, praní peněz, financování terorismu a řešit výzvy, které představuje kybernetický terorismus a kryptoměny a další alternativní platební metody;

67. konstatuje, že kybernetické útoky, jako je NotPetya, se rychle šíří, čímž způsobují nahodilou škodu, neexistuje-li všeobecná odolnost na celém světě; domnívá se, že odborná příprava a vzdělání v oblasti kybernetické obrany by měly být součástí vnější činnosti EU a že budování kybernetické odolnosti ve třetích zemích přispívá k mezinárodnímu míru a bezpečnosti, což nakonec zvyšuje bezpečnost evropských občanů;

Institucionální posílení

68. vyzývá členské státy k ambicióznější spolupráci v kybernetické oblasti v rámci stálé strukturované spolupráce; navrhuje, aby členské státy v rámci stálé strukturované spolupráce zahájily nový program spolupráce v kybernetické oblasti s cílem podpořit rychlé a efektivní plánování, velení a kontrolu současných a budoucích operací a misí EU; konstatuje, že by to mělo vést k lepší koordinaci operačních kapacit v kybernetickém prostoru a může to vést ke vzniku společného velení v oblasti kybernetické obrany, pokud tak rozhodne Evropská rada;

69. připomíná svou výzvu členským státům a vysoké představitelce, místopředsedkyni, aby předložily bílou knihu EU o bezpečnosti a obraně; vyzývá členské státy a vysokou představitelku, místopředsedkyni, aby z obrany a odrazování učinily základní prvek bílé knihy týkající se jak ochrany kybernetické oblasti pro operace stanovené v článku 43, tak společné obrany stanovené v čl. 42 odst. 7 SEU;

70. konstatuje, že nový program spolupráce v kybernetické oblasti v rámci stálé strukturované spolupráce by měli střídavě vést vysoce postavení vojenští i civilní zaměstnanci ze všech členských států, kteří by odpovídali ministrům obrany EU v rámci stálé strukturované spolupráce a vysoké představitelce, místopředsedkyni, aby se podpořily zásady důvěry mezi členskými státy a orgány a agenturami EU při výměně informací a zpravodajských informací;

71. opakuje svou výzvu ohledně vytvoření Rady pro obranu EU, která by vycházela ze stávajícího ministerského řídícího výboru agentury EDA a formátu stálé strukturované spolupráce ministrů obrany EU, s cílem zaručit stanovování priorit, operacionalizaci zdrojů a účinnou spolupráci a integraci mezi členskými státy;

72. připomíná, že je třeba zajistit, aby Evropský obranný fond pokračoval nebo byl dokonce v příštím VFR navýšen a měl dostatečný rozpočet na kybernetickou obranu;

73. požaduje vyšší zdroje na modernizaci a zefektivnění kybernetické bezpečnosti a šíření zpravodajských informací mezi ESVČ / Zpravodajským a informačním centrem EU (INTCEN), Radou a Komisí;

Partnerství veřejného a soukromého sektoru

74. uznává, že soukromé společnosti hrají hlavní úlohu při předcházení a odhalování incidentů v oblasti kybernetické bezpečnosti, při zabraňování jejich šíření a reakci na ně, a to nikoli jen jako poskytovatelé technologie, ale také jako poskytovatelé jiných služeb, než jsou služby v oblasti IT;

75. uznává úlohu soukromého sektoru při předcházení a odhalování incidentů v oblasti kybernetické bezpečnosti, při zabraňování jejich šíření a reakci na ně spolu s jeho úlohou při podněcování inovací v oblasti kybernetické obrany, a požaduje proto posílenou spolupráci se soukromým sektorem s cílem zajistit společné chápání požadavků EU a NATO a podporu při hledání společných řešení;

76. vyzývá EU, aby provedla komplexní přezkum softwaru, vybavení v oblasti IT a komunikací a infrastruktury používané v orgánech s cílem vyloučit programy a zařízení, která by mohla být nebezpečná, a zakázat ta, jejichž škodlivost se prokázala, jako je Kaspersky Lab;

o

o o

77. pověřuje svého předsedu, aby předal toto usnesení Evropské radě, Radě, Komisi, místopředsedkyni Komise, vysoké představitelce Unie pro zahraniční věci a bezpečnostní politiku, agenturám EU v oblasti obrany a kybernetické bezpečnosti, generálnímu tajemníkovi NATO a vnitrostátním parlamentům členských států EU.