



EVROPSKÁ  
KOMISE

VYSOKÝ PŘEDSTAVITEL  
UNIE PRO ZAHRANIČNÍ  
VĚCI A BEZPEČNOSTNÍ  
POLITIKU

V Bruselu dne 3.12.2025  
JOIN(2025) 977 final

## **SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ**

### **Posílení hospodářské bezpečnosti EU**

## 1. Úvod

Stále častější a cílenější využívání **hospodářských nástrojů k prosazování strategických cílů** se stalo charakteristickým rysem dnešní geopolitické situace. Hlavní aktéři zneužívají hospodářské páky k prosazování svých strategických a geopolitických cílů, od rušivých cel a zneužívání závislostí jako zbraní až po svévolné zavádění opatření na ochranu obchodu, čímž ohrožují bezpečnost, veřejný pořádek, konkurenceschopnost a hospodářství EU.

Rizika pro hospodářskou bezpečnost EU nejsou nová, ale v poslední době se zintenzivnila: zranitelnost je nyní viditelnější, naléhavější a není možné ji přehlížet. Mezi tato rizika patří:

- rostoucí **nestabilita v globálním obchodním a investičním prostředí**, která se vyznačuje nárůstem rušivých obchodních opatření a omezení vývozu s cílem zneužívat závislosti jako zbraně,
- šíření **predátorských praktik** zaměřených na kritické dodavatelské řetězce a technologie, které podkopávají naši průmyslovou základnu a z nichž některé (např. státem financované nadměrné kapacity) vytvářejí nové závislosti,
- pokračující zhoršování bezpečnostní situace, mimo jiné v souvislosti s pokračující **agresivní válkou** Ruska proti Ukrajině a nárůstem hybridních útoků.

**Strategie evropské hospodářské bezpečnosti** z roku 2023 stanovila prvotní reakci EU na tyto výzvy<sup>1</sup>. Představila řadu opatření, která vycházejí z posouzení rizik a jejichž cílem je posílit hospodářskou bezpečnost EU **podporou** konkurenceschopnosti, **ochranou** před riziky a **partnerstvím** s těmi, kdo sdílejí naše obavy. Tyto tři pilíře zůstávají jádrem našeho přístupu k hospodářské bezpečnosti a Komise se společně s členskými státy snaží o jejich začlenění do všech politických úvah a opatření. Kromě toho je hospodářská bezpečnost nezbytná pro to, aby EU mohla zachovat své hodnoty, zásady a blahobyt svých občanů a posílit naši ekonomickou nezávislost.

Za dobu od přijetí strategie v roce 2023 však potřeba, aby EU jednala odvážněji, rychleji a jednotněji, ještě zesílila. Toto sdělení nastiňuje strategičtější a asertivnější využití nástrojů Unie – doplňující jejich původní politické cíle – na podporu hospodářské bezpečnosti Evropy, která se týká schopnosti Unie zajistit bezpečnost, spolu s dalšími cíli, prostřednictvím silného, dynamického a odolného hospodářství předvídaním potenciálních nebo skutečných hrozeb, jejich odvracením a reakcí na ně, spjatých s hospodářskými vztahy EU s širším světem. EU toho může dosáhnout zejména tím, že se udrží na čele v oblasti kritických technologií, průmyslových odvětví a služeb. Odráží to **změnu paradigmatu** a přechod od reaktivního postoje k proaktivnějšímu a systematičtějšímu nasazení našeho souboru nástrojů. Kromě toho budou muset být EU, její členské státy a průmysl v některých případech stále více připraveny akceptovat hospodářské náklady ve prospěch snížení zranitelnosti a zvýšení celkové bezpečnosti.

Tato výzva k činnosti zahrnuje **zlepšení** shromažďování, monitorování a analýzy informací, jakož i schopnost předvídat vznikající hrozby; **odrazování** třetích zemí od zneužívání závislostí Unie jako zbraní; **snížování** naší expozice třetím zemím, které mohou tyto

---

<sup>1</sup> JOIN(2023) 20 final.

závislosti zneužívat jako zbraně, a **zabraňování** snahám o podkopání našich opatření na snížení rizika.

Důležité je, že tato výzva k činnosti rovněž uznává potřebu **využít silných stránek EU**, mimo jiné pokud jde o bezkonkurenční váhu jednotného trhu EU, naše technologické a průmyslové schopnosti a přístup k financování z prostředků EU a programů EU. To zahrnuje identifikování hospodářských příležitostí EU i těch oblastí, v nichž jsou ostatní závislí na EU. Toto sdělení proto vyzývá k **integrovanému, celovládnímu a podnikatelskému přístupu, lepšímu řízení a ještě užší spolupráci s obdobně smýšlejícími partnery a případně ke společnému postupu**. Doplnuje komplexní Strategii unie připravenosti EU. Hospodářská bezpečnost EU je založena na bezpečnosti členských států. Je také neodmyslitelně spjata s širšími vztahy se světem, a tedy se společnou zahraniční a bezpečnostní politikou, která bude systematictěji využívána k podpoře stanovených cílů.

Na tomto základě a na základě analýzy rizik se toto sdělení zaměřuje na šest vysoce rizikových oblastí uvedených v oddíle 3, uplatňuje nástroje, které máme k dispozici, a nastiňuje, jak je lze dále zlepšit.

## **2. Proaktivní přístup k hospodářské bezpečnosti**

EU disponuje celou řadou nástrojů, které přispívají k její hospodářské bezpečnosti. Nyní je musí k tomu, aby posílila svou hospodářskou bezpečnost, využívat **strategičtěji, efektivněji a aktivněji**. Ačkoli většina z těchto nástrojů nebyla původně vyvinuta s ohledem na hospodářskou bezpečnost, jsou přesto pro dosažení cílů hospodářské bezpečnosti Unie velmi důležité.

Neúplný seznam klíčových nástrojů je uveden na *obrázku 1* a jejich koordinované použití je dále popsáno v *oddíle 3*.

Obrázek 1: Neúplný seznam nástrojů na podporu hospodářské bezpečnosti



V zájmu posílení hospodářské bezpečnosti EU bude Komise v koordinaci s členskými státy tyto nástroje využívat takto:

- **Nástroje v oblasti obchodu a hospodářské soutěže** budou využívány k postupnému snižování vystavení EU rizikům a k tomu, aby se předcházelo ohrožení cílů EU v oblasti snižování rizik. To zahrnuje rozšíření možností diverzifikace, a tím i naší širší bezpečnosti v rámci obchodních dohod EU, strategické využití souboru celních nástrojů a řešení narušení způsobených zahraničními subvencemi, a to jak v rámci jednotného trhu, tak prostřednictvím subvencí nebo dumpingového dovozu.
- Nástroje **odolnosti a kybernetické bezpečnosti** se zaměří na přípravu na mimořádné situace a jejich zvládnutí, jakož i na snížení vystavení vnějším hrozbám, jako jsou kybernetické hrozby.
- **Nástroje bezpečnosti a veřejného pořádku** budou využívány ke snížení nadměrného vystavení EU rizikům, aby bylo mimo jiné zajištěno normální fungování společnosti, a zároveň budou podporovat opatření zaměřená na rozvoj jejího postavení v kritických technologiích a průmyslových odvětvích, jakož i na předcházení ohrožování jejích cílů v oblasti snižování rizik.

- Cílem v oblasti **nátlakových a omezujících opatření** bude odrazovat od nátlaku a řešit situace, kdy se třetí země pokoušejí vyvíjet nátlak na EU, chránit podniky EU před účinky opatření přijatých určitou třetí zemí uplatňovaných mimo její území (extrateritoriální opatření), a případně vyvolat změnu v chování dotčené země.
- **Financování a omezení** prostřednictvím nástrojů EU, jako jsou NDICI (Global Gateway), Horizont Evropa, NextGenerationEU, InvestEU, program Digitální Evropa, Nástroj pro propojení Evropy, nástroje předvstupní pomoci, plány růstu pro západní Balkán a Moldavsko, jakož i Nástroj pro Ukrajinu, EU4Health a budoucí Evropský fond pro konkurenceschopnost, by měly v souladu s pravidly programů posílit hospodářskou bezpečnost EU nebo ji přinejmenším neoslabit.
- **Odvětvové iniciativy** – budou využity k budování vlastních kapacit a strategických schopností EU ve vysoce rizikových oblastech zjištěných v procesu posouzení rizik.

Úzká spolupráce a koordinace se zeměmi, které přikládají podobný význam hospodářské bezpečnosti a globálnímu řádu založenému na pravidlech, je důležitější než kdy jindy. EU bude usilovat o posílení **mezinárodní spolupráce v otázkách hospodářské bezpečnosti**, zejména s **důvěryhodnými partnery**, a to i prostřednictvím **cílených dialogů o hospodářské bezpečnosti vedených na dvoustranné i vícestranné úrovni**. Tato spolupráce podpoří společnou činnost v oblasti společných zájmů nebo obav týkajících se hospodářské bezpečnosti. Rovněž prohloubí kolektivní chápání rizik, pomůže předvídat hrozby, umožní navrhnout zmírňující opatření, která **minimalizují negativní externality**, přispěje k budování a udržení spolehlivých a odolných dodavatelských řetězců v klíčových strategických odvětvích a pomůže zabránit negativním dopadům na naše obdobně smýšlející mezinárodní partnery.

Komise bude usilovat o spolupráci se třetími zeměmi na dvoustranné úrovni, prostřednictvím skupiny G7 a v rámcích, jako je komplexní a progresivní dohoda o transpacifickém partnerství a další příslušná fóra. Bude spolupracovat s partnery na vývoji a zavádění norem hospodářské bezpečnosti pro odolné dodavatelské řetězce. Užší spolupráce může zahrnovat **koordinované nasazení nástrojů** a vytváření koalic s partnery, kteří mají podobné cíle v oblasti hospodářské bezpečnosti nebo se potýkají s podobnými výzvami.

Rovněž je třeba odpovídajícím způsobem zohlednit význam a dopad **politik sousedství a rozšiřování EU**.

Rizika a příležitosti pro hospodářskou bezpečnost EU budou začleněny do provádění politik a

#### ***Zavádění norem hospodářské bezpečnosti***

V návaznosti na práci skupiny G7 v oblasti obchodu vycházejícího z norem bude Komise podporovat rozvoj a používání norem hospodářské bezpečnosti. Ty budou:

- zaměřené na opatření k diverzifikaci kritických dodavatelských řetězců vytvořením podmínek pro vstup nových dodavatelů na trh nebo omezením přístupu dominantních dodavatelů,
- založené na zásadách transparentnosti, interoperability a souladu s mezinárodními pravidly,
- cílené a přizpůsobené, zohledňující specifická rizika, hospodářské dopady a obchodní realitu každého z dodavatelských řetězců.

Tato práce se prioritně zaměří na kritické suroviny a dodavatelské řetězce polovodičů a zároveň prozkoumá další spolupráci v jiných oblastech.

programů Komise s těmito regiony. Kandidátské země jsou na cestě k budoucímu členství v EU; jejich přizpůsobení hospodářské bezpečnostní politiky a postupná integrace do jednotného trhu jsou zásadní pro zajištění jejich úspěšného přistoupení a zároveň pro zvýšení schopnosti EU řešit stávající i nová rizika. Je proto důležité, aby kandidátské země zohledňovaly přístup EU k hospodářské bezpečnosti a případně se postupně přizpůsobovaly právním předpisům EU, které jsou pro cíle hospodářské bezpečnosti relevantní.

### **3. Zvýšení evropské hospodářské bezpečnosti: vysoce rizikové oblasti**

Strategie přijatá v roce 2023 zahájila posuzování rizik, která se týkají odolnosti dodavatelského řetězce a energetické bezpečnosti, kritické infrastruktury, zneužívání hospodářských závislostí jako zbraní a technologické bezpečnosti a úniku technologií. Čtyři kritické technologie – umělá inteligence, kvantové technologie, polovodiče a biotechnologie – již byly posouzeny. Na základě této práce Komise určila **šest vysoce rizikových oblastí**, na které v nejbližší době a v krátkodobém horizontu zaměří své úsilí, a to v úzké spolupráci s členskými státy, průmyslem a důvěryhodnými partnery. Komise bude zároveň nadále sledovat vývoj a v případě potřeby posuzovat nově vznikající vysoce rizikové oblasti a konat v nich.

#### **Přehled šesti vysoce rizikových oblastí**



#### **3.1 Posílení odolnosti dodavatelského řetězce a odstraňování vysoce rizikových závislostí u kritického zboží a služeb**

##### **Nekumulativní znaky vysoce rizikové závislosti:**

- 60 % nebo více dodávek do EU kontroluje *jediná třetí země nebo její subjekty*,
- vstupy/služby mají *systémovou hodnotu pro hospodářství EU vzhledem k jejich úloze ve vícero odvětvích, např. kritické suroviny, polovodiče*,
- vstupy/služby mají *zásadní význam pro obranný průmysl / strategické kapacity EU nebo specifické kritické technologické dodavatelské řetězce, jako jsou technologie čisté energie*,
- *třetí země již hospodářské závislosti zneužila jako zbraň nebo tím hrozí, např. prostřednictvím omezení vývozu*,
- *již existuje netržní nadbytečná kapacita nebo se vytváří.*

**Riziko.** Moderní hospodářství jsou hluboce propojená a opírají se o širokou škálu vstupů, meziproductů a základních služeb od partnerů z celého světa. V některých případech je nabídka vysoce koncentrovaná – často v zemích, které nesdílejí stejné strategické zájmy a které mají schopnost a vůli tuto závislost zvýšit a zneužívat ji jako zbraň. Tato rizika pro dodavatelské řetězce EU se projevují zejména v naší závislosti na některých **kritických surovinách, zpracovaných a pokročilých materiálech, komponentech čistých technologií a běžných polovodičích**, jakož i ve **finančních službách**,

**farmaceutickém průmyslu, letectví, digitálních a vesmírných technologiích.** Jsou patrná i v **zemědělsko-potravinářském odvětví**, kde Vize pro zemědělství a potraviny<sup>2</sup> stanoví potřebu snížit strategické závislosti, zejména pokud jde o dovoz krmiv a doplňkových látek a hnojiv, kde je EU závislá na několika málo partnerech.

Vysoce rizikové závislosti mohou: i) být **zneužívány jako zbraně** k donucovacím účelům (např. kritické suroviny, běžné polovodiče, pokročilé materiály, energetické produkty, hrozby vyřazení některých služeb z provozu); ii) vytvářet **systémovou hospodářskou zranitelnost** nebo systémové riziko pro veřejný pořádek a ochranu veřejného zdraví v krizových situacích (např. osobní ochranné prostředky, kritické dodávky léků, zásobování potravinami); iii) vytvářet riziko rozsáhlého narušení napříč odvětvími (např. pronikáním do telekomunikačních sítí, závislostí na jediném poskytovateli cloudových služeb, vypínače („kill switches“) digitálních služeb); iv) **ovlivnit konkurenceschopnost EU a zpomalit ekologickou a digitální transformaci**, pokud dojde k narušení dodávek (např. baterií, permanentních magnetů, výrobků a komponentů z oblasti čistých technologií, pokročilých materiálů); v) **ovlivnit autonomii členských států při rozvoji a provozování vojenských schopností** nebo vi) **ohrožovat potravinovou soběstačnost EU**.

***Příklady použití: běžné polovodiče***

**Riziko:** strukturální závislost na jediném dodavateli ze třetí země při výrobě základních čipů s nízkou marží ohrožuje několik evropských průmyslových odvětví. Tyto polovodiče jsou důležitou součástí mnoha dodavatelských řetězců.

**Použití nástrojů:** Komise bude spolupracovat s důvěryhodnými partnery na diverzifikaci zdrojů dodávek a bude se snažit podpořit zvýšení výroby v EU. Účinná zmírňující opatření budou stanovena v připravované revizi aktu o čipech. Kybernetická bezpečnost dovážených běžných polovodičů používaných v aplikacích souvisejících s bezpečností by nadále měla být posuzována podle Aktu o kybernetické odolnosti.

**Cíl.** Komise a členské státy se budou snažit **minimalizovat možnost krátkodobého narušení** a zároveň zavést opatření, která **postupně sníží stávající vysoce rizikové závislosti na jednotném trhu a budou čelit snahám o vytvoření nových**. Využije své nástroje k monitorování dodavatelského řetězce, vytvoří rámec na podporu diverzifikace dodávek a zabrání oslabování akceschopnosti EU tím, že bude řešit narušování hospodářské soutěže na jednotném trhu. Důležitou roli budou hrát také opatření v souvislosti s přechodem na oběhové hospodářství.

Komise přijme nezbytná opatření, aby zajistila, že její alternativní dodavatelské řetězce nebudou narušovány dumpingem a cenovou manipulací.

Komise bude členským státům nápomocna při plném a účinném využívání stávajících nástrojů, zejména kritérií odolnosti, která budou muset členské státy od ledna 2026 uplatňovat při zadávání veřejných zakázek, aukcích a režimech veřejné podpory podle Aktu o průmyslu pro nulové čisté emise.

<sup>2</sup> COM/2024/75 ze dne 19. února 2025.

Komise rovněž přijme opatření jak k rozvoji **vnitřních kapacit a schopností EU**, tak k diverzifikaci dodávek **prostřednictvím spolupráce s partnery, včetně využití rozsáhlé sítě obchodních dohod a dalších forem dvoustranné a vícestranné spolupráce**. To bude zahrnovat zvážení výroby určitých kritických produktů v našich kandidátských zemích a našich partnerských zemích v širším smyslu, včetně regionů, jako je Blízký východ a severní Afrika. Posílí to odolnost diverzifikovaných dodavatelských řetězců v EU a otevře další příležitosti pro podniky z EU. Komise bude i nadále identifikovat a průběžně monitorovat zranitelná místa dodavatelského řetězce a **vysoce rizikové závislosti** prostřednictvím procesu hodnocení rizik a spolupráce s členskými státy a průmyslem.

### 3.2 Přilákání příchozích investic s přidanou hodnotou, které posilují hospodářskou bezpečnost EU

**Riziko.** Příchozí investice zvyšují odolnost a konkurenceschopnost EU vytvářením pracovních míst, rozvojem průmyslových kapacit, využíváním principu financování a rozšiřování („financing and scale“), podporou inovací a přenosem technologií. Některé formy příchozích investic však mohou představovat rizika. Mezi tato rizika patří: i) rizika pro **bezpečnost a veřejný pořádek**, včetně přístupu k citlivým údajům (např. geolokalizace, biometrické údaje, obchodní tajemství), přístupu ke kritické infrastruktuře, přístupu k technologiím dvojího užití a jiným kritickým technologiím; ii) **rizika pro hospodářskou odolnost**, jako je hlubší závislost nebo selhání jednoho bodu v kritických dodavatelských řetězcích kontrolovaných vysoce rizikovými subjekty nebo třetími zeměmi, které ohrožují naše zájmy v oblasti hospodářské bezpečnosti (např. baterie, kritické suroviny, software a komponenty), jež činí EU zranitelnou vůči hospodářským narušením nebo zneužívání závislosti jako zbraní, a iii) **problémy spojené s nízkou konkurenceschopností**, jako je nedostatečný přenos technologií, omezená tvorba přidané hodnoty (např. pouze montážní linky), zaměstnávání pracovníků pocházejících z investující země, což má mimo jiné dopad na místní trh práce.

**Cíl.** Komise se zaměří na to, aby EU zůstala otevřená a atraktivní pro zahraniční investice. Bude usilovat o vyvažování této otevřenosti tam, kde je to nezbytné pro hospodářskou bezpečnost EU, s potřebou vyhnout se prohlubování závislosti nebo vytváření

#### ***Příklad: bateriová elektrická vozidla***

**Riziko.** Dominantní postavení některých dodavatelů bateriových elektrických vozidel a striktní držení technologií potřebných pro jejich výrobu představují riziko, že bude oslabena klíčová úloha automobilového odvětví v hospodářství EU, přičemž tito dodavatelé zároveň mají prospěch z trhu EU. S propojenými vozidly jsou také spojena rizika kybernetické bezpečnosti.

**Použití nástrojů:** Komise zkoumá způsoby, jakými lze podpořit investice s přidanou hodnotou, a to i prostřednictvím iniciativ v oblasti obchodu a politiky hospodářské soutěže. Bude nadále sledovat obchodní toky a využívat svůj soubor nástrojů pro zmírnění rizik s cílem snížit riziko prvků zajišťujících propojitelnost vozidel, podporovat investice do nové generace technologií bateriových elektrických vozidel, aby Evropa zůstala odolná a konkurenceschopná, a v případě potřeby omezit vystavení vysoce rizikovým subjektům, které prvky pro propojení u bateriových elektrických vozidel dodávají. Komise bude podněcovat sdílení technologií a souvisejícího know-how, které může posílit cíle EU v oblasti hospodářské bezpečnosti.

nových. Kromě toho je zásadní zachovat schopnost společností v EU inovovat, a to i prostřednictvím zahraničního nákupu klíčového duševního vlastnictví od nově vznikajících šampionů, a zajistit bezpečnost dodávek a kontinuitu služeb. Komise využije své nástroje a iniciativy, aby stanovila a provedla cílená opatření, jako je podmiňování příchozích investic, jež usnadňují přenos technologií, u subjektů v zemích, které záměrně podkopávají naši hospodářskou bezpečnost.

### 3.3 Podpora dynamického obranného a kosmického průmyslu a dalších vysoce rizikových průmyslových odvětví

**Riziko.** Ruská agresivní válka proti Ukrajině, rostoucí geopolitické napětí a politicky motivované kroky k zneužívání obchodních závislostí jako zbraní zvyšují význam investic do dynamické domácí průmyslové základny, zejména v obranném a kosmickém průmyslu a ve strategických odvětvích dvojího užití, např. v dopravě (např. letectví, letecký průmysl, stavba lodí a přístavy), která je motorem hospodářství EU a podporuje její strategickou autonomii. Rizika v této oblasti zahrnují: i) nedostatečné (vnitřní) investice; ii) nízký objem výroby v kombinaci s nedostatečným opatřováním technologií z domácích zdrojů pro institucionální infrastrukturu; iii) netržní politiky a postupy třetích zemí, které vedou k narušení globálních a regionálních trhů; iv) neodůvodněné nebo nepřiměřené kontroly vývozu ze strany třetích

#### ***Příklady použití: Klíčové komponenty pro drony a protidronové systémy***

**Riziko:** Závislost na dodavateli ze třetích zemí, pokud jde o klíčové součásti dronů, baterie a protidronové systémy; extrémně krátký inovační cyklus nutný k tomu, aby bylo řešení s drony provozně efektivní, založené na reálných zkušenostech z bojiště (počítáno v měsících, někdy v týdnech).

**Použití nástrojů:** Komise využije své nástroje v rámci evropských programů pro obranný průmysl k zajištění výrobních kapacit v EU a ke zkrácení inovačních cyklů pro technologie bezpilotních letadel na základě skutečných zkušeností z provozu. Bude nadále posilovat spolupráci a výměnu informací na dobrovolném základě mezi příslušnými subjekty (např. národními agenturami pro veřejné zakázky, mezinárodními organizacemi pro veřejné zakázky – OCCAR, EDA, NATO) a v rámci nástrojů/akcí evropských programů pro obranný průmysl. Za účelem zajištění odolnosti dodavatelského řetězce vytvoří cílené mapování dodavatelských řetězců pro konkrétní výrobky a zařízení, včetně zboží dvojího užití, a podpoří výrobu prostřednictvím společných investic.

zemí uvalené na evropské výrobky a technologie (extraterritorialita vývozních režimů třetích zemí); v) ztráta vlastnictví a kontroly v důsledku zahraničních akvizic, včetně akvizic portfolia v určitých případech; vi) nepružný regulační rámec a roztržité kapitálové trhy, které neusnadňují tok finančních prostředků ani nenapomáhají rozvoji kapacit vysoce rizikových a vysoce výnosných technologií s dvojím užitím formou startupů a scalupů.

Některé komponenty v kritických odvětvích, jako je obrana, pocházejí od vysoce rizikových subjektů, což by v případě geopolitického napětí mohlo zabránit přístupu k **obránnému vybavení, technologiím dvojího užití a vojenským mobilním prostředkům** a jejich používání. Kromě toho je zásadní, aby si EU udržela vysoce kvalifikovanou pracovní sílu a nezaostávala v inovacích v technologiích, které jsou základem strategických odvětví. Účinné zmírnění těchto rizik prostřednictvím rychlé mobilizace cílených a účinných nástrojů je pro obranné a

vojenské schopnosti v EU zásadní.

**Cíl.** Komise využije své nástroje k udržení a rozvoji strategických výrobních kapacit a schopností v EU, zejména prostřednictvím: i) podpory a případně snižování rizik veřejných a soukromých **investic**; ii) **podpory poptávky** (pobídky) také prostřednictvím sdružování nebo společného nákupu; iii) **zabránění přemístění** strategických schopností a odvětví; iv) **postupného vyřazení potenciálně nepřátelských subjektů** z obranných a jiných kritických dodavatelských řetězců, včetně omezení možnosti nákupu kritických obranných a vesmírných technologií ze zemí mimo EU na minimum; v) zmírnění **hrozeb, jaké představují přímé zahraniční investice** do společností dodávajících kritické výrobky nebo technologie; vi) **podpory vývoje kritických technologií, komponent a materiálů** v EU v návaznosti na dlouhodobé cíle, jakož i jejich opatrování z domácích zdrojů pro institucionální infrastruktury; vii) zajištění podmínek pro **startupy a podniky** v EU, které jsou nezbytné pro jejich rozvoj, například prostřednictvím odpovídajícího financování a dočasného zvýhodněného celního zacházení pro určité vstupy.

Prioritou bude podpora **obránné a kosmické průmyslové základny**. Ačkoli se Komise bezprostředně zaměří na konkrétní vysoce rizikové situace zjištěné v procesu posuzování

rizik, bude z hlediska hospodářské bezpečnosti pečlivě sledovat všechna klíčová odvětví, jako jsou čisté technologie, energetika a energeticky náročná a oběhová odvětví, zemědělství a potravinářství, digitální a elektronický průmysl, letectví (včetně leteckého průmyslu), stavba lodí, automobilový průmysl a zdravotnictví.

### 3.4 Rozvoj a udržení vedoucího postavení v oblasti kritických technologií

**Riziko.** Některé třetí země a podniky projeví zájem o získání kontroly nad vznikajícími nebo pokročilými technologiemi a know-how EU. V některých případech byly tyto kroky zaměřeny na ohrožení schopnosti Unie soutěžit v oblasti technologií. Tento cíl sledují například akvizicemi, spoluprací ve výzkumu a vývoji, reverzním inženýrstvím nebo průmyslovou špiónáží. Děje se tak také tím, že se uměle odebírá podíl na trhu inovativnějším společnostem, což jim následně přináší menší příjmy, které

#### ***Příklady použití: kvantové technologie***

**Riziko:** Zahraniční subjekty podporované státem nebo vysoce rizikové subjekty usilují o přístup ke kvantovému výpočetnímu, komunikačnímu a snímacímu know-how a infrastrukturu EU prostřednictvím investic, akvizic nebo partnerství v oblasti výzkumu a vývoje, což urychluje citlivé vojenské a zpravodajské využití v zahraničí a narušuje technologickou suverenitu EU.

**Použití nástrojů:** Komise bude pokračovat v mapování klíčových aktérů/infrastruktur EU v oblasti kvantových technologií a ve sledování zahraničních investic, partnerství a toků duševního vlastnictví, aby tyto poznatky mohla využít pro prověřování přímých zahraničních investic, kontrolu vývozu a posuzování bezpečnostních rizik v souvislosti s výzkumem. Využije své nástroje k prověřování rizikových investic a ke spolupráci s členskými státy při koordinaci rychlé reakce na pokusy o nepřátelské převzetí nebo případy úniku informací. V zájmu podpory cílů hospodářské bezpečnosti bude upřednostňovat financování a dodavatele kritických kvantových komponent a služeb z EU a podobně smýšlejících zemí a omezovat závislost na vysoce rizikových poskytovatelích kvantových/cloudových služeb v citlivých odvětvích. Dále se bude snažit zajistit, aby subjekty pod nepatřičným zahraničním vlivem neměly přístup k citlivým kvantovým projektům.

mohou investovat do špičkového výzkumu a vývoje. V dlouhodobém horizontu bude hospodářská výkonnost, bezpečnost a geopolitické postavení EU záviset na udržení a rozvoji našich technologických schopností. Strategický význam má proto zachování schopností EU v oblasti těchto technologií, a to posílením specializovaných nástrojů financování EU a řešením bezpečnosti a úniku technologií. Zároveň je třeba věnovat velkou pozornost stále roztržitějšímu provádění a prosazování kontrol vývozu zboží dvojího užití.

**Cíl.** Komise využije své nástroje k podpoře pozitivního rámcového prostředí pro rozvoj kritických technologií v EU a k tomu, aby mohla odstraňováním narušení trhu překazit kroky, které by úsilí EU oslabovaly. Bude sledovat vývoj na trhu a poskytovat další podporu výzkumu a inovacím v EU prováděným startupy a scaleupy, zavedenými podniky, výzkumnými a inovačními organizacemi a akademickou obcí. Zaměří se na zajištění průmyslového rozšíření a využití („valorizaci“) výsledků výzkumu, vývoje a inovací v průmyslové základně jednotného trhu. 28. režim, který podnikům poskytuje jednotný harmonizovaný soubor pravidel platných v celé EU pro zakládání společností, správu a řízení, mobilitu a přístup k financování, posílí hospodářskou odolnost EU tím, že umožní bezpečnější přeshraniční operace a robustnější a diverzifikovanější dodavatelské řetězce.

Komise bude podporovat bezpečnost výzkumu a inovací a přijímat doprovodná opatření potřebná ke zmírnění rizika úniku technologií nebo know-how, například prostřednictvím predátorských akvizic, spolupráce v oblasti výzkumu a vývoje a investic na strategických a nově vznikajících trzích EU v citlivých destinacích nebo odvětvích, a zároveň bude nadále podporovat důvěryhodná mezinárodní partnerství v oblasti výzkumu a inovací, jež mají zásadní význam pro cíle hospodářské bezpečnosti Unie. Bude zkoumat, jak zajistit, aby se podniky a výzkumné a inovační organizace v EU mohly rozšiřovat a zdržet se akvizicí / převodů vlastnictví motivovaných výlučně nedostatečnými možnostmi financování z důvěryhodných zdrojů. Komise se zároveň bude snažit zabránit přístupu vysoce rizikových subjektů k akcím podporovaným Unií v oblasti kritických technologií, které mohou být potenciálně zneužity jako zbraně proti EU.

### 3.5 Zamezit přístupu k citlivým informacím a údajům, který by mohl ohrozit hospodářskou bezpečnost EU

**Riziko.** Třetí země získávají přístup k citlivým informacím/údajům EU nebo jejích členských států buď v důsledku průmyslové špionáže, dodávek hardwaru nebo softwaru používaného v určitých produktech (např. propojená vozidla, 5G/jiné telekomunikační systémy, infrastruktura elektrické sítě, platformy pro sekvenování DNA) nebo v důsledku

#### ***Příklad: detekční zařízení na hranicích EU (přístavy, letiště, pozemní hranice atd.)***

**Riziko:** chybějící společný postup v rámci EU, závislost na jediném dodavateli nebo omezeném počtu dodavatelů, neoprávněný přístup (včetně prostřednictvím povolených cest, např. údržby), který ovlivňuje výkon detekčního zařízení a integritu a/nebo důvěrnost souvisejících citlivých informací, zranitelnost vůči škodlivému softwaru, který by mohl ohrozit nebo narušit související informace/systémy/sítě prostřednictvím zařízení.

**Použití nástrojů:** na základě posouzení rizik kybernetické bezpečnosti podle směrnice NIS2 bude Komise usilovat o zmírnění zjištěných rizik prostřednictvím identifikace vysoce rizikových dodavatelů, využívání systémů certifikace kybernetické bezpečnosti, zpřísnění norem kybernetické bezpečnosti a začlenění bezpečnostních požadavků do výzev k předkládání nabídek. Komise posoudí možnou roli zahraničních subvencí v poskytování konkurenční výhody některým dodavatelům.

vlastnictví a kontroly určitých podniků, které disponují citlivými informacemi/údaji (např. provozovatelé přístavů, letišť a dopravních podniků, finanční sítě, modely umělé inteligence, datové portály, telekomunikace, osobní údaje nebo citlivé informace o trhu). Jsou tu jasné důsledky pro bezpečnost a veřejný pořádek, které jsou dále umocněny potenciálními hospodářskými dopady, například v souvislosti s roztržitostí dodavatelských řetězců. Například v odvětví energetiky se toto riziko vztahuje na akvizice společností z EU, které vlastní pokročilé technologie pro monitorování a zpracování provozních údajů z kritické energetické infrastruktury, investory ze zemí mimo EU.

**Cíl.** Snížit a pokud možno vyloučit riziko přístupu vysoce rizikových subjektů a spřízněných subjektů k citlivým informacím/údajům EU nebo jejích členských států, a tím omezit potenciální negativní dopady na hospodářství a bezpečnost EU. Pozornost bude věnována také riziku, které mohou představovat zahraniční pracovníci ve strategických odvětvích a zahraniční studenti na vysokých školách, včetně oborů vědy, technologie, inženýrství a matematiky (STEM), v souladu s příslušnými postupy.

### 3.6 Předcházet narušením kritické infrastruktury EU, která mají vliv na hospodářství EU, a zmírňovat jejich důsledky

**Riziko.** Narušení kritické infrastruktury EU – včetně kritické dopravní, kosmické, energetické a komunikační infrastruktury, zejména pokud jsou označeny za strategické pro vojenskou mobilitu – zahraničními aktéry, které by mohlo vést k řetězovým dopadům na evropské hospodářství. Důraz bude kladen na zajištění stability poskytovaných služeb. K narušení může

#### ***Příklad: měniče pro solární aplikace***

**Riziko:** rostoucí závislost na jediném dodavateli; kybernetická rizika – manipulace s parametry výroby elektřiny, znemožnění výroby elektřiny, přístup k provozním údajům, proniknutí do dodavatelského řetězce.

**Použití nástrojů:** Komise bude pokračovat v posuzování kybernetických rizik prostřednictvím koordinovaného posouzení v rámci směrnice NIS2 (má být uzavřeno v roce 2026). Na tomto základě bude zavádět zmírňující opatření zaměřená jak na posílení připravenosti (např. nařízení o rizikové připravenosti v odvětví elektroenergetiky, směrnice o odolnosti kritických subjektů), tak na řešení zjištěné zranitelnosti, např. prostřednictvím: certifikace a standardizace podle Aktu o kybernetické odolnosti a necenových kritérií podle Aktu o průmyslu pro nulové čisté emise. Komise bude sledovat vývoj na trhu a snažit se předcházet vysoce rizikovým investicím nebo je zmírňovat. Komise bude i nadále posuzovat roli zahraničních subvencí, které mohou narušovat rovné podmínky na trzích se solární energií, zejména prostřednictvím subvencovaného dovozu.

dojít fyzickými, kybernetickými nebo hybridními útoky, včetně sabotáže celých zařízení nebo jejich částí / dílčích komponent. Mohly by být také spjaty s dodavatelskými řetězci IKT, které jsou základem kritických komponent nebo služeb pro kritické infrastruktury. Existuje také riziko, že se v kritické infrastruktuře EU budou předem nacházet vysoce rizikové třetí země a provozovatelé, aby získali kapacitu k jejímu narušení (takovým způsobem a v takovou dobu, jak je třeba). Kromě toho existuje reputační riziko a riziko důvěryhodnosti, jestliže je určitá infrastruktura ohrožena nebo skutečně zasažena. V neposlední řadě existuje riziko spojené s tím, že třetí země převezmou vedoucí úlohu při stanovování mezinárodních

norem, což může ovlivnit kritickou infrastrukturu.

**Cíl.** V souladu s příslušnými strategiemi EU pro obranu, vnitřní bezpečnost a připravenost prosazovat stávající pravidla s cílem snížit riziko úniku údajů / špionáže a fyzického a kybernetického narušení, zejména prostřednictvím: i) **omezení vlastnictví/kontroly/provozu evropské kritické infrastruktury vysoce rizikovými subjekty**; ii) zvýšení opatření **fyzické ochrany**; iii) **omezení kybernetické zranitelnosti** a iv) **omezení závislosti na jednotlivých dodavatelích nebo vysoce rizikových dodavatelích**, jakož i skryté zranitelnosti, zadních vrátek nebo možných systémových narušení dodávek IKT, zejména v případech technologického uzamčení („lock-in“) nebo závislosti na dodavateli; v) **vyhrazování kritických výrobních kapacit EU** s potenciálem rozšíření v době narušení globálního dodavatelského řetězce nebo zdravotních krizí; vi) toho, že Komise **zabrání přístupu vysoce rizikových subjektů k akcím podporovaným Unií**, včetně akcí podporovaných finančními institucemi a nástroji; vii) podpory **rozvoje důvěryhodných dodavatelů kritických dílčích komponentů** v EU a v důvěryhodných třetích zemích, aby existovaly životaschopné alternativy; viii) podpory **stěžejních iniciativ** v oblasti obrany a souvisejících oblastech (Hlídky východního křídla, Iniciativa pro evropskou dronovou obranu).

#### **4. Opatření k posílení hospodářské bezpečnosti EU**

Přístup ke kvalitním informacím a jejich důkladné analýze je výchozím bodem pro účinnou a dobře informovanou politiku hospodářské bezpečnosti EU a pro rozhodování. Systém posuzování rizik, který byl zahájen strategií z roku 2023, zůstane jádrem tohoto úsilí. Stávající posouzení budou aktualizována, prohloubena a doplněna o nová posouzení kritických technologií a dodavatelských řetězců.

Komise bude dále rozvíjet svou schopnost shromažďovat informace o hospodářské bezpečnosti. Urychlí **mapování strategických závislostí v hodnotových řetězcích, které vedou ke zranitelnosti hospodářství Unie**, a posílí **monitorování a předvídání opatření** třetích zemí, jejichž cílem je vytvořit nové závislosti nebo udržet ty stávající.

Úspěch politiky hospodářské bezpečnosti EU bude navíc záviset na **lepší koordinaci na úrovni EU i s členskými státy**. Zahrnuje to budování společného chápání hrozeb pro hospodářskou bezpečnost, identifikaci konkrétních rizik a vypracování opatření na jejich zmírnění. To by mělo být podpořeno lepšími informačními toky, plným porozuměním nákladům a přínosům činnosti EU a ochotou jednat společně, pokud je to nutné, což by EU postavilo do silné pozice. Komise podnikla nezbytné vnitřní organizační kroky. Vyžaduje to však také nový způsob spolupráce s členskými státy a stále více i mezi členskými státy samotnými, zejména pokud jde o oblasti politiky, které jsou stále strategičtější, ale tradičně decentralizované, jako je výzkum a inovace.

EU bude i nadále úzce spolupracovat s **průmyslem** a zajistí bezpečnou výměnu informací a strukturovanější zapojení. Průmysl je v první linii hospodářské bezpečnosti EU. Podniky se musí stát odolnějšími a diverzifikovat své kritické dodavatelské řetězce, zejména tím, že se zcela zbaví závislosti na jediném vysoce rizikovém dodavateli. Je také důležité, aby do svých obchodních modelů začlenily náklady, které jsou spojeny s větší diverzifikací, a uznaly přínosy, které přináší odolnost vůči geopolitickým rizikům. Musí se jednat o **obousměrný**

**proces a odpovědnost, která musí být sdílena mezi veřejným a soukromým sektorem**, což umožní tvůrcům politik zlepšit kapacitu EU pro vyhodnocování hrozeb a obchodní zpravodajství a připravit ji na opatření, zatímco průmyslu pomůže realizovat opatření ke zmírnění dopadů na úrovni podniků.

Komise s podporou vysoké představitelky:

- Zlepší **kapacitu pro shromažďování informací a analýzu** tím, že bude rychleji provádět posouzení rizik v konkrétních kritických dodavatelských řetězcích, kritické infrastruktury a kritických technologiích, a bude pravidelně vyhlašovat výzvy k předkládání důkazů s cílem získat podněty od průmyslu a zúčastněných stran ohledně zranitelnosti dodavatelského řetězce a jeho vystavení vnějšímu tlaku.
- Bude podporovat větší **koordinaci a výměnu informací prostřednictvím své sítě pro hospodářskou bezpečnost s členskými státy**. Komise bude síť využívat k podpoře vypracovávání scénářů, sjednocování chápání hrozeb, rizik a možností jejich zmírňování, usnadňování výměny informací a podpoře provádění, zejména při používání nástrojů, které jsou v kompetenci členských států. V této souvislosti Komise zajistí, aby byly k dispozici vhodné informační systémy na podporu **rychlé a bezpečné výměny utajovaných informací mezi členskými státy navzájem a s členskými státy** o otázkách hospodářské bezpečnosti – včetně posouzení rizik, kritických a vysoce rizikových subjektů a transakcí, které mohou vzbuzovat obavy. Doplní tak práci sítě EU pro vytváření zásob, která se zaměřuje na zajištění zásobování základním zbožím v krizových situacích.
- Vytvoří **informační centrum pro hospodářskou bezpečnost** s podporou ESVČ, INTCEM/SIAC<sup>3</sup>, sítě delegací EU a členských států, jakož i stávajících nástrojů pro monitorování hospodářské situace na jednotném trhu, jako je monitorovací systém „SCAN“ (Supply Chain Alert Notification – varovná hlášení týkající se dodavatelského řetězce); bude mapovat a konsolidovat dostupné informace v rámci stávajících veřejných a soukromých mechanismů a koordinovat shromažďování dalších informací důležitých pro hospodářskou bezpečnost. To bude zahrnovat **mechanismus monitorování trhu**, který bude shromažďovat informace o vývoji ve vysoce rizikových oblastech, včetně rychlých informací o obchodních tocích v odvětvích podléhajících diverzifikaci, aby se zajistilo, že akceschopnost EU nebude oslabena. Bude také konsolidovat informace o **vysoce rizikových subjektech**, aby se podpořil proces posuzování způsobilosti pro financování z prostředků EU a účast na investici nebo veřejné zakázce v EU. Kromě toho by Evropský celní úřad a Celní datové centrum EU měly účinně **podporovat a prosazovat provádění souvisejících iniciativ EU v oblasti hospodářské bezpečnosti** a usnadňovat rovněž výměnu příslušných informací.

<sup>3</sup> Středisko Evropské unie pro analýzu zpravodajských informací (EU INTCEM) při Evropské službě pro vnější činnost je součástí společné zpravodajsko-analytické složky EU (SIAC) a je civilním zpravodajským střediskem EU, které poskytuje hloubkové analýzy pro rozhodovací orgány ve všech institucích EU.

- Zintenzivní **strukturované zapojení delegací EU** ve spojení s misemi členských států, dalšími orgány EU a podnikatelskou komunitou EU působící ve třetích zemích; k zajištění účinných příspěvků k posuzování, monitorování a zmírňování rizik v oblasti hospodářské bezpečnosti, včetně usnadnění výměny informací mezi podniky navzájem a mezi podniky a vládami.
- Do třetího čtvrtletí roku 2026 vyhodnotí, do jaké míry akt pro odolnost a mimořádné situace na vnitřním trhu (IMERA) umožňuje shromažďovat informace o dodavatelském řetězci na úrovni podniků ve vysoce rizikových odvětvích. Na základě této analýzy Komise posoudí nutnost dalších opatření.
- Doporučí členským státům, aby jmenovaly **poradce pro hospodářskou bezpečnost** na vysoké úrovni, kteří budou odpovědní za koordinaci posuzování a zmírňování rizik v oblasti hospodářské bezpečnosti mezi jednotlivými vládami. Komise podpoří lepší koordinaci politik a společné akce tím, že bude **tyto poradce pravidelně svolávat na společné jednání**. Vyzývá rovněž Radu EU, aby zvažila pravidelné svolávání příslušných složení Rady k jednání na politické úrovni.
- Vytvoří **skupinu důvěryhodných poradců složenou ze zástupců podniků EU**, která by mimo jiné poskytovala poradenství ohledně konkrétních rizik a možných reakcí na ně a diskutovala o strategiích snižování rizik. Komise bude pravidelně zvat zástupce průmyslu, aby se účastnili odvětvových diskusí v rámci sítě pro hospodářskou bezpečnost, a v případě potřeby bude informovat evropské komisaře.
- Zřídí **informační portál o odolnosti obchodu**, který by v rámci portálu pro přístup na trhy (A2M) poskytoval podnikům v EU aktuální informace o vývozních omezeních a dalších restriktivních opatřeních zavedených třetími zeměmi, jakož i o potenciálních rizicích spojených s potřebou budovat odolnost EU.
- Rozšíří **Observatoř pro kritické technologie** s cílem identifikovat, monitorovat a analyzovat obranný a kosmický průmysl a související dodavatelské řetězce, zahrnout nově vznikající technologie a podporovat provádění výsledných technologických plánů EU na úrovni EU a na vnitrostátní úrovni.
- Využije budoucí **Odborné centrum pro bezpečnost výzkumu** k podpoře bezpečnosti výzkumu a zvýšení odolnosti výzkumné komunity, mimo jiné vytvořením platformy náležité péče na podporu univerzit při výběru jejich mezinárodních partnerů.
- Prozkoumá způsoby, jak sladit a případně **začlenit kandidátské země do našeho přístupu k hospodářské bezpečnosti**, zejména v oblastech, kde jejich zranitelnost v oblasti hospodářské bezpečnosti může představovat bezpečnostní riziko pro EU.

Na základě posílené analýzy a správy může EU lépe plnit své cíle v oblasti hospodářské bezpečnosti tím, že i) vyjasní a zlepší používání stávajících nástrojů a ii) v případě potřeby vytvoří nástroje nové.

Za prvé, **Komise upraví způsob, jakým používá některé své nástroje**, aby byly účinnější při řízení rizik pro hospodářskou bezpečnost, a bude usilovat o zlepšení koordinace mezi těmito nástroji.

**Komise podnikne následující kroky ke zlepšení používání nástrojů:**

→ Financování z prostředků EU:

- V budoucnu bude Komise **ve svých finančních aktivitách podněcovat projekty, které podporují hospodářskou bezpečnost EU**.
- Zejména by měla mobilizovat dostatečnou úroveň financování pro snížení závislostí u kritických technologií, komponentů a materiálů, zejména ve strategických odvětvích, jako je kosmický průmysl a obrana, včetně plné realizace technologických plánů Observatoře pro kritické technologie (OCT).
- Komise, členské státy a prováděcí partneři by se měli snažit zabránit přístupu vysoce rizikových subjektů k citlivým akcím podporovaným Unií. Článek 136 finančního nařízení poskytuje horizontální právní základ pro ochranu bezpečnosti a veřejného pořádku EU při provádění rozpočtu EU Komisí a prováděcími partnery. To umožňuje zabránit vysoce rizikovým subjektům v čerpání finančních prostředků EU a omezit přístup k finančním prostředkům EU ve strategických odvětvích a oblastech kritických technologií a infrastruktury subjektům ze třetích zemí, které ohrožují zájmy hospodářské bezpečnosti EU. Aby se předešlo pochybnostem, měli by se prováděcí partneři zdržet podpory projektů, které jsou v rozporu s výše uvedeným, a to i v rámci operací na vlastní riziko. Za tímto účelem a za účelem zajištění lepšího sladění politik programů EU s cíli v oblasti hospodářské bezpečnosti budou v prvním čtvrtletí roku 2026 k dispozici pokyny, které podpoří rozvoj soudržnějšího a účinnějšího přístupu. Komise bude dále vybízet členské státy, **skupinu EIB a další mezinárodní finanční instituce / národní rozvojové banky a instituce, které provádějí vnitrostátní nebo unijní rozpočty**, aby upřednostňovaly podporu podnikům v EU, které snižují zahraniční závislost v kritických odvětvích, zejména v případě konkrétních projektů, kritických technologií a kritické infrastruktury, které jsou považovány za vysoce rizikové. Stejně tak by měl být dodavatelům z vysoce rizikových třetích zemí znemožněn přístup k financování ze strany EU a členských států, pokud jsou tyto třetí země na základě specifických kritérií označeny za země, které ohrožují zájmy hospodářské bezpečnosti EU.

→ Prověřování přímých zahraničních investic:

- Vypracuje **pokyny** vycházející ze zkušeností s prováděním stávajícího nařízení o prověřování přímých zahraničních investic, aby se zajistil konzistentní přístup vnitrostátních prověřovacích orgánů k prověřování, a to i ve strategických odvětvích. Pokyny by rovněž stanovily, jak zohlednit potenciální kumulativní riziko řady investic. To bude doplněno pokyny týkajícími se vzájemného působení mezi požadavky na úrovni EU a uplatňováním vnitrostátních mechanismů prověřování ve finančním odvětví.

→ Kontrola vývozu zboží dvojího užití:

- Provede **celkové hodnocení** nařízení o kontrole vývozu zboží dvojího užití. V rámci tohoto hodnocení Komise posoudí, zda nařízení dosahuje svých cílů v kontextu nové geopolitické a geoeconomické skutečnosti, včetně dopadů rostoucího využívání jednostranných kontrol, které mohou mít dopad i na jednotný trh. Spolu s členskými státy bude i nadále zkoumat, jak v tomto novém kontextu účinně přijmout evropské kontroly v nově vznikajících technologických oblastech. Během procesu hodnocení Komise zajistí aktivní oslovení zúčastněných stran z členských států, průmyslu, výzkumných ústavů a akademické obce.

→ Nástroje na ochranu obchodu:

- Pokud je zahájen případ, který má význam pro hospodářskou bezpečnost EU, **bude hospodářská bezpečnost EU zohledněna při vedení šetření a navrhování možných opatření.**

→ Nástroje pro vnitřní trh, cla a hospodářskou soutěž:

- Bude plně využívat **nařízení o zahraničních subvencích** k zachování spravedlivé hospodářské soutěže v oblastech, kde zahraniční subvence vedou k narušení hospodářské bezpečnosti.
- Bude povzbuzovat členské státy, aby plně využívaly stávající možnosti státní podpory, jako je rámec státní podpory Dohody o čistém průmyslu, pokyny k regionální podpoře, rámec pro výzkum, vývoj a inovace, obecné nařízení o blokových výjimkách a důležité projekty společného evropského zájmu, jakožto nástroje pro budování větší odolnosti.
- **Přezkoumá využívání strategických celních nástrojů (pozastavení cel, autonomní kvóty) pro klíčové vstupy s cílem podpořit konkurenceschopnost podniků Unie.**

Za druhé, Komise **vypracuje nová opatření** na podporu hospodářské bezpečnosti EU.

**Komise:**

- Prozkoumá pilotní zavedení **mechanismu monitorování startupů na úrovni EU, jehož cílem by bylo identifikovat startupy v oblastech kritických technologií, které jsou ohroženy rizikem nepřátelských zahraničních akvizic**, a přesměrovat je k investičním alternativám EU a dalším formám podpory (např. poradenství, budování kapacit, zprostředkování kontaktů s investory). Tento mechanismus by fungoval v souladu se stávajícími iniciativami, jako je Strategie EU pro startupy a scaleupy.
- Bude spolupracovat s orgány dohledu na monitorování **portfoliových investic** (které nespadají do oblasti působnosti mechanismu koordinace přímých zahraničních investic) v oblastech, které byly z hlediska hospodářské bezpečnosti označeny za vysoce rizikové.
- Zahrne složku hospodářské bezpečnosti pro klíčová strategická odvětví do připravovaného **nástroje pro koordinaci konkurenceschopnosti.**

- Posílí průmyslovou základnu EU a odolnost dodavatelských řetězců prostřednictvím **aktu o akcelérátoru průmyslu**.
- Jak je uvedeno v dokumentu ResourceEU, bude dále rozvíjet **sekundární trhy s** kritickými surovinami, mimo jiné prostřednictvím aktu o oběhovém hospodářství, aby se usnadnilo financování strategických projektů kritických surovin v oblastech, které byly z hlediska hospodářské bezpečnosti označeny za vysoce rizikové.
- Do 3. čtvrtletí 2026 posoudí způsoby **posílení ochrany průmyslu před nespravedlivými obchodními politikami a negativním vývojem na světovém trhu, jako je nadměrná kapacita**. Komise zde vyhodnotí účinnost a přiměřenost stávajících nástrojů a zváží nutnost případných nových opatření.
- Přezkoumá **blokovací nařízení**, aby se zjednodušilo jeho uplatňování a snížily náklady na dodržování předpisů pro osoby a podniky v EU a aby se vytvořil věrohodný odrazující prostředek proti extraterritoriálnímu uplatňování sankcí přijatých určitou třetí zemí. Tím se posílí evropská hospodářská bezpečnost, neboť hospodářské subjekty v EU budou lépe chráněny před protichůdnými opatřeními třetích zemí a bude zajištěn předvídatelnější, účinnější a asertivnější rámec.
- Prozkoumá možnosti, jak povzbudit společnosti v konkrétních vysoce rizikových odvětvích, aby si zajistily **dodávky od nejméně dvou různých dodavatelů** a omezily vystavení jedinému dominantnímu dodavateli.
- Prozkoumá možnosti poskytnutí **finanční podpory společností, na které se vztahují rozhodnutí o prověřování přímých zahraničních investic**, v situacích, kdy by bez investice mohla být ohrožena jejich finanční životaschopnost, aniž by byla dotčena pravidla státní podpory.
- V rámci revize směrnic o veřejných zakázkách **navrhne evropská preferenční kritéria v konkrétních strategických odvětvích**, v nichž naše veřejné zakázky stimulují poptávku po vedoucím postavení evropského průmyslu, zvyšují naši odolnost a zmírňují bezpečnostní rizika.
- Bude podněcovat společnosti ke **snížování závislostí v oblastech nových technologií** v rámci připravovaného aktu o čipech 2.0, aktu o kvantové technologii, aktu pro rozvoj cloudu a umělé inteligence a strategie Komise pro otevřený zdrojový kód.
- Využije nadcházejícího přezkumu **aktu o kybernetické bezpečnosti** k zavedení omezení přístupu vysoce rizikových dodavatelů ke kritické infrastruktuře na úrovni EU.

## 5. Závěr

EU je i nadále pevně odhodlána podporovat otevřený a na pravidlech založený obchod, investiční vztahy a mezinárodní spolupráci. Proto bude i nadále podporovat otevřený obchod a investice s partnery z celého světa a těžit z nich. V dnešním geopolitickém prostředí je zároveň nezbytné zajistit hospodářskou bezpečnost EU. Řešení rizik, která s sebou nese

otevřenost, je klíčem k jejímu zachování, stejně jako k naší širší bezpečnosti a konkurenceschopnosti našeho průmyslu.

EU již má k dispozici mnoho nástrojů, jak tento cíl naplnit. Tyto nástroje je nyní třeba strategicky využívat a v případě potřeby dále zdokonalovat, aby bylo možné důvěryhodně odrazovat od hrozeb pro hospodářskou bezpečnost EU ještě před jejich vznikem a účinně reagovat, když k nim dojde. K dosažení tohoto cíle je zapotřebí, aby Komise, Evropský parlament a členské státy pracovaly v součinnosti a úzce spolupracovaly s průmyslem na účinném a informovaném rozhodování.

EU je odhodlána proaktivněji, strategičtěji a koordinovaněji využívat všechny dostupné nástroje k vybudování dlouhodobě silného, bezpečného a odolného hospodářství a k efektivnímu fungování v nových geopolitických a geoekonomických podmínkách, které ovlivňují světový obchod.