

# I. ÚVOD

Návrat války v Evropě v podobě neodůvodněné a nevyprovokované vojenské agrese Ruska vůči Ukrajině byl varovným signálem pro všechny, kdo zpochybňují přístup EU k bezpečnosti a obraně, její schopnost prosazovat svou vizi a hájit své zájmy, a to i v kyberprostoru. Autoritářské režimy se snaží zpochybňovat a narušovat mezinárodní řád v kyberprostoru založený na pravidlech a společně s pevninou, mořem, vzduchem a vesmírem se z něj stává stále spornější oblast. V posledních letech se zintenzivnilo nepřátelské chování státních i nestátních subjektů v kyberprostoru, včetně rostoucího počtu kybernetických útoků zaměřených na vojenskou a civilní kritickou infrastrukturu v EU, jakož i na nasazené mise a operace.

Hranice mezi civilním a vojenským rozměrem kyberprostoru jsou nejasné, jak je patrné z nedávných útoků na energetické sítě, dopravní infrastrukturu a kosmické prostředky. To rovněž ilustruje vzájemnou závislost mezi fyzickou a digitální infrastrukturou a potenciál významných kybernetických bezpečnostních incidentů narušit nebo poškodit kritickou infrastrukturu. Jedná se o jasnou připomínku toho, že EU v kyberprostoru potřebuje úzkou vojenskou a civilní spolupráci, aby mohla lépe zaručovat bezpečnost.

EU musí za svou vlastní bezpečnost převzít větší odpovědnost. To vyžaduje moderní a interoperabilní evropské ozbrojené síly. Členské státy se proto musí co nejrychleji a přednostně zavázat ke zvýšení investic do vytvoření schopnosti komplexní kybernetické obrany, včetně aktivních obranných schopností. I když EU nadále plně podporuje uplatňování mezinárodního práva a norem v kyberprostoru, měla by dát najevo svou ochotu využívat tyto schopnosti v případě kybernetického útoku na členský stát koordinovaně.

Má-li EU v této oblasti uspět, musí zajistit svou technologickou a digitální suverenitu v kybernetické oblasti. Schopnost EU jednat bude záviset na její schopnosti ovládnout a rozvíjet špičkové technologie pro kybernetickou bezpečnost a kybernetickou obranu v EU. Vzhledem k tomu, že kybernetické technologie mají silný potenciál dvojího užití, musí odvětví kybernetické bezpečnosti a kybernetické obrany, výzkum a vývoj a inovační činnosti fungovat v mnohem větší synergii, aby se rozvinuly lepší schopnosti.

Důležitou součástí obranných schopností EU jsou společná prevence a detekce. EU musí být schopna odhalit útoky v rané fázi. Zjištěné údaje musí být přeměněny na bezprostředně použitelné zpravodajské informace, které mohou sloužit kybernetické bezpečnosti i kybernetické obraně. Tato spolupráce mezi obrannou a civilní kybernetickou komunitou je základem lepšího společného situačního povědomí v kyberprostoru a je stejně tak zásadní pro koordinovanou reakci na krize na technické i na provozní úrovni.

Ozbrojený konflikt na Ukrajině rovněž ukázal hodnotu úzké spolupráce se soukromým sektorem a nutnost mít přístup k soukromým důvěryhodným poskytovatelům, kteří fungují jako kybernetické rezervy pro posílení reakce v případě závažných kybernetických útoků. Je proto nezbytné zajistit, aby se členské státy mohly spolehnout na podporu z důvěryhodných kybernetických rezerv a aby k tomu docházelo bezpečným a koordinovaným způsobem.

Toto společné sdělení, které vychází z politického rámce pro kybernetickou obranu[[1]](#footnote-2), navrhuje ambiciózní strategii, která EU a jejím členským státům umožní jednat v kybernetickém prostoru sebejistě a asertivně. Jeho cílem je podpořit schopnosti kybernetické obrany prostřednictvím individuálních nebo společných akcí členských států a posílit koordinaci a spolupráci mezi kybernetickými komunitami EU. Bude rovněž pracovat na snížení strategické závislosti EU na kritických kybernetických technologiích a na posílení evropské technologické a průmyslové základny obrany (dále jen „EDTIB“). Tato politika stanoví pravidla hry EU a navrhne způsoby, jak posílit solidaritu v jádru EU v oblasti kybernetické obrany, jakož i spolupráci se soukromým sektorem za účelem posílení reakce v případě závažných kybernetických útoků. Vzhledem k nadnárodní povaze kybernetických hrozeb bude rozvíjet vzájemně výhodná a přizpůsobená partnerství v oblasti kybernetické obrany, včetně budování kapacit kybernetické obrany, a posilovat kybernetickou odolnost partnerských zemí.

Jak je navrženo ve Strategickém kompasu pro bezpečnost a obranu[[2]](#footnote-3) přijatém Radou v březnu 2022, současná politika kybernetické obrany tak posílí schopnost předcházet kybernetickým útokům zaměřeným na EU a její členské státy a všemi dostupnými prostředky je odhalovat, bránit před nimi, překonat jejich následky a odrazovat od nich. To je v souladu s digitálními prioritami Komise, ambicemi stanovenými ve Strategii kybernetické bezpečnosti EU z roku 2020[[3]](#footnote-4), oznámením předsedkyně von der Leyenové v jejím projevu o stavu Unie v roce 2021[[4]](#footnote-5) a závěry Rady o rozvoji kybernetické pozice Evropské unie[[5]](#footnote-6) ze dne 23. května 2022. Společné sdělení o nedostatcích v oblasti investic do obrany z roku 2022[[6]](#footnote-7) rovněž vyzvalo EU a její členské státy, aby zahájily práci na vytvoření schopnosti komplexní kybernetické obrany – od výzkumu, detekce a ochrany až po reakci.

# II. KYBERNETICKÁ OBRANA EU K PŘEDCHÁZENÍ KYBERNETICKÝM ÚTOKŮM, JEJICH ODHALOVÁNÍ, ODRAZOVÁNÍ OD NICH A OBRANĚ PŘED NIMI

**1. Společné úsilí o silnější kybernetickou obranu**

Kybernetické útoky mají často přeshraniční povahu a mohou mít fyzický dopad na kritickou infrastrukturu v EU. Významné kybernetické bezpečnostní incidenty mohou mít často příliš závažné negativní účinky na to, aby je jeden nebo několik členských států zvládly řešit samostatně. Mohou být rovněž součástí rozsáhlejších hybridních útoků prováděných třetími zeměmi s cílem destabilizovat hospodářství a společnost, oslabit kritickou infrastrukturu potřebnou k zajištění bezpečnosti EU nebo narušit a poškodit fungování demokracií, a to mimo jiné prostřednictvím útoků na volební infrastruktury.

V roce 2018 EU určila kybernetický prostor jako oblast vojenských operací. „Vojenská vize a strategie pro kyberprostor jako oblast operací“[[7]](#footnote-8) přijatá v roce 2021 stanoví rámcové podmínky a popisuje cíle, způsoby a prostředky potřebné k využívání kyberprostoru jako oblasti operací na podporu operací společné bezpečnostní a obranné politiky (dále jen „SBOP“) EU. Kybernetická obrana a využití souvisejících schopností v celém spektru vojenských operací v kyberprostoru je vnitrostátní výsadou členských států, přičemž se opírají o širší ekosystém, včetně silné průmyslové základny podporované rozvojem schopností na úrovni EU.

Komunita EU pro kybernetickou obranu složená z obranných orgánů členských států a podporovaná orgány, institucemi a jinými subjekty EU má ve srovnání s ostatními kybernetickými komunitami[[8]](#footnote-9) určitá specifika a řídí se odlišným modelem správy. Neexistence zavedeného rámce pro výměnu informací a spolupráci mezi vojenskými týmy EU pro reakci na počítačové hrozby (dále jen „vojenské týmy CERT“), včetně podpory vojenských misí a operací v rámci SBOP, je s ohledem na zvýšenou míru kybernetických hrozeb ze strany státních a nestátních subjektů problematická.

Spolupráce mezi kybernetickými komunitami působícími v civilní sféře, v diplomatické oblasti a v oblasti vymáhání práva a jejich protějšky v oblasti obrany přinese všem dotčeným subjektům vysokou přidanou hodnotu. Je proto nezbytné tuto spolupráci umožnit poskytnutím vhodných a bezpečných prostředků pro výměnu informací a zapojením do cvičení a jiných činností, které budují důvěru a společné porozumění.

Kromě toho v současné době existuje mezi členskými státy pouze omezená vzájemná operační pomoc. Mělo by se prozkoumat další rozšíření koncepce týmů rychlé kybernetické reakce v celé EU, a to na základě souvisejících týmů rychlé kybernetické reakce a vzájemné pomoci v oblasti kybernetické bezpečnosti (CRRT)[[9]](#footnote-10) v rámci projektu stálé strukturované spolupráce (PESCO), a to i v souvislosti s čl. 42 odst. 7 Smlouvy o Evropské unii (SEU)[[10]](#footnote-11) (dále jen „ustanovení o vzájemné pomoci“) a článkem 222 Smlouvy o fungování Evropské unie (SFEU)[[11]](#footnote-12) (dále jen „doložka solidarity“). V podobném duchu je jedním z poznatků plynoucích z úspěšné ukrajinské kybernetické obrany v kontextu ruské útočné války rozhodující role, kterou hraje soukromý sektor. Mělo by proto být prozkoumáno, do jaké míry by soukromý sektor mohl rovněž přispět k posílení kybernetické reakce.

### 1.1 Posílení společného situačního povědomí a koordinace v rámci obranné komunity

Vzhledem k rozsahu rizika spojeného s kybernetickými útoky musí mít členské státy k dispozici co nejúplnější kolektivní situační povědomí, včetně schopnosti včasné detekce a zdrojů pro řádnou reakci a solidární a koordinovanou obnovu.

Co se týče vojenského situačního povědomí, je třeba zřídit **koordinační středisko EU pro kybernetickou obranu (EUCDCC)**, které by podporovalo zvyšování situačního povědomí v rámci obranné komunity, včetně všech vojenských velitelů EU v oblasti SBOP. Vysoký představitel představí návrh střediska EUCDCC pro posouzení členskými státy, a to na základě projektu Koordinačního střediska pro kybernetický a informační prostor (CIDCC) v rámci PESCO[[12]](#footnote-13). Jeho cílem bude poskytnout ucelenou analýzu kyberprostoru, elektromagnetického prostředí a kognitivní oblasti tím, že spojí různé zdroje informací na vojenské strategické a operační úrovni. Měly by být vytvořeny vhodné vazby mezi střediskem EUCDCC, Zpravodajským a informačním centrem EU (EU INTCEN) a zpravodajským ředitelstvím Vojenského štábu EU, a to v rámci společné zpravodajsko-analytické složky. Kromě vnějších informačních zdrojů by mělo středisko EUCDCC zřídit a integrovat nezávislý aktivní senzorový systém informačních technologií s cílem posílit sledování uzlů ve vlastnictví EU, které podporují vojenské mise a operace v rámci SBOP. Poskytne silnější detekční schopnosti a vytvoří novou vrstvu informací s cílem dále posílit informační základnu pro posuzování kybernetických rizik a situační povědomí.

K těmto účelům jsou požadovány kapacity, které umožňují a zajišťují vytvoření a udržování nepřetržitého provozního a pokud možno rozpoznatelného obrazu kyberprostoru, včetně probíhajících a bezprostředně hrozících kybernetických operací jak nepřátelských, tak přátelských sil. Tento obraz by přispěl k plánování a provádění vojenských misí a operací EU v rámci SBOP. Stane se tak vojenským příspěvkem k tomu, aby EU měla více informací o nepřátelských činnostech v kyberprostoru a mohla na ně zareagovat.

Za účelem zlepšení důvěry a výměny spolehlivých a včasných strategických informací o závažných kybernetických incidentech se bude dále rozvíjet a posilovat **konference velitelů kybernetických sil EU**[[13]](#footnote-14). S Evropskou obrannou agenturou (EDA), která působí jako sekretariát, a s účastí Vojenského štábu EU se bude konat nejméně dvakrát ročně, aby mohly být projednány operativní záležitosti a další důležitá témata.

Zřídí se operační síť pro **vojenské týmy CERT (MICNET)** s podporou agentury EDA. Všechny členské státy se vyzývají, aby se zapojily do sítě MICNET, jejíž zprovoznění se očekává v lednu 2023.

Usnadněním výměny informací mezi vojenskými týmy CERT podpoří síť MICNET důraznější a koordinovanější reakci na kybernetické hrozby postihující obranné systémy v EU, včetně těch, které se používají ve vojenských misích a operacích v rámci SBOP. Síť MICNET rovněž umožní v průběhu času udržet procesy odborné přípravy a neustálé určování nových požadavků na komunitu vojenských týmů CERT. V příštích čtyřech letech vyvine agentura EDA společně s členskými státy infrastrukturu pro sdílení informací a související nástroje a postupy na podporu sdílení informací mezi vojenskými týmy CERT. Síť MICNET rovněž poskytne rámec pro každoroční testování, validaci a identifikaci nových požadavků a řešení.

### 1.2 Posílení koordinace s civilními komunitami

Síť MICNET by měla sloužit jako rámec a infrastruktura pro sdílení informací mezi různými úrovněmi v rámci komunity pro kybernetickou obranu a externími zúčastněnými stranami.

Jakmile síť MICNET dosáhne vyšší úrovně vyspělosti, agentura EDA podpoří členské státy při zkoumání možností spolupráce se sítí **týmů pro reakci na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“)**, která sdružuje vnitrostátní týmy CSIRT a tým pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (dále jen „tým CERT-EU“). Tato spolupráce by mohla zahrnovat společná setkání a cvičení. Rovněž by mělo být prozkoumáno zapojení soukromého sektoru do sdílení příslušných informací a úsilí o reakci na incidenty.

Aby bylo možné účinněji zvládat kybernetické krize, měla by se konference velitelů kybernetických sil EU zapojit do činnosti Evropské sítě styčných organizací pro řešení kybernetických krizí (dále jen „CyCLONe“), která sdružuje členské státy a Komisi za účelem podpory koordinace a řešení rozsáhlých kybernetických bezpečnostních incidentů v EU. Díky tomuto zapojení budou vojenské zkušenosti zkombinovány s civilním situačním povědomím na strategické a operativní úrovni.

Vzhledem k tomu, že středisko EUCDCC by mělo působit jako ústřední uzel pro sběr, analýzu, posuzování a konečnou distribuci informací souvisejících s kybernetickou obranou, zejména v souvislosti s vojenskými misemi a operacemi v rámci SBOP, mohlo by se rovněž spojit s interinstitucionální pracovní skupinou pro řešení kybernetických krizí[[14]](#footnote-15), která byla zřízena s cílem zajistit informované rozhodování a koordinovanou reakci orgánů, institucí a jiných subjektů EU na závažné kybernetické krize na strategické a operativní úrovni.

Středisko EUCDCC si může rovněž vyměňovat příslušné informace se situačním a analytickým střediskem pro kybernetickou bezpečnost, které Komise zřizuje s podporou Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) a týmem CERT-EU s cílem poskytovat analýzu a účinnější podporu při řešení krizí.

Hlavní překážkou navíc zůstává nedostatek společně sdílených nebo interoperabilních zabezpečených komunikačních nástrojů a platforem mezi členskými státy a příslušnými orgány, institucemi a jinými subjekty EU. Komise a příslušné instituce v současné době mapují stávající nástroje pro zabezpečenou komunikaci v kybernetické oblasti. Na základě zmapování stávajících nástrojů Komise na konci roku 2022 předloží Radě svá doporučení, aby se mohly dohodnout na dalších opatřeních.

**Kybernetická solidarita EU pro lepší společnou detekci a situační povědomí**

Civilní podpůrná opatření mohou společné situační povědomí dále zvyšovat. Komunita pro kybernetickou obranu bude moci využívat silnější schopnosti v oblasti civilní detekce a situačního povědomí, které byly vyvinuty za účelem ochrany kritické infrastruktury EU. Za tímto účelem Komise připravuje iniciativu na podporu zavádění infrastruktury EU bezpečnostních operačních středisek (SOC), která bude založena na první fázi, jež má být zahájena v nadcházejících týdnech, a která bude poté rozšířena a zavedena ve větším měřítku[[15]](#footnote-16). V konečném důsledku by se jednalo o několik platforem bezpečnostních operačních středisek pro více zemí, z nichž každá by sdružovala národní bezpečnostní operační střediska, s podporou programu Digitální Evropa[[16]](#footnote-17), který doplní vnitrostátní finanční prostředky. Legislativní změny programu Digitální Evropa by umožnily dlouhodobou finanční podporu pro společné zadávání veřejných zakázek na mimořádně bezpečné nástroje a infrastrukturu nové generace. To by umožnilo, aby plánovaná infrastruktura EU bezpečnostních operačních středisek zlepšila kolektivní detekční schopnosti pomocí nejnovější umělé inteligence (UI) a analýzy dat, které by pokrývaly civilní komunikační sítě. Tato generace bezprostředně použitelných zpravodajských informací o kybernetických hrozbách by umožnila včasné varování orgánů a příslušných subjektů, aby mohly odhalit závažné incidenty a účinně na ně reagovat. Rozsah a působnost infrastruktury bude záviset na celkových finančních prostředcích, které mohou být použity na vnitrostátní úrovni a na úrovni Unie, v závislosti na dostupném rozpočtu v rámci víceletého finančního rámce.

Tato bezpečnostní operační střediska pro více zemí by rovněž mohla umožnit účast obranných subjektů vytvořením „obranného pilíře“, pokud jde o správu a druh sdílených informací. Tento „obranný pilíř“ by byl vypracován spolu s vysokým představitelem a mohl by zahrnovat zvláštní mechanismus pro výměnu informací s vojenskými činiteli, včetně střediska EUCDCC, pro něž by mohly být vypracovány bezpečnostní normy na úrovni obrany.

**Kybernetická solidarita EU v oblasti připravenosti, reakce a obnovy**

Významné kybernetické bezpečnostní incidenty mají často příliš závažné negativní účinky na to, aby je jeden nebo několik členských států zvládly řešit samostatně. V takových případech musí mít členské státy možnost využít vzájemnou pomoc a solidaritu, a to i v souvislosti s čl. 42 odst. 7 Smlouvy o EU a článkem 222 Smlouvy o fungování EU. Vysoký představitel ve spolupráci s Komisí a členskými státy prozkoumá možnosti **rozšíření koncepce týmů rychlé kybernetické reakce (CRRT)** na základě souvisejícího projektu CRRT v rámci PESCO s cílem lépe podporovat členské státy EU a mise a operace v rámci SBOP. Úlohou těchto týmů by bylo poskytovat přizpůsobenou a cílenou krátkodobou pomoc na vyžádání a v závislosti na konkrétních potřebách každého jednotlivého případu. Mohla by rovněž případně zahrnovat možnosti podpory ze strany důvěryhodných soukromých partnerů s cílem zajistit účinnou reakci a obnovu.

V rámci iniciativy EU pro kybernetickou solidaritu připravuje Komise opatření na posílení připravenosti a reakce v celé EU. To by zahrnovalo **testování základních subjektů provozujících kritickou infrastrukturu, pokud jde o potenciální zranitelná místa, na základě posouzení rizik na úrovni EU**, přičemž by se vycházelo z opatření, která již Komise zahájila spolu s agenturou ENISA, jakož i opatření pro reakci na incidenty, s cílem zmírnit dopad závažných incidentů, podpořit okamžitou obnovu nebo obnovit fungování základních služeb[[17]](#footnote-18).

Iniciativa EU pro kybernetickou solidaritu by mohla podpořit **postupné vytváření kybernetické rezervy na úrovni EU se službami od důvěryhodných soukromých poskytovatelů**, kteří by byli připraveni zasáhnout na žádost členských států v případě závažných přeshraničních incidentů. Úlohy a povinnosti by měly být jasně určeny a plně koordinovány se stávajícími subjekty, aby se zajistilo, že podpora z kybernetické rezervy na úrovni EU je poskytována tam, kde je zapotřebí, a doplňuje další možné formy pomoci. Zatímco rozsah opatření a přidělení nákladů na konkrétní zásahy by závisely na dostupných finančních prostředcích EU, EU by rovněž přidala hodnotu tím, že by zajistila dostupnost a připravenost této rezervy na úrovni EU. V zájmu zajištění vysoké úrovně důvěry Komise rovněž zváží možnosti podpory rozvoje systémů certifikace v oblasti kybernetické bezpečnosti pro tyto soukromé společnosti zabývající se kybernetickou bezpečností.

Klíčovým prvkem při budování připravenosti jsou cvičení. Ta podporují rozvoj společné znalostní základny a chápání kybernetické obrany, což následně zvyšuje operační připravenost. Společná cvičení v oblasti kybernetické obrany rovněž vytvoří interoperabilitu a důvěru mezi zúčastněnými stranami, včetně podpory vojenských misí a operací v rámci SBOP. Na základě série kurzů CYBER PHALANX[[18]](#footnote-19) a cvičení vojenských týmů CERT **vypracuje agentura EDA nový projekt CyDef-X, který spojí všechny členské státy a který bude sloužit jako rámec pro cvičení EU v oblasti kybernetické obrany**. Tento projekt by mohl sloužit k poskytování vzájemné pomoci podle čl. 42 odst. 7 Smlouvy o EU. Rovněž by mělo být prozkoumáno využití specializovaných prostředí pro testování, výcvik a cvičení v oblasti kybernetické obrany (např. Propojené kybernetické polygony), a to i využitím projektu Propojených kybernetických polygonů v rámci PESCO[[19]](#footnote-20).

Cvičení mohou rovněž hrát důležitou úlohu při zlepšování spolupráce mezi civilními a vojenskými subjekty. Při organizování cvičení by proto agentura ENISA, agentura EDA a další příslušné subjekty měly systematicky zvažovat začlenění účastníků z jiných kybernetických komunit.

V rámci posilování schopnosti EU předcházet kybernetickým útokům, odrazovat od nich a reagovat na ně a v souladu se Strategií kybernetické bezpečnosti EU z roku 2020 a Strategickým kompasem navrhne vysoký představitel v roce 2023 možnosti dalšího posílení souboru nástrojů EU pro diplomacii v oblasti kybernetiky[[20]](#footnote-21), přičemž bude vycházet z kybernetické pozice EU a poznatků získaných při provádění souboru nástrojů od jeho vytvoření.

|  |
| --- |
| ***Opatření v oblasti kybernetické obrany***   * Zřídit koordinační středisko EU pro kybernetickou obranu jako středisko pro společné vojenské situační povědomí a prozkoumat způsoby spolupráce se situačním a analytickým střediskem Komise, * dále rozvíjet a posilovat konferenci velitelů kybernetických sil EU, * povzbuzovat členské státy, aby se aktivně zapojily do sítě MICNET, sítě vojenských týmů CERT, a usilovat o navázání spolupráce se sítí civilních týmů CSIRT, * vypracovat nový rámcový projekt CyDef-X na podporu cvičení EU v oblasti kybernetické obrany, * prozkoumat možnosti dalšího rozvoje koncepce týmů rychlé kybernetické reakce na základě projektu CRRT v rámci PESCO, * prozkoumat možnosti dalšího rozvoje projektů Propojených kybernetických polygonů.   ***Civilní podpůrná opatření***   * Připravit iniciativu EU pro kybernetickou solidaritu, včetně případného aktu o legislativních změnách programu Digitální Evropa s cílem:   + posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce,   + postupně vytvářet kybernetickou rezervu na úrovni EU se službami od důvěryhodných soukromých poskytovatelů,   + podporovat testování kritických subjektů, pokud jde o potenciální zranitelná místa, na základě posouzení rizik na úrovni EU, * prozkoumat vývoj systémů certifikace v oblasti kybernetické bezpečnosti na úrovni EU pro odvětví kybernetické bezpečnosti a soukromé společnosti, * posílit spolupráci na strategické, operativní a technické úrovni mezi kybernetickou obranou a ostatními kybernetickými komunitami. |

**2. Zabezpečení obranného ekosystému EU**

V posledních letech se výrazně zvýšil počet kybernetických útoků, včetně útoků na dodavatelské řetězce zaměřených na kybernetickou špionáž, ransomware nebo narušení. V roce 2020 zasáhl útok na dodavatelský řetězec společnosti SolarWinds[[21]](#footnote-22) více než 18 000 organizací po celém světě, včetně vládních agentur, velkých podniků a společností z odvětví obrany. Zneužití zranitelnosti Apache log4j[[22]](#footnote-23) zdůraznilo, že i softwarové komponenty, které nejsou považovány za vysoce rizikové nebo kritické, mohou být využity k úspěšným útokům na velké společnosti nebo vlády v EU, a to i v oblasti obrany. To prokazuje jasnou potřebu dále posílit kybernetickou odolnost subjektů, které působí v obranném ekosystému EU, včetně vojenských subjektů, obranného průmyslu a soukromých subjektů.

Ozbrojené síly jsou do značné míry závislé na kritické civilní infrastruktuře, ať už se jedná o mobilitu, komunikace nebo energii. Tento vzájemný vztah dokládá ruský útok na družicovou síť KA-SAT[[23]](#footnote-24), kdy došlo k narušení komunikace mezi několika veřejnými orgány i ukrajinskými ozbrojenými silami. To dokazuje, že je nutné tuto kritickou infrastrukturu zabezpečit.

Za účelem řešení otázek souvisejících s bezpečností svých komunikačních a informačních systémů členské státy vypracovávají vlastní bezpečnostní normy a požadavky na vojenské systémy, které ne vždy zohledňují potřebu interoperability nebo existenci civilních norem pro výrobky dvojího užití. To má negativní dopad na schopnost členských států jednat v kybernetickém prostoru společně, a to i v souvislosti s vojenskými misemi a operacemi v rámci SBOP, a vytváří překážky pro vzájemnou pomoc. Kromě toho je rovněž nezbytné podporovat větší součinnost mezi vojenskými a civilními standardizačními postupy, neboť dodržování podobných, ale odlišných norem pro civilní a vojenské zákazníky vede v daném odvětví ke zvýšení výrobních nákladů na vývoj výrobků dvojího užití v průmyslu.

***2.1 Zvýšení kybernetické odolnosti obranného ekosystému***

Posílení kybernetické odolnosti obranného ekosystému vyžaduje cílená opatření a investice napříč širokou škálou subjektů od vojenské infrastruktury členských států a misí a operací v rámci SBOP až po kritickou infrastrukturu, obranný průmysl a příslušné výzkumné subjekty.

Pro úspěšné mise a operace v rámci SBOP je nezbytná ochrana informací potřebných pro informované rozhodování. EU a její členské státy musí ještě více posílit své vojenské velitelské a řídící struktury a rozvíjet a zabezpečovat svou infrastrukturu. To platí i pro politicko-vojenské konzultace v rané fázi řešení krizí pro účinné nasazení operačního velitelství, včetně útvaru schopnosti vojenského plánování a vedení (MPCC). To bude řešeno zejména pokračujícím rozvojem operační rozhlehlé sítě EU.

V souvislosti s vojenskými misemi a operacemi se subjekty působící v oblasti kybernetické obrany zabývají informacemi v různých formátech a s různým stupněm utajení, které pocházejí z různých zdrojů. Proto je používání nejmodernějších zabezpečených technologií, jako je umělá inteligence, s podporou průmyslu nanejvýš důležité.

Bezpečnost infrastruktury komunikačních a informačních systémů je třeba zlepšit uplatňováním vzájemně dohodnutých řídicích postupů, čímž se posílí důvěra v integritu informací dostupných mezi zúčastněnými stranami. Kromě toho bude vysoký představitel, a to i ve své funkci vedoucího agentury EDA, s podporou Komise pomáhat členským státům při vypracovávání **právně nezávazných doporučení pro obrannou komunitu**, **inspirovaných směrnicí o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS 2)**[[24]](#footnote-25), neboť obrana je z oblasti působnosti směrnice vyňata. To přispěje ke zvýšení celkové vyspělosti kybernetické obrany.

Návrh aktu o kybernetické odolnosti[[25]](#footnote-26) předložený Komisí, jehož cílem je stanovit požadavky na kybernetickou bezpečnost u výrobků s digitálními prvky, rovněž ještě více omezí prostor k útokům u výrobků dvojího užití používaných například v komunikačních a informačních systémech obranným průmyslem a vládními subjekty v oblasti obrany. Podle návrhu by výrobci byli povinni aktivně oznámit zneužití zranitelných míst do 24 hodin agentuře ENISA, která následně informuje příslušné vnitrostátní týmy CSIRT. V tomto ohledu by bylo rovněž důležité zajistit, aby byla obranná komunita rychle informována o zranitelných místech výrobků s digitálními prvky, jakož i o dostupných anebo použitých opravách a zmírňujících opatřeních.

Tím spíše ve světle toho, že armáda je závislá na kritické civilní infrastruktuře, **je také třeba dále zvyšovat ochranu kritické infrastruktury před rozsáhlými kybernetickými útoky**. Na žádost Rady[[26]](#footnote-27) vypracovávají Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací[[27]](#footnote-28) rizikové scénáře pro bezpečnost digitální infrastruktury. Pozornost bude v první řadě věnována kybernetické bezpečnosti v odvětví energetiky, telekomunikací, dopravy a vesmíru. Kromě toho budou také vypracována cílená posouzení rizik v oblasti kybernetické bezpečnosti pro komunikační infrastrukturu a sítě v EU (včetně pevné a mobilní infrastruktury, satelitů, podmořských kabelů a internetového směrování)[[28]](#footnote-29). Pokud jde o ochranu kritické infrastruktury před hrozbami způsobenými člověkem, včetně hybridních hrozeb, návrh doporučení Rady o koordinovaném přístupu Unie za účelem posílení odolnosti kritické infrastruktury[[29]](#footnote-30) vyzývá členské státy, aby mimo jiné zajistily vhodné zátěžové testování a krizovou koordinaci. Námořní kritická infrastruktura, včetně ochrany podmořských datových kabelů, bude dále řešena prostřednictvím nadcházející revize Strategie EU pro námořní bezpečnost a jejího akčního plánu. Další opatření na posílení kybernetické bezpečnosti kritické infrastruktury v energetickém systému jsou stanovena v Akčním plánu EU pro digitalizaci energetického systému[[30]](#footnote-31).

Kosmické služby mají pro obranu stále větší význam, ať už se jedná o dohled, situační povědomí, přesné určování polohy nebo ultra zabezpečenou komunikaci. Pro technologickou suverenitu jsou proto klíčovými strategickými aktivy. Narušení kosmických služeb by mohlo mít velký dopad na obranné systémy a také na celou společnost a hospodářství. Jejich odolnost je pro celkovou odolnost kybernetické obrany klíčová, neboť mohou být terčem nepřátelských útoků. Jak je patrné z útoků na sítě KA-SAT, vesmírné systémy jsou stále více vystavovány kybernetickým hrozbám, které mohou narušit dostupnost nebo kontinuitu kosmických služeb. To představuje riziko pro strategické a bezpečnostní zájmy EU v oblasti vesmíru a také pro schopnosti v oblasti vesmíru, které umožňují kybernetickou obranu a napomáhají jí. Kosmická strategie EU pro bezpečnost a obranu oznámená ve Strategickém kompasu[[31]](#footnote-32) nastíní opatření ke zlepšení spolehlivosti a kybernetické odolnosti kosmických infrastruktur a souvisejících služeb a k odrazování od veškerých hrozeb pro citlivé kosmické systémy a služby v EU a reakci na ně, přičemž se bude zabývat konkrétně kybernetickými hrozbami.

Komise rovněž vyzývá členské státy, aby urychleně realizovaly opatření doporučená v souboru opatření EU pro kybernetickou bezpečnost sítí 5G[[32]](#footnote-33). Členské státy, které dosud nepřijaly omezení týkající se vysoce rizikových dodavatelů, by tak měly bezodkladně učinit vzhledem k tomu, že časová prodleva může zvýšit zranitelnost sítí v EU. Tato rizika mohou mít význam pro vojenské prostředky a mohou mít dopad na celkové obranné prostředí členských států.

Co se týče **kybernetické odolnosti evropského obranného průmyslu a subjektů pro výzkum a vývoj v oblasti obrany**, tyto subjekty spadají do oblasti působnosti směrnice o bezpečnosti sítí a informací 2, pokud je členské státy výslovně nevyloučí. To by vyžadovalo, aby tyto subjekty měly zaveden program řízení rizik v oblasti kybernetické bezpečnosti, který zahrnuje bezpečnost dodavatelského řetězce a také hlášení incidentů. Vzhledem k tomu, že soukromý sektor hraje významnou úlohu v poskytování služeb v oblasti kybernetické bezpečnosti v rámci obranného ekosystému, měly by členské státy dále využívat systémy certifikace v oblasti kybernetické bezpečnosti. Na základě zkušeností agentury ENISA by mohl být prozkoumán **systém certifikace v oblasti kybernetické bezpečnosti v EU pro společnosti poskytující služby obrannému průmyslu** jako způsob, jak na trh vnést harmonizovanou úroveň důvěry.

## 2.2 Zajištění interoperability kybernetické obrany EU a soudržnosti norem

Interoperabilita a shodnost jsou důležitými požadavky, které je třeba zvážit od fáze navrhování schopností v oblasti kybernetické obrany, a to rovněž s ohledem na poznatky získané během probíhajících misí a operací, které byly s podporou agentury EDA identifikovány pod vedením Vojenského štábu EU. Vodítkem pro rozvoj vnitrostátních schopností v oblasti kybernetické obrany k zajištění interoperability by měly být zásady, postupy a normy, které jsou dohodnuty v rámci Federated Mission Networking (FMN)[[33]](#footnote-34).

Úsilí o spolupráci lze usnadnit harmonizací požadavků na schopnosti v oblasti kybernetické obrany příští generace, což by případně mohlo vést ke společným iniciativám v oblasti rozvoje a zadávání veřejných zakázek a integrované podpoře životního cyklu. Z tohoto důvodu agentura EDA a Vojenský štáb EU vypracují **doporučení týkající se souboru požadavků EU na interoperabilitu v oblasti kybernetické obrany**. Tyto požadavky musí být brány v úvahu ve všech horizontech plánování, aby byly zaručeny všechny aspekty standardizace jako kritické podpůrné schopnosti pro interoperabilitu. Dalšími kritickými podpůrnými schopnostmi jsou požadavky na testování, hodnocení a certifikaci.

Harmonizované normy kybernetické bezpečnosti budou vypracovány pro hardwarové a softwarové produkty a součásti v souvislosti s navrhovaným aktem o kybernetické odolnosti[[34]](#footnote-35). Tyto normy se budou týkat všech civilních výrobků a výrobků dvojího užití s digitálními prvky, které tvoří velkou část výrobků používaných v odvětví obrany. Pokud to bude možné, bude Komise podporovat soudržnost s normami kybernetické bezpečnosti souvisejícími s obranou pro digitální produkty. Jak je stanoveno v Akčním plánu pro synergie mezi civilním, obranným a kosmickým průmyslem[[35]](#footnote-36) (dále jen „Akční plán pro synergie“), Komise v úzké spolupráci s klíčovými zúčastněnými stranami předloží plán na podporu využívání stávajících hybridních civilních/obranných norem a vytváření nových norem. Měla by se dále rozvíjet spolupráce mezi všemi příslušnými zúčastněnými stranami, včetně evropských normalizačních organizací, Organizace Severoatlantické smlouvy (NATO) a dalších partnerů, přičemž by se měl co nejlépe využít Evropský výbor pro obrannou standardizaci. V podobném duchu platí, že když vojenské standardizační orgány vytvářejí nové normy související s kybernetickou bezpečností pro výrobky s digitálními prvky pro použití v obraně, měly by být jako základ použity harmonizované normy vypracované v rámci aktu o kybernetické odolnosti[[36]](#footnote-37).

***Opatření v oblasti kybernetické obrany***

* Podporovat členské státy při vypracovávání právně nezávazných doporučení pro obrannou komunitu, inspirovaných směrnicí NIS 2, s cílem přispět ke zvýšení celkové vyspělosti v oblasti kybernetické obrany na vnitrostátní úrovni,
* vypracovat doporučení týkající se požadavků EU na interoperabilitu v oblasti kybernetické obrany,
* posílit spolupráci se všemi příslušnými subjekty v oblasti obranných standardů v rámci Evropského výboru pro obrannou standardizaci.

***Civilní podpůrná opatření***

* Vypracovat rizikové scénáře pro kritickou infrastrukturu, která je důležitá pro vojenskou komunikaci a mobilitu, s cílem zaměřit se na opatření v oblasti připravenosti, a to i prostřednictvím penetračního testování,
* podporovat při vypracovávání harmonizovaných norem pro výrobky dvojího užití spolupráci mezi civilními a vojenskými standardizačními orgány.

**3. Investice do schopností v oblasti kybernetické obrany**

V posledních letech se investice do kybernetické obrany v EU zvýšily v souvislosti s rostoucí nepřátelskou kybernetickou činností státních a nestátních subjektů. Je zásadní, aby EU posílila své schopnosti v oblasti kybernetické obrany. Ruská útočná válka proti Ukrajině dále zvyšuje potřebu větších investic, aby se zajistilo, že členské státy budou mít v oblasti kybernetické obrany nejmodernější schopnosti, a to stacionární i připravené k nasazení.

Technologická vylepšení jsou nezbytná k zachování výhody oproti konkurentům a protivníkům, kteří do nových technologií také masivně investují. Proto musí EU a členské státy rovněž posílit svou spolupráci a interoperabilitu v oblasti kybernetické obrany prostřednictvím společného rozvoje schopností a zvýšených investic do výzkumu a vývoje.

Kromě toho jetřeba zabývat se zranitelnými místy vyplývajícími ze strategické závislosti a roztříštěnosti evropské technologické a průmyslové základny obrany[[37]](#footnote-38). K překonání strategické závislosti v oblasti kybernetické bezpečnosti a kybernetické obrany v Evropě jsou nezbytné zejména dovednosti a schopnosti. Evropský obranný průmysl si musí zachovat klíčové dovednosti a získat nové dovednosti, aby mohl i nadále poskytovat technologicky vyspělá řešení v celosvětovém měřítku[[38]](#footnote-39). Nedostatek dovedností má na odvětví obrany negativní dopad, neboť brání rozvoji schopností ve všech oblastech. Všechna opatření budou plně v souladu s přístupy oznámenými v Akčním plánu pro synergie, v Plánu pro technologie s kritickým významem pro obranu a bezpečnost (dále jen „Plán pro kritické technologie“)[[39]](#footnote-40) a v analýze nedostatků[[40]](#footnote-41).

## 3.1 Rozvoj nejmodernějších schopností v oblasti komplexní kybernetické obrany

Členské státy nesou odpovědnost a mají pravomoc využívat schopnosti v oblasti kybernetické obrany, zatímco EU hraje důležitou úlohu při podpoře dalšího rozvoje specifických vojenských schopností v rámci metodologie Doktríny, organizace, výcvik, technika, personál, velení, infrastruktura a interoperabilita (DOTMLPF-I) za účelem nastolení svobody jednání v kybernetickém prostoru. Je třeba ještě více sjednotit přístup ke kybernetické obraně ve všech oblastech schopností a přizpůsobit jej měnícímu se geopolitickému prostředí. Proto je nezbytné určit chybějící prvky u stávajících schopností a koordinovaně a měřitelně podporovat rozvoj nových schopností.

Úroveň zapojení členských států do projektů spolupráce v oblasti rozvoje kybernetické obrany je však prozatím nedostatečná a měla by být zvýšena, aby se maximalizoval dopad na úrovni EU. Všechny členské státy musí zvýšit své investice do rozvoje schopností v oblasti komplexní kybernetické obrany a rozvíjet je ve spolupráci s ostatními. Členské státy by měly zvážit **vypracování souboru dobrovolných závazků pro rozvoj vnitrostátních schopností v oblasti kybernetické obrany**, a to i nadnárodních schopností nad rámec stávajících projektů PESCO v oblasti kybernetické obrany[[41]](#footnote-42). K zahájení dialogu s členskými státy o požadavcích na kybernetickou obranu a vnitrostátních cílech pro rozvoj schopností v oblasti kybernetické obrany a k posouzení provádění závazků by mohl být využit proces koordinovaného každoročního přezkumu v oblasti obrany (dále jen „CARD“). Komise prostřednictvím Evropského obranného fondu podporuje a spolufinancuje rozvoj a výzkum schopností v oblasti komplexní kybernetické obrany, včetně aktivních obranných schopností. Komise již zvýšila investice do kybernetické obrany prostřednictvím Evropského obranného fondu, což by mělo vést k rozvoji společných a/nebo interoperabilních evropských nástrojů pro operace a řešení incidentů v kyberprostoru, obranné operace a preventivní opatření v oblasti informační války a ke zlepšení odolnosti komunikačních a informačních systémů. Zaměřuje se na oblasti, jako jsou kybernetické situační povědomí, vyhledávání hrozeb v reálném čase a schopnosti responzivních operací, schopnosti kybernetických operací a kybernetický výcvik a cvičení[[42]](#footnote-43). Aby se zajistilo, že členské státy budou schopny provádět společné kybernetické operace, budou v nadcházejících letech v rámci Evropského obranného fondu podporovány schopnosti responzivních operací a kybernetických operací. Členské státy se rovněž vyzývají, aby se aktivně zapojily do různých rámců spolupráce a používaly všechny nástroje vytvořené na úrovni EU, včetně projektového týmu agentury EDA pro kybernetickou obranu[[43]](#footnote-44).

Probíhající revize priorit rozvoje schopností EU z roku 2018[[44]](#footnote-45) představuje vhodnou příležitost k vymezení aktualizovaných priorit pro rozvoj spolupráce, což tento nárůst rozvoje schopností spolupráce umožní. Přezkum zvláštní priority v oblasti kybernetické obrany by měl zohlednit výsledky přezkumu CARD 2022 a také zjištění analýzy nedostatků předložené členským státům v květnu 2022. Přezkum CARD následně nabídne pravidelný rámec pro přezkum pokroku při provádění této aktualizované priority na vnitrostátní úrovni a pro prozkoumání nových možností pro společný rozvoj schopností v oblasti kybernetické obrany s členskými státy. Aktualizované priority rozvoje schopností EU budou sloužit jako klíčový referenční bod pro projekty PESCO v oblasti kybernetické obrany.

V tomto ohledu vypracuje Vojenský štáb EU na základě pověření Vojenského výboru EU a v úzké koordinaci s členskými státy plán provádění operací v kybernetické oblasti s cílem poskytnout přehled o aktuálním stavu provádění schopností v oblasti kybernetické obrany a poskytnout podporu členským státům, aby lépe sladily své úsilí a činnosti. Toto úsilí je založeno na koncepci kybernetické obrany EU pro vojenské operace a mise pod vedením EU, která odráží nastavení priorit plánu rozvoje schopností.

**Posílení výzkumného úsilí v oblasti klíčových technologií pro kybernetickou obranu**

Udržení nejmodernějších schopností v oblasti kybernetické obrany vyžaduje, aby byl udržen krok s technologickým vývojem a jeho použitím v systémech souvisejících s obranou, zejména se vznikajícími a přelomovými technologiemi (např. umělá inteligence, šifrování a kvantová výpočetní technika)[[45]](#footnote-46). Aby EU zajistila, že její obranné systémy zůstanou bezpečné, musí investovat zejména do postkvantové kryptografie. Vzhledem k rychlému tempu rozvoje technologie je třeba přizpůsobit úsilí o společný výzkum a technologický rozvoj s cílem dosáhnout dostatečně pokročilé úrovně technologické připravenosti, aby bylo možné jejich výsledky rychleji začlenit do stávajících a budoucích schopností.

Komise v rámci Evropského obranného fondu financuje technologické inovace v oblasti obrany a podporuje rozvoj vznikajících, přelomových a také nejmodernějších technologií, a to i v oblasti kybernetické obrany. Až 8 % rozpočtu Evropského obranného fondu je vyčleněno na témata zabývající se přelomovými technologiemi pro obranu, včetně některých témat souvisejících s kybernetickou obranou. Zvláštní pozornost bude v nadcházejících letech v rámci Evropského obranného fondu věnována výzkumným akcím a projektům zaměřeným na nové technologie vyvinuté pro boj proti nově vznikajícím a vyvíjejícím se hrozbám, jakož i na zvýšení odolnosti, kybernetické bezpečnosti a jejich začlenění do obranných schopností.

V souladu s Akčním plánem pro vznikající a přelomové technologie[[46]](#footnote-47) bude agentura EDA každoročně informovat členské státy o situaci v oblasti vznikajících technologií, včetně těch, které se vztahují na kybernetickou obranu. Kromě toho agentura EDA vypracuje strategické posouzení evropských vznikajících a přelomových technologií s cílem podpořit členské státy při provádění dlouhodobého strategického řízení a při určování synergií a příležitostí ke spolupráci. Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC) přijme strategickou agendu pro investice do klíčových oblastí kybernetické bezpečnosti, která bude vodítkem pro přípravu budoucích pracovních programů v rámci programů Digitální Evropa a Horizont Evropa v souvislosti s kybernetickou bezpečností, a to na podporu výzkumu, inovací a uvádění na trh. V zájmu podpory součinnosti centrum ECCC a agentura EDA rovněž vypracují pracovní ujednání, které usnadní sdílení informací mezi příslušnými pracovníky o prioritách v oblasti civilních technologií, technologií dvojího užití a obranných technologií.

**Jednání na základě technologických potřeb v oblasti kybernetické obrany**

Je třeba dalších opatření a koordinace, aby se zajistilo, že rychlý technologický vývoj v kybernetické oblasti bude rychle převzat odvětvím obrany. To zahrnuje zintenzivnění úsilí o identifikaci kritických technologií pro kybernetickou obranu a kybernetickou bezpečnost, které by měly být upřednostňovány, aby se snížila technologická závislost EU a aby se posoudilo, zda stávající nástroje stanovování priorit a financování tyto závislosti řeší dostatečně.

Za tímto účelem Komise spolu s agenturou EDA a členskými státy navrhne v roce 2023 **technologický plán pro kritické kybernetické technologie** založený na příslušných konzultacích, případně i konzultacích s odvětvím. Tento technologický plán určí kybernetické technologie důležité pro technologickou suverenitu EU, bude zahrnovat kybernetickou obranu i kybernetickou bezpečnost, zmapuje technologický vývoj a strategickou závislost a bude usilovat o její snížení. Plán pro kybernetické technologie bude sloužit jako základ strategických priorit pro nástroje financování EU a navrhne plné využití programů civilního a obranného výzkumu a vývoje a rozvoje schopností a nástrojů financování v souladu s příslušnými pravidly řízení. Navrhne rovněž další způsoby, jak podpořit rozvoj výzkumu, technologického rozvoje a inovací dvojího užití v oblasti kybernetické bezpečnosti a kybernetické obrany na úrovni EU a členských států.

V této souvislosti Komise[[47]](#footnote-48) ve spolupráci s centrem ECCC a agenturou EDA v roce 2023 posoudí technologie, které již byly označeny za kritické pro kybernetickou obranu, a případně s podporou Observatoře pro kritické technologie zmapuje a dále určí stávající závislosti[[48]](#footnote-49). Přitom se zohlední práce vykonaná v souvislosti s výročním dokumentem agentury EDA o monitorování[[49]](#footnote-50) a strategickým posouzením evropských vznikajících a přelomových technologií[[50]](#footnote-51). Kromě toho by centrum ECCC mohlo zahájit specializovaný projekt na podporu politiky, který by mohl přispět k procesu technologického plánování a spojit a zapojit příslušné zúčastněné strany z civilní a vojenské sféry.

V rámci činností nastíněných v Akčním plánu pro synergie, Plánu pro kritické technologie a analýze nedostatků již probíhá několik opatření k posílení synergií s cílem lépe využít plný potenciál technologií dvojího užití, a to také v kybernetické oblasti.

Kromě toho se členské státy vybízejí, aby plně využívaly stávajících iniciativ na podporu výzkumu a technologického rozvoje, konkrétně v oblasti obrany se jedná o skupiny agentury EDA pro technologie obranných schopností[[51]](#footnote-52) a související technologické stavební bloky v rámci zastřešujícího strategického plánu výzkumu (OSRA)[[52]](#footnote-53), *ad hoc* rámec agentury EDA[[53]](#footnote-54), Evropský obranný fond a projekt PESCO. Pokud jde o civilní technologie a technologie dvojího užití, mohou centrum ECCC a síť řídit projekty s obranným i civilním rozměrem, jak je stanoveno v jejich právním základu[[54]](#footnote-55). Jak bylo oznámeno v Akčním plánu pro synergie a v Plánu pro kritické technologie, Komise bude rovněž usilovat o posílení součinnosti mezi činnostmi centra ECCC a Evropského obranného fondu v oblasti kybernetické bezpečnosti a kybernetické obrany v souladu s pravidly řízení Evropského obranného fondu.

## 3.2 Agilní, konkurenceschopný a inovativní evropský obranný průmysl

EU potřebuje silný, agilní, konkurenceschopný a inovativní evropský obranný průmysl, který je schopen poskytovat celé spektrum nejmodernějších obranných schopností, včetně schopností v oblasti kybernetické obrany. Co se však týče kybernetické obrany, spoléhá se obranný průmysl EU v současné době do velké míry na civilní řešení a na vnější trhy, které poskytují nejmodernější řešení. Přestože technologický pokrok v civilní oblasti je rychlý a trh s civilními informačními produkty a produkty kybernetické bezpečnosti roste rychle, existují specifické vojenské požadavky, které dostupné civilní produkty nesplňují. Důležité části hardwaru a softwaru, které se v současné době používají pro kybernetickou obranu, se v EU nevyrábějí, což může vytvářet průmyslovou a technologickou závislost. EU také postrádá silné zastoupení v celosvětovém odvětví kybernetické bezpečnosti a kybernetické obrany. Její vysoce roztříštěná **evropská technologická a průmyslová základna obrany** značně snižuje její schopnost zlepšit konkurenceschopnost[[55]](#footnote-56), přičemž většinu společností v oblasti kybernetické bezpečnosti v EU tvoří malé a střední podniky[[56]](#footnote-57). Základem schopnosti EU jednat je technologicky suverénní průmyslová kapacita.

EU podporuje rozvoj silné evropské technologické a průmyslové základny obrany prostřednictvím řady programů a iniciativ. Zatímco Evropský obranný fond financuje technologické inovace v oblasti obrany a podporuje rozvoj technologií, které v konečném důsledku vedou ke společnému rozvoji nejmodernějších vojenských schopností a přispívají ke konkurenceschopnosti obranného průmyslu EU, program Horizont Evropa a program Digitální Evropa podporují výzkum v oblasti kybernetické bezpečnosti a rozvoj technologií dvojího užití, včetně kvantové technologie, šifrování, zabezpečeného cloudu a umělé inteligence[[57]](#footnote-58).

Měla by být přijata další opatření související s kritickými technologiemi pro potřeby kybernetické obrany a průmyslu, která jsou stanovená v **technologickém plánu pro kritické kybernetické technologie**. Je nezbytné určit vhodné podpůrné toky, například s cílem stimulovat společné úsilí v oblasti zadávání veřejných zakázek, mimo jiné prostřednictvím budoucího Evropského programu investic do obrany, nebo usnadnit přístup ke kapitálu a půjčkám prostřednictvím Evropského investičního fondu a Evropské investiční banky.

V zájmu silné evropské technologické a průmyslové základny obrany je nutné zajistit využívání a zvyšování účinku synergií mezi civilními společnostmi a podniky působícími v oblasti obrany. Inovační opatření navrhovaná v rámci Programu EU pro obranné inovace (EUDIS), včetně oslovení malých a středních podniků a technologického skautingu, by mohla mít na obranný průmysl EU a evropskou technologickou a průmyslovou základnu obrany pozitivní dopad.

Komise rovněž zahájí odvětvový dialog s cílem rozvíjet odvětví kybernetické obrany EU, do něhož bude případně zapojena agentura EDA.

Komise a vysoký představitel navrhují zavést několik opatření, jež mají zajistit, aby bylo odvětví připraveno na plnění cílů v krátkodobém i dlouhodobém horizontu. Jejich plnění v nejbližší době vyžaduje důkladné zmapování výrobních kapacit EU v oblasti obranného průmyslu, aby bylo možné přesně určit nedostatky a oblasti, v nichž je zapotřebí zvýšení kapacity.

Snížení kritických závislostí v oblasti kybernetiky, na něž mohlo být poukázáno v technologických plánech, by mohl řešit rovněž nový Fond pro evropskou suverenitu, který oznámila předsedkyně von der Leyenová ve svém projevu o stavu Unie v září 2022.

Rámec EU pro prověřování přímých zahraničních investic se bude i nadále používat ke zmírňování rizik akvizic evropských technologií nebo řešení, které představují rizika pro obranu a bezpečnost. Členské státy, které vnitrostátní mechanismy prověřování dosud nezavedly, by tak měly neprodleně učinit.

## 3.3 Pracovní síla EU v oblasti kybernetické obrany

Evropa čelí skutečnému a alarmujícímu nedostatku kybernetických dovedností, přičemž Evropská organizace pro kybernetickou bezpečnost (ECSO) odhaduje, že již nyní v roce 2022 je zapotřebí celkem 500 000 odborníků. Tento nedostatek dovedností zhoršuje schopnost EU vyvíjet nové technologie a bránit naši kritickou infrastrukturu. V případě vládních subjektů, jako jsou ministerstva obrany a armáda, silná konkurence v oblasti dovedností a atraktivní platy nabízené soukromým sektorem dále zhoršují obtíže spojené s přilákáním a udržením talentů v oblasti kybernetiky.

V souvislosti s Evropským rokem dovedností 2023 **zahájí Komise iniciativu pro Akademii kybernetických dovedností.** Bude se jednat o zastřešující iniciativu, jejímž cílem je zvýšit počet odborníků vyškolených v oblasti kybernetické bezpečnosti. Sjednotí mnoho různých iniciativ v oblasti kybernetických dovedností a zajistí u nich koordinaci, integraci a společnou komunikaci. Akademie kybernetických dovedností, která je organizována na základě několika pilířů činnosti, k nimž patří financování, komunitní podpora, odborná příprava a certifikace, zapojení zúčastněných stran a získávání znalostí, bude rovněž přínosem pro pracovníky v oblasti kybernetické obrany. Evropská bezpečnostní a obranná škola (EBOŠ) prozkoumá, jak usnadnit výměnu osvědčených postupů a další součinnost mezi vojenskou a civilní oblastí, pokud jde o odbornou přípravu a rozvoj vojenských dovedností specifických pro kybernetický prostor.

Na základě analýzy požadavků na odbornou přípravu EU a potřeb odborné přípravy budou škola EBOŠ, agentura EDA a členské státy dále rozvíjet a organizovat činnosti a cvičení v oblasti kybernetické obrany pro orgány EU, operace a mise v rámci společné bezpečnostní a obranné politiky, jakož i pro úředníky členských států. Rovněž bude prozkoumán další **rozvoj platformy EBOŠ pro vzdělávání, odbornou přípravu, hodnocení a cvičení v oblasti kybernetické bezpečnosti**, aby se vytvořilo více kapacit pro odbornou přípravu. Tento rozvoj by měl rovněž zahrnovat kurzy odborné přípravy pro konkrétní operační oblast a operace ve více oblastech. Zejména by se mělo usilovat o součinnost s projektem Akademického a inovačního střediska EU pro kybernetickou oblast (EU CAIH) v rámci PESCO[[58]](#footnote-59).

Členské státy se vyzývají k vypracování specifických vzdělávacích programů v oblasti kybernetické obrany, zapojení vysokoškolských a akademických institucí (civilních a vojenských) do rozvoje a vytváření společných osnov kybernetické obrany, sdílení osvědčených postupů, vytváření partnerství a společných projektů a usnadňování výměn školitelů a stážistů. V zájmu zajištění interoperability a společné kultury v celé EU bude škola EBOŠ podporovat výměnu mezi členskými státy prostřednictvím platformy pro vzdělávání, odbornou přípravu, hodnocení a cvičení v oblasti kybernetické bezpečnosti.

Členské státy by měly posílit širší spolupráci mezi subjekty působícími v oblasti odborné přípravy a vzdělávání a spojit civilní a vojenské aspekty v technické, operativní, strategické a právní oblasti, a vytvořit tak základ pro vypracování společných a standardizovaných programů odborné přípravy na různých úrovních pro komunity působící v civilní sféře, v oblasti prosazování práva, v diplomatické oblasti a v oblasti kybernetické obrany. Kromě toho by členské státy měly spolupracovat s evropskými poskytovateli odborné přípravy v soukromém sektoru a s akademickými institucemi s cílem zvýšit úroveň schopností a dovedností personálu ve vojenských misích a operacích v rámci SBOP.

Dále by měla být podporována spolupráce mezi členskými státy, orgány, institucemi a jinými subjekty EU, mezinárodními partnery a dalšími subjekty, včetně soukromého sektoru a akademické obce, v oblasti norem a certifikace odborné přípravy v oblasti kybernetické obrany. Škola EBOŠ na základě stávajících civilních iniciativ, jako je evropský rámec dovedností v oblasti kybernetické bezpečnosti (ECSF), který vyvinula agentura ENISA, vypracuje rámec pro certifikaci dovedností v oblasti kybernetické obrany. Komise by rovněž zvážila přístupy k certifikaci kybernetických dovedností, které jsou k dispozici na trhu a od akademické obce, a zároveň by se snažila prostřednictvím Akademie kybernetických dovedností stimulovat součinnost mezi těmito přístupy a odstranit nedostatky, zejména cíleným financováním z EU.

***Opatření v oblasti kybernetické obrany***

* Vypracovat strategické posouzení vznikajících a přelomových technologií na podporu dlouhodobých strategických investičních rozhodnutí,
* vypracovat technologický plán pro kritické kybernetické technologie pro EU, který by zahrnoval kritické technologie pro kybernetickou obranu a kybernetickou bezpečnost s cílem posoudit míru závislosti,
* navrhnout způsoby, jak snížit závislost s využitím všech nástrojů EU, včetně programu Digitální Evropa, programu Horizont Evropa a Evropského obranného fondu, a předvídat technologický rozvoj s cílem zvýšit technologickou suverenitu a zajistit schopnost jednat,
* podpořit rozvoj rámce pro certifikaci dovedností v oblasti kybernetické obrany,
* vypracovat cvičení EU v oblasti kybernetické obrany a prozkoumat, jak lze dále rozvíjet platformu pro vzdělávání, odbornou přípravu, hodnocení a cvičení v oblasti kybernetické bezpečnosti v rámci školy EBOŠ, aby se vytvořilo více kapacit pro odbornou přípravu.

***Civilní podpůrná opatření***

* Zřídit akademii EU v oblasti kybernetických dovedností s ohledem na potřeby specifických dovedností pro různé profesní profily a odvětví činnosti, včetně pracovních sil v oblasti obrany,
* analyzovat přístupy k certifikaci kybernetických dovedností a zároveň se snažit podporovat součinnost a odstranit nedostatky, mimo jiné prostřednictvím financování EU.

**4. Partner pro řešení společných výzev**

Přínosem pro partnery bude schopnější a odolnější EU v kybernetickém prostoru, jakož i pomoc EU v oblasti kybernetické obrany a budování kapacit poskytované prostřednictvím příslušných nástrojů EU. EU bude usilovat o vytvoření přizpůsobených partnerství v oblasti kybernetické obrany tam, kde jsou vzájemně výhodná. Partnerství v oblasti kybernetické obrany budou rovněž řešena v souvislosti s účastí partnerských zemí na vojenských misích a operacích v rámci SBOP.

Tato činnost bude případně vycházet ze stávajících dialogů v oblasti kybernetiky, jakož i z dialogů o bezpečnosti a obraně. Vysoký představitel bude rovněž zkoumat synergie mezi **neformální sítí EU pro kybernetickou diplomacii a sítí atašé pro obranu v delegacích EU.**

***4.1 Spolupráce s NATO***

Strategické partnerství EU s NATO má pro euroatlantickou bezpečnost i nadále zásadní význam, jak zdůrazňuje Strategický kompas a Strategická koncepce NATO pro rok 2022[[59]](#footnote-60). EU je i nadále plně odhodlána toto klíčové partnerství posilovat, a to i v oblasti kybernetické obrany, přičemž k rozvoji sdílených řešení společných hrozeb a výzev je třeba podniknout další kroky. V souladu se společnými prohlášeními z Varšavy a Bruselu o spolupráci mezi EU a NATO[[60]](#footnote-61) a na základě zásad transparentnosti, reciprocity a inkluzivnosti, otevřenosti a rozhodovací samostatnosti obou organizací představují kybernetická bezpečnost a kybernetická obrana jednu z klíčových prioritních oblastí spolupráce EU.

Na základě reciprocity si bude EU i nadále s NATO vyměňovat informace o vojenském koncepčním rámci týkajícím se začlenění aspektů kybernetické obrany do plánování a provádění vojenských misí a operací v rámci SBOP. EU bude v maximální možné míře usilovat o kompatibilitu s koncepcemi NATO a doktrínou o kybernetické obraně.

Vzhledem k vysoké poptávce po schopnostech v oblasti kybernetické obrany bude EU podporovat součinnost a doplňkovost s NATO napříč organizačními a státními hranicemi. EU bude s NATO spolupracovat na posílení technické a procedurální interoperability schopností v oblasti kybernetické obrany, včetně rozvoje schopností v souladu s iniciativou FMN. To připraví půdu pro potenciální vzájemně se podporující rozvoj a využití schopností v oblasti kybernetické obrany. Zvláštní pozornost by měla být věnována interoperabilitě norem, která přispívá ke kybernetické odolnosti a interoperabilitě vojenských komunikačních a informačních systémů, a to případně zapojením průmyslu.

V zájmu zajištění souladu odborné přípravy příslušných pracovníků v oblasti kybernetické obrany bude EU v příslušných případech rovněž posilovat spolupráci s NATO, pokud jde o harmonizaci potřeb v oblasti odborné přípravy a analýzu požadavků a vypracovávání společných osnov, kurzů a cvičení. Na základě zásad reciprocity a nediskriminace otevře škola EBOŠ své kurzy odborné přípravy v oblasti kybernetické obrany zaměstnancům NATO a zřídí platformu pro propagaci společných kurzů. EU bude rovněž podporovat účast zaměstnanců NATO na kybernetických cvičeních a cvičeních pro řešení krizí s kybernetickými prvky.

EU a NATO se rovněž zapojí do dalšího zlepšování vzájemného situačního povědomí a prozkoumají způsoby koordinace, mimo jiné posílením spolupráce mezi složkou NATO pro schopnost reakce na počítačové incidenty a týmem CERT-EU. V zájmu podpory spolupráce v oblasti kybernetických aspektů a dopadů řešení krizí a reakce na ně bude EU přispívat k výměně pracovníků v souvislosti s vojenskými, civilními a společnými iniciativami a případně k rozvoji možných synergií příslušných rámců a iniciativ pro řešení krizí, a to i v případě rozsáhlých incidentů. S cílem zajistit vzájemnou doplňkovost a zamezit zbytečnému zdvojování úsilí bude EU usilovat o užší spolupráci a výměnu informací s NATO v oblasti budování kapacit kybernetické obrany v partnerských zemích.

***4.2 Spolupráce s podobně smýšlejícími partnery***

Vysoký představitel bude otázky kybernetické obrany systematičtěji zahrnovat do stávajících a budoucích dialogů s partnery v oblasti kybernetiky a také bezpečnosti a obrany. Vzhledem k tomu, že se aspekty kybernetické obrany budou rozvíjet ve dvoustranných dialozích, rozšíří se možnosti zavedení otázek kybernetické obrany do dalších forem spolupráce s partnery EU.

Strategické partnerství EU se **Spojenými státy** bude pokračovat v prohlubování spolupráce v oblasti bezpečnosti a obrany vzájemně prospěšným způsobem, mimo jiné prostřednictvím strukturované výměny informací o situačním povědomí. Silné transatlantické partnerství potvrzují pravidelné dialogy v oblasti kybernetiky, bezpečnosti a obrany mezi EU a USA. Vysoký představitel do těchto dialogů v případně zahrne příslušné aspekty kybernetické obrany.

Spolu se svými mezinárodními partnery bude EU **Ukrajinu** i nadále podporovat, a to i prostřednictvím kybernetického dialogu. Vzhledem ke zkušenostem Ukrajiny s budováním kapacit v oblasti kybernetické odolnosti a kybernetické obrany je společným zájmem výměna osvědčených postupů v oblasti kybernetické obrany, včetně informací o typech ohrožení a situačním povědomí, jakož i o příslušném vývoji politik, která bude pokračovat a bude se rozšiřovat.

Podobně smýšlející partneři hrají důležitou úlohu při udržování globálního, otevřeného, stabilního a bezpečného kyberprostoru a mohou posílit schopnost EU předcházet nepřátelskému chování v kyberprostoru, odrazovat a odstrašovat od něj a reagovat na něj. EU je i nadále otevřena široké, ambiciózní a vzájemně prospěšné spolupráci v oblasti bezpečnosti a obrany, včetně kybernetické obrany, se všemi podobně smýšlejícími partnery.

***4.3 Podpora při budování kapacit v oblasti kybernetické obrany pro partnerské země***

Globální a regionální výzvy zvýšily vzájemnou závislost mezi EU a jejími partnery a zdůraznily potřebu navázat užší partnerství v oblasti bezpečnosti a obrany. To je obzvláště důležité pro kandidátské země EU. Nedávné rozsáhlé kybernetické útoky naznačují potřebu většího zapojení a partnerství EU v oblasti kybernetické bezpečnosti a kybernetické obrany, a to na základě stávajících programů. Vzhledem k nadnárodní povaze kybernetických hrozeb přispěje posílení kybernetické odolnosti partnerských zemí, zejména zemí s nižší úrovní kybernetické vyspělosti, k bezpečnějšímu a lépe chráněnému kybernetickému prostoru. EU by tak byla lépe schopna kybernetickým útokům předcházet, odhalovat je, bránit se před nimi a odrazovat od nich.EU posílí bezpečnostní a obrannou spolupráci s partnerskými zeměmi s cílem posílit jejich kybernetickou odolnost, a to i prostřednictvím stávajících dialogů. Ve vhodných a vzájemně prospěšných případech bude EU spolupracovat s partnery, a zejména s těmi kandidátskými zeměmi EU, které jsou v souladu se společnou zahraniční a bezpečnostní politikou EU a se společnou bezpečnostní a obrannou politikou EU, při jejich úsilí o budování kapacit v oblasti kybernetické obrany. Tato spolupráce by mohla zahrnovat podporu politických a legislativních rámců, výcvik, poradenství, odborné vedení a vybavení ozbrojených sil a bezpečnostních sil partnerů. Členské státy by se mohly rozhodnout, že partnerům poskytnou operativní pomoc v oblasti kybernetické obrany. Kromě toho bude EU pomáhat partnerům posilovat jejich schopnost přispívat k vojenským misím a operacím v rámci SBOP, neboť se jedná o cenný příspěvek ke společnému úsilí o podporu míru a bezpečnosti.

Evropský mírový nástroj (EPF) bude i nadále podporovat úsilí EU o pomoc při budování obranných kapacit, včetně kybernetické obrany, v partnerských zemích, zejména v sousedství EU, a bude doplňovat úsilí SBOP v oblasti řešení krizí. V tomto ohledu bude EU v případě potřeby také lépe propojovat pomoc v oblasti kybernetické obrany s budováním civilních kapacit v oblasti kybernetické bezpečnosti, zejména prostřednictvím Sboru EU pro budování kybernetických kapacit. Pro dosažení úspěchu opatření při budování kapacit v oblasti kybernetické obrany a kybernetické bezpečnosti bude nezbytná účinná koordinace mezi příslušnými programy a nástroji EU, včetně Evropského mírového nástroje, a členskými státy.

Při poskytování podpory partnerským zemím v jejich úsilí o budování kapacit v oblasti kybernetické obrany bude EU úzce spolupracovat s ostatními dárci na rozvoji platforem pro zvyšování situačního povědomí a koordinaci s cílem poskytovat co nejlepší cílenou podporu a zajistit soudržnost a nezdvojování úsilí.

***Opatření v oblasti kybernetické obrany***

* Posílit spolupráci mezi EU a NATO v oblasti odborné přípravy, vzdělávání, situačního povědomí a cvičení v oblasti kybernetické obrany,
* zahrnout do dialogů s partnerskými zeměmi vedených EU v oblasti kybernetiky a také bezpečnosti a obrany témata kybernetické obrany,
* spolupracovat s podobně smýšlejícími zeměmi, a to i v souvislosti s rozvojem schopností v oblasti kybernetické obrany a kybernetickou odolností,
* zintenzivnit pomoc poskytovanou partnerům při rozvoji schopností v oblasti kybernetické obrany, mimo jiné prostřednictvím Evropského mírového nástroje (EPF), zejména v sousedství EU a na podporu kandidátských zemí EU.

***Civilní podpůrná opatření***

* Posílit spolupráci mezi EU a NATO v oblasti kybernetické bezpečnosti, pokud jde o situační povědomí, reakci na krize, ochranu kritické infrastruktury a standardizaci a certifikaci.

# III. ZÁVĚR

Vysoký představitel, rovněž ve funkci vedoucího agentury EDA, a Komise vyzývají členské státy, aby vypracovaly příslušné aspekty této politiky kybernetické obrany, a budou s členskými státy spolupracovat na určení praktických prováděcích opatření. Ve spolupráci s členskými státy by mohl být stanoven prováděcí plán. Výsledky provádění politiky kybernetické obrany EU přispějí k celkovým cílům Strategie kybernetické bezpečnosti EU i Strategického kompasu.

Za účelem sledování a hodnocení pokroku při provádění politiky kybernetické obrany bude Radě předložena výroční zpráva. Členské státy se vyzývají, aby přispěly svými poznatky o pokroku v provádění opatření, která probíhají na vnitrostátní úrovni nebo v rámci spolupráce.

1. Aktualizace politického rámce EU pro kybernetickou obranu z roku 2018, 19. listopadu 2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/cs/pdf [↑](#footnote-ref-2)
2. [Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti.](https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/cs/pdf) [↑](#footnote-ref-3)
3. Strategie kybernetické bezpečnosti EU pro digitální dekádu, [JOIN(2020) 18 final](https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=JOIN:2020:18:FIN). [↑](#footnote-ref-4)
4. https://ec.europa.eu/commission/presscorner/detail/cs/SPEECH\_21\_4701 [↑](#footnote-ref-5)
5. [9364/22](https://www.consilium.europa.eu/media/56358/st09364-en22.pdf) [↑](#footnote-ref-6)
6. [JOIN(2022) 24 final](https://ec.europa.eu/info/sites/default/files/join_2022_24_2_en_act_part1_v3_1.pdf). [↑](#footnote-ref-7)
7. EEAS(2021) 706 REV4. [↑](#footnote-ref-8)
8. Kybernetické komunity působící v civilní sféře, v diplomatické oblasti a v oblasti vymáhání práva. [↑](#footnote-ref-9)
9. Týmy rychlé kybernetické reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti. [↑](#footnote-ref-10)
10. Smlouva o Evropské unii, konsolidované znění: Úř. věst. C 326, 26.10.2012, s. 1. [↑](#footnote-ref-11)
11. Smlouva o fungování Evropské unie, konsolidované znění: Úř. věst. C 326, 26.10.2012, s. 1. [↑](#footnote-ref-12)
12. Cílem projektu je vytvořit, zřídit a provozovat nadnárodní Koordinační středisko pro kybernetický a informační prostor (CIDCC) jako stálý nadnárodní vojenský prvek. [↑](#footnote-ref-13)
13. V návaznosti na první dvě zasedání strategických konferencí evropských velitelů v kybernetické oblasti (CyberCo) v lednu a červnu 2022 se velitelé EU v kybernetické oblasti rozhodli zřídit na své úrovni trvalejší fórum. [↑](#footnote-ref-14)
14. Neformální skupina zahrnující příslušné útvary Komise, ESVČ, Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA), tým CERT-EU a Europol, které společně předsedá Komise a vysoký představitel. [↑](#footnote-ref-15)
15. Strategie kybernetické bezpečnosti EU pro digitální dekádu (JOIN(2020) 18 final) a Strategie bezpečnostní unie EU (COM(2020) 605). [↑](#footnote-ref-16)
16. V souladu s nařízením Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240 (Úř. věst. L 166, 11.5.2021, s. 1), s výhradou možných změn. [↑](#footnote-ref-17)
17. [Výzva z Nevers k posílení kapacit EU v oblasti kybernetické bezpečnosti](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/). [↑](#footnote-ref-18)
18. https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx [↑](#footnote-ref-19)
19. https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/ [↑](#footnote-ref-20)
20. Závěry Rady o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“). [↑](#footnote-ref-21)
21. https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/ [↑](#footnote-ref-22)
22. https://english.ncsc.nl/topics/log4j-vulnerability [↑](#footnote-ref-23)
23. Prohlášení vysokého představitele jménem Evropské unie k nepřátelské kybernetické činnosti prováděné hackery a hackerskými skupinami v souvislosti s agresí Ruska vůči Ukrajině: https://www.consilium.europa.eu/cs/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/ [↑](#footnote-ref-24)
24. Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148, která byla nedávno schválena spolunormotvůrci a měla by být formálně přijata do konce tohoto roku. [↑](#footnote-ref-25)
25. Návrh nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, [COM(2022) 454 final](https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52022PC0454). [↑](#footnote-ref-26)
26. Závěry Rady o rozvoji kybernetické pozice Evropské unie, ST09364/22, 23. května 2022. [↑](#footnote-ref-27)
27. https://digital-strategy.ec.europa.eu/cs/policies/nis-cooperation-group [↑](#footnote-ref-28)
28. [Výzva z Nevers k posílení kapacit EU v oblasti kybernetické bezpečnosti](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/). [↑](#footnote-ref-29)
29. Návrh DOPORUČENÍ RADY o koordinovaném přístupu Unie za účelem posílení odolnosti kritické infrastruktury, [COM(2022) 551 final](https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270). [↑](#footnote-ref-30)
30. Digitalizace energetického systému – akční plán EU, COM(2022) 552 final. [↑](#footnote-ref-31)
31. Strategický kompas pro bezpečnost a obranu, 21. března 2022 https://www.eeas.europa.eu/sites/default/files/documents/strategic\_compass\_en3\_web.pdf [↑](#footnote-ref-32)
32. [Soubor opatření EU pro kybernetickou bezpečnost sítí 5G |Formování digitální budoucnosti Evropy (europa.eu)](https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures). [↑](#footnote-ref-33)
33. https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx [↑](#footnote-ref-34)
34. COM(2022) 454 final. [↑](#footnote-ref-35)
35. COM(2021) 70 final. [↑](#footnote-ref-36)
36. V současné době probíhají na základě nařízení v přenesené pravomoci (EU) 2022/30 standardizační činnosti v souvislosti s požadavky na kybernetickou bezpečnost rádiových zařízení. Pokud Komise toto nařízení v přenesené pravomoci zruší nebo změní s tím důsledkem, že se přestane uplatňovat na některé produkty, na něž se vztahuje akt o kybernetické odolnosti, měly by Komise a evropské normalizační organizace při přípravě a vypracovávání harmonizovaných norem s cílem usnadnit provádění aktu o kybernetické odolnosti zohlednit standardizační práci provedenou v souvislosti s prováděcím rozhodnutím Komise C(2022) 5637 o žádosti o vypracování norem pro výše uvedené nařízení v přenesené pravomoci. [↑](#footnote-ref-37)
37. Např. jak je uvedeno v analýze nedostatků v oblasti investic do obrany. [↑](#footnote-ref-38)
38. Bylo zahájeno několik iniciativ, např. evropské partnerství pro obranné dovednosti. [↑](#footnote-ref-39)
39. Komise v Plánu pro kritické technologie vyzvala k posílení spolupráce v oblasti technologií, které mají kritický význam pro dlouhodobou obranu a bezpečnost Evropy, a k úsilí o snížení souvisejících strategických závislostí. [↑](#footnote-ref-40)
40. Společné sdělení o analýze nedostatků v oblasti investic do obrany a dalším postupu, v němž Komise a vysoký představitel navrhli několik opatření s cílem zajistit, aby byl průmysl EU připraven na plnění cílů v krátkodobém i dlouhodobém horizontu. [↑](#footnote-ref-41)
41. Týmy rychlé kybernetické reakce a vzájemná pomoc v oblasti kybernetické bezpečnosti (CRRT), Koordinační středisko pro kybernetický a informační prostor (CIDCC), platforma pro sdílení informací o kybernetických hrozbách a reakci na incidenty (CTIRISP), Propojené kybernetické polygony (CRF), Akademické a inovační středisko EU pro kybernetickou oblast (EU CAIH). [↑](#footnote-ref-42)
42. V rámci Evropského programu rozvoje obranného průmyslu (EDIDP) bylo financováno šest projektů (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET a HERMES) s rozpočtem ve výši 39 milionů EUR. V rámci Evropského obranného fondu na rok 2021 bude téměř 40 milionů EUR věnováno na tři projekty spolupráce v oblasti výzkumu a vývoje kybernetické obrany, které budou vybrány k financování (ACTING, AInception, EU-GUARDIAN). [↑](#footnote-ref-43)
43. Projektový tým pro kybernetickou obranu poskytuje členským státům fórum pro diskusi o otázkách kybernetické obrany s vojenskými důsledky. [↑](#footnote-ref-44)
44. Informační přehled plánu rozvoje schopností agentury EDA (28. 6. 2018): [Informační přehled plánu rozvoje schopností](https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0fInsert%20). [↑](#footnote-ref-45)
45. Jak je uvedeno ve strategickém plánu výzkumu v oblasti kybernetické obrany a v zastřešujícím strategickém plánu výzkumu. [↑](#footnote-ref-46)
46. Akční plán „Vznikající a přelomové technologie: Akční plán zaměřený na schopnosti“ byl schválen Řídícím výborem agentury EDA ve složení ředitelů pro výzkum a technologie dne 16. prosince 2021. [↑](#footnote-ref-47)
47. Včetně Společného výzkumného střediska. [↑](#footnote-ref-48)
48. Observatoř pro kritické technologie, oznámená v Akčním plánu pro synergie mezi civilním, obranným a kosmickým průmyslem. [↑](#footnote-ref-49)
49. První fáze Akčního plánu agentury EDA pro vznikající a přelomové technologie z roku 2021. [↑](#footnote-ref-50)
50. Druhá fáze akčního plánu agentury EDA z roku 2021. [↑](#footnote-ref-51)
51. Tyto skupiny nazývané CapTech poskytují odborníkům členských států fóra pro vytváření sítí a flexibilní rámec pro projekty spolupráce. Další informace o těchto skupinách souvisejících s kybernetikou (kybernetika, informace, komponenty) jsou k dispozici na adrese: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs). [↑](#footnote-ref-52)
52. OSRA mapuje příslušné oblasti výzkumu a technologií v oblasti obrany a uvádí konkrétní příležitosti ke spolupráci. Existuje sedmnáct technologických stavebních bloků spolu s jejich technologickými plány souvisejícími s kybernetickými technologiemi, které se zabývají situačním povědomím v oblasti kybernetické obrany, ochranou vojenských komunikačních systémů, zpracováním informací z různorodých zdrojů, modelováním a simulací, kvantovou výpočetní technikou a kryptografií, jakož i zkoumáním synergií mezi kybernetickými operacemi a elektronickým bojem. Klíčovou úlohu při zpracování informací hrají umělá inteligence a data velkého objemu. [↑](#footnote-ref-53)
53. *Ad hoc* rámec agentury EDA je vymezen rozhodnutím Rady (SZBP) 2015/1835. V současné době se v tomto rámci realizuje šest projektů s prvky kybernetických technologií s rozpočtem ve výši cca 20 milionů EUR (ANQUOR, CERERE, EDA SOC 2, MASFAD II, PASEI II, ASSAI). [↑](#footnote-ref-54)
54. Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. [↑](#footnote-ref-55)
55. Jak je uvedeno ve společném sdělení o analýze nedostatků v oblasti investic do obrany a dalším postupu. [↑](#footnote-ref-56)
56. Celkový počet malých a středních podniků v EU, které působí v mnohovrstevnatých a často přeshraničních dodavatelských řetězcích v oblasti obrany, se odhaduje na 2 500. Slouží zákazníkům v oblasti obrany, přičemž 7,8 % jejich podnikání souvisí s kybernetikou. [↑](#footnote-ref-57)
57. Program Horizont Evropa předpokládá, že součinnost s Evropským obranným fondem bude přínosem pro civilní a obranný výzkum, ačkoli činnosti v rámci rámcového programu budou výhradně zaměřené na civilní aplikace. [↑](#footnote-ref-58)
58. https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/ [↑](#footnote-ref-59)
59. https://www.nato.int/strategic-concept/ [↑](#footnote-ref-60)
60. Podepsána v roce 2016 a 2018. [↑](#footnote-ref-61)