# Studie o bezpečnostním trhu EU

**Autor:** Generální ředitelství pro migraci a vnitřní záležitosti (Červenec 2022)

**Zdroj:** Studie

## Souhrn

**Evropská komise zveřejnila studii o bezpečnostním trhu EU s cílem lépe porozumět trhu civilní bezpečnosti EU a jeho dynamice. Studie bude sloužit jako srovnávací nástroj poskytující spolehlivé aktuální informace o trhu EU, včetně oblastí boje proti kriminalitě a terorismu, odolnosti kritické infrastruktury, správy hranic a řízení rizik katastrof, a to jak pro nabídku, tak pro poptávku.**

Bezpečnostní trh v EU je stále do značné míry nedostatečně prozkoumán a roztříštěný napříč zeměpisnými oblastmi, bezpečnostními oblastmi a průmyslovými odvětvími. Tato studie se snaží o spolehlivý přehled trhu EU a poskytnutí potřebných údajů umožňujících lepší analýzu jeho dynamiky, včetně trendů jeho vývoje. Důležitým hlediskem pro tuto studii je soulad mezi bezpečnostním výzkumem, průmyslem samotným a prioritami EU v bezpečnostní politice. Studie uvádí hlavní zjištění o dynamice trhu civilní bezpečnosti EU, jeho trendech a potenciálním vývoji, formuluje závěry a navrhuje doporučení pro budoucí opatření.

**Studie vytvořila čtyři nástroje:**

**Prvním** výstupem studie jsou budoucí scénáře trhu civilní bezpečnosti, který se snaží odpovědět na následující ústřední otázku: „Jak bude vypadat trh civilní bezpečnosti EU do roku 2032?“ Toto cvičení spojilo pozorovanou dynamiku trhu a plánování scénářů, což znamená proces, který vede k extrémním, ale věrohodným alternativním hypotézám o tom, jak by se svět mohl vyvíjet, navržených speciálně tak, aby upozornil na rizika a příležitosti.

**Druhým** klíčovým výstupem studie je taxonomie, tj. společný jazyk nebo harmonizovaná terminologie pro bezpečnostní produkty a služby.

**Třetím** klíčovým výstupem je katalog zúčastněných stran v oblasti civilní bezpečnosti EU, a to jak na straně poptávky, tak na straně nabídky, které mohou uživatelé prozkoumat prostřednictvím interaktivní mapy. Katalog zúčastněných stran poskytuje reprezentativní vzorek aktérů zapojených do odvětví civilní bezpečnosti na základě údajů o zadávání zakázek a výzkumu a inovací shromážděných a analyzovaných pro tuto studii (tj. kupující a prodejci bezpečnostních produktů a služeb na základě smluvních údajů).

**Čtvrtým** výstupem je **model segmentace** trhu.

**Výsledky studie jsou důležité pro podporu různého publika:**

- **Tvůrci politik** a **vlády** mohou použít výsledky jako vstup pro formulaci a programování politiky a také k vyjádření politických nástrojů (např. financování) k překonání tržních omezení pro přijímání inovativních bezpečnostních řešení.
- **Bezpečnostní průmysl EU, včetně malých a středních podniků**, může výsledky využít k porovnávání svých investic, k utváření své obchodní strategie a k lepší viditelnosti poptávky i potenciálních konkurentů mimo EU.
- **Provozovatelé EU, uživatelé, předepisující osoby a zadavatelé veřejných zakázek** mohou výsledky studie využít k lepší viditelnosti nabídky a plánování rozvoje schopností na základě důkladné znalosti současné a předpokládané průmyslové kapacity EU.

## K vybraným částem dokumentu

**Účel studie**

Celkovým účelem tohoto zadání je vytvořit spolehlivý přehled o situaci na bezpečnostním trhu v EU a získat potřebná data umožňující lepší analýzu jeho dynamiky, včetně trendů jeho vývoje. Na základě předchozích studií o trhu civilní bezpečnosti EU si tato studie klade za cíl poskytnout první jasný přehled trhu civilní bezpečnosti EU, včetně segmentace trhu.

Za tímto účelem studie nejprve charakterizuje trh EU s bezpečností tím, že vypracuje zdůvodnění segmentace trhu, zmapuje zúčastněné strany poptávky a nabídky a taxonomii bezpečnosti. Dále poskytuje komplexní pohled na dynamiku trhu z hlediska hodnoty, nabídky a poptávky, konkurence a trendů v současnosti i budoucnosti. Nakonec přináší závěry a doporučení pro trh s bezpečností, pokud jde o tvorbu politik, technologie, investice a data. Důležitým hlediskem pro tuto studii je soulad mezi bezpečnostním výzkumem, samotným průmyslem a prioritami EU v bezpečnostní politice. Nakonec studie také zkoumá, do jaké míry je (a může být lépe) zajištěna nezávislost bezpečnostního průmyslu a souvisejících technologií.

**Boj proti zločinu a terorismu**

V oblasti civilní bezpečnosti jsou různé oblasti civilní bezpečnosti často do určité míry vzájemně propojeny. Jak je vidět v předchozí kapitole, migrační krize – která způsobila obrovské problémy pro správu hranic v Evropě – byla výsledkem různého problematického vývoje na Blízkém východě. Jedním z těchto vývojů byl vzestup teroristických hnutí jako ISIS, islamistická militantní džihádistická skupina a bývalý neuznaný kvazistát. Teroristická skupina měla během svého povstání také za cíl narušit evropskou bezpečnost a vytvořit nepřetržitou atmosféru strachu prostřednictvím cílených teroristických útoků po celé Evropě. V důsledku toho bylo vyčleněno mnoho finančních prostředků na prevenci těchto útoků.

Kromě rizika, které představují teroristické útoky, je třeba vyčlenit vnitrostátní a evropské finanční prostředky na ochranu evropské společnosti prostřednictvím prevence a boje proti trestné činnosti. Evropa čelí širokému spektru kriminálních aktivit, jako je počítačová kriminalita, nelegální obchod s drogami, environmentální kriminalita, obchod s nelegálními střelnými zbraněmi a výbušninami, podvody, podvody, obchodování s lidmi, podvody s dokumenty, současné padělání a další.

Podle obdržených údajů bylo na boj proti trestné činnosti a terorismu v období 2015–2020 přiděleno více než 7,7 miliardy EUR. Většina těchto prostředků pochází z národních výdajů. To se liší od dříve vysvětlené oblasti správy hranic, kde byly nejvýznamnější výdaje na úrovni EU (AMIF ISF, Frontex a eu-LISA), a nikoli na vnitrostátní úrovni.

Kromě vnitrostátních výdajů, které budou podrobně posouzeny níže, patří mezi největší výdaje dva programy EU: fond Horizont a Fond pro vnitřní bezpečnost. Pokud jde o posledně jmenovaný, jeho cíle jsou jasně v souladu s cíli uvedenými v této oblasti civilní bezpečnosti, konkrétně (1) prevence a boj proti terorismu a radikalizaci, závažné a organizované trestné činnosti a kybernetické kriminalitě (2) pomoc a ochrana obětí trestných činů a (3) příprava na incidenty, rizika a krize související s bezpečností, ochrana proti nim a jejich účinné řízení.

Při hlubším pohledu na výdaje na tuto oblast civilní bezpečnosti v průběhu času se zdá, že se až do roku 2019 jedná o trvale rostoucí výdaje. To je v souladu s náhlým nárůstem teroristických útoků v tomto období. Pak dochází k náhlému poklesu financování, který může souviset s výrazným poklesem počtu teroristických útoků a zatýkání, jakož i náhlý nárůst finančních prostředků na potlačení pandemie koronaviru a zmírnění jejích hospodářských a sociálních dopadů.

Shromážděné údaje naznačují, že Francie je v této oblasti civilní bezpečnosti zdaleka největším utrácejícím. Když se zaměříme na francouzské výdaje na obrázku níže, zdá se, že od roku 2016 (120 milionů EUR) do roku 2018 (700 milionů EUR) prudce stoupá, aby pak v roce 2020 klesal (100 milionů EUR). Tento vzorec do jisté míry odpovídá hlavním útokům, kterým Francie čelila (útok na Charlie Hebdo a útoky v Paříži v roce 2015, útok v Nice v roce 2016 a útok ve Štrasburku v roce 2018).

Bez ohledu na francouzské výdaje se zdá, že všechny ostatní členské státy vynakládají podobnou částku na boj proti zločinu a terorismu. V případě Itálie a Nizozemska došlo během jednoho roku (2019) k náhlým skokům ve výdajích na přibližně 450 milionů EUR (viz obrázek níže). Podobný vzorec lze identifikovat u ostatních hlavních členských států utrácejících v této oblasti civilní bezpečnosti. Tento trend se neomezuje pouze na výdaje členských států. Také fond Horizon, hlavní přispěvatel k boji proti zločinu a terorismu, se řídí tímto vzorem.

Když přiblížíme výdaje evropských fondů, je pozoruhodné, že fond Horizon je považován za čtvrtého největšího přispěvatele v této oblasti civilní bezpečnosti. Podrobnější analýza na

obrázku níže uvádí, že většina finančních prostředků je alokována na sledovací systémy, řízení přístupu k dokumentům a objektům/osobám a také na produkty a služby digitální bezpečnosti.

Abychom získali lepší přehled o cílech výdajů v této oblasti civilní bezpečnosti, je možné podat přehled produktů a služeb, do kterých Evropská unie a její členské státy investují. Jak je uvedeno na obrázku níže, největší náklady představují investice do (policejních) vozidel a sledovacího zařízení, následují produkty a služby digitálního zabezpečení a vybavení OOP. Toto rozdělení naznačuje, že členské státy stále výrazně více investují do tradičních zdrojů pro boj proti trestné činnosti.

Data neukazují žádný znatelný nárůst rozvoje boje proti počítačové kriminalitě (obrázek níže). V letech 2016 a 2019 došlo k nejvýznamnějším investicím. Abychom získali přesnější přehled o vývoji investování v boji proti počítačové kriminalitě, byly produkty a služby související s touto oblastí podrobně popsány na obrázku níže. Za prvé je zřejmé, že absolutní investice do těchto produktů a služeb jsou podstatně nižší než do klasičtějších kategorií, jako jsou bezpečnostní vybavení, sledovací systémy a vybavení pro odstrašení/prevenci (což by zahrnovalo nesmrtící zbraně, střelné zbraně atd.). Kromě postupného nárůstu investic do digitální forenzní analýzy se také zdá, že neexistuje žádný vzorec ve výdajích za jiné digitální produkty a služby.

**Kritická infrastruktura**

Měnící se povaha hrozeb vyžaduje zvýšenou ochranu evropské kritické infrastruktury a také dodatečné investice do kapacit EU pro odolnost k zabezpečení její kritické infrastruktury. V roce 2018 byl veškerý letecký provoz v Londýně zastaven kvůli nedostatku infrastruktury na ochranu před hrozbami dronů, nazývanými také „incident dronů na letišti Gatwick“. To jasně ukazuje potřebu bezpečné, zabezpečené a aktuální infrastruktury. Ať už se jedná o jaderné elektrárny, logistické uzly, letiště, kancelářské budovy, přístavy a datová centra, všechny se musí spoléhat na zabezpečenou a bezpečnou infrastrukturu, aby správně fungovaly.

Navíc vzhledem k rostoucí závislosti kritické infrastruktury na digitálních službách a také vývoji nových technologií (např. šíření IOT, cloudu, dronů) se kybernetická bezpečnost stala zásadní strategickou prioritou. Tato závislost na technologiích, a tím i vystavení kybernetickým hrozbám, byla zvýrazněna krizí Covid-19.

Kromě toho došlo k prudkému nárůstu hrozeb, které kombinují fyzický i kybernetický aspekt, známé také jako hybridní hrozby (např. brání demokratickému rozhodování, destabilizují vlády pomocí dezinformací…). Tyto hrozby vyžadují, aby EU a její členské státy identifikovaly a zmírnily slabá místa ve vztahu ke své kritické infrastruktuře z jiného úhlu.

Aby se EU vyrovnala s těmito výzvami, zvyšuje své úsilí, pokud jde o výdaje na kritickou infrastrukturu. Jak bylo vysvětleno výše, lze tuto oblast bezpečnosti považovat za nejvýznamnější oblast z hlediska výdajů. Celkem bylo v posledních letech (2015–2020) v této

oblasti vynaloženo přibližně 19 miliard EUR. Zatímco od roku 2015 do roku 2016 došlo k poklesu o 18 %, výdaje od té doby až do roku 2020 neustále rostou. Ve skutečnosti se celkové výdaje na kritickou infrastrukturu zdvojnásobily, z celkových výdajů 2,48 miliardy EUR v roce 2016 na EUR 4,89 miliardy.

Celkem bylo v posledních letech (2015–2020) v této oblasti vynaloženo přibližně 19 miliard EUR. Zatímco od roku 2015 do roku 2016 došlo k poklesu o 18 %, výdaje od té doby až do roku 2020 neustále rostou. Ve skutečnosti se celkové výdaje na kritickou infrastrukturu zdvojnásobily, z celkových výdajů 2,48 miliardy EUR v roce 2016 na EUR 4,89 miliardy.

V roce 2020 dojde v rámci programu CEF k výraznému nárůstu. To je způsobeno především dvěma projekty financovanými v rámci tohoto programu. První byla poskytnuta pobaltským zemím v hodnotě 1 miliardy EUR, zatímco druhá byla přidělena Slovensku a Maďarsku v hodnotě 300 milionů EUR. Smyslem obou projektů je dosažení plně fungujícího a propojeného vnitřního trhu s energií.

Správné fungování vnitřního trhu s energií závisí na bezpečnosti dodávek elektřiny, zemního plynu a ropy. Je proto zásadní zajistit, aby byla zajištěna bezpečnost dodávek energie spolu s odpovídající úrovní propojení mezi členskými státy. Závislost EU na dovozu energie spolu s geopolitickým napětím těchto třetích zemí, jako je Rusko a Ukrajina, mohou ohrozit bezpečnost dodávek energie v EU (např. současná rusko-ukrajinská krize v roce 2022, rusko-ukrajinská plynová krize během zima 2008-2009). Z tohoto důvodu se fondy EU zaměřují na fungování energetického trhu, jak je uvedeno výše.

Na vnitrostátní úrovni existuje 5 nejvyšších výdajů, které na tuto oblast civilní bezpečnosti přidělují více než 1 miliardu EUR. Mezi tyto země patří nejprve Francie jako největší utrácející (1,83 miliardy EUR), následuje Česko (1,44 miliardy EUR), Rumunsko (1,31 miliardy EUR), Slovinsko (1,25 miliardy EUR) a Německo (1,21 miliardy EUR). Ze všech těchto členských států mají Česko i Rumunsko výrazně vyšší výdaje v jednom roce ve srovnání s jejich výdaji v jiných letech. Další trvale vysoké výdaje na kritickou infrastrukturu jsou Nizozemsko (940 milionů EUR) a Španělsko (840 milionů EUR).

Podle údajů ostatní členské státy vynakládají na kritickou infrastrukturu ročně většinou méně než 100 milionů EUR. Existují však určité odlehlé hodnoty, podobně jako v Česku a Rumunsku, kde lze zjistit náhlý nárůst ročních výdajů. To je případ Slovenska (500 milionů EUR v roce 2019), Finska (420 milionů EUR v roce 2018), Rakouska (390 milionů EUR v roce 2020), Chorvatska (275 milionů EUR v roce 2019) a Portugalska (225 milionů EUR v roce 2018).

Pozoruhodným nedostatkem v analýze této bezpečnostní oblasti je Itálie. Na základě našich údajů se umístila pouze na 12. místě ve výdajích na kritickou infrastrukturu ve výši 400 milionů EUR během 5 let.

Pokud jde o produkty a služby, logistika a veřejné služby tvoří 30 % všech výdajů v této oblasti civilní bezpečnosti. Po této kategorii produktů a služeb následuje kritická interoperabilní komunikace. Následují vozidla a OOP/bezpečnostní vybavení.

**Katalog zúčastněných stran**

Přestože katalog zúčastněných stran představuje důležitý zdroj informací pro analýzu, jeho záměrem není poskytnout vyčerpávající obrázek o celém bezpečnostním ekosystému; spíše poskytuje reprezentativní vzorek aktérů zapojených do odvětví civilní bezpečnosti na základě údajů o zadávání zakázek a výzkumu a inovací shromážděných a analyzovaných pro tuto studii (tj. kupující a prodejci bezpečnostních produktů a služeb na základě smluvních údajů).

**Účastníci na straně poptávky** v katalogu představují ty, kteří požadují produkty a služby pro účely civilní bezpečnosti v rámci jedné z bezpečnostních oblastí. Hlavními zúčastněnými stranami jsou ministerstva, agentury, donucovací síly a výzkumné instituce. **Účastníci na straně nabídky** v katalogu představují ty, kteří poskytují produkty a služby pro účely civilní bezpečnosti v rámci jedné z bezpečnostních oblastí.

Katalog je plánován jako živý produkt, který by měl být udržován a aktualizován po dokončení studie (např. mohou být přidáni noví zainteresovaní, jak se ekosystém rozrůstá nebo se mění). Poskytnuté informace vycházejí z údajů shromážděných do května 2022.

| Pillar level L1 | **Disaster Resilient Societies** | | |
|---|---|---|---|
| L2 | **Natural disasters** | **Accidental disasters** | **Human-induced disasters** |
| L3 | Geophysical | Natech | |
| L4 | Earthquake<br>Mass movement<br>Volcanic activity | | |
| L3 | Meteo-Hydro-Climato | Chemical / Biological / Humanitarian | Chemical / Biological / Humanitarian |
| L4 | Flood<br>Heatwave<br>Hurricane<br>Storm<br>Wildfire<br>Drought | Animal and plant safety/security<br>Food and water safety/security<br>Air safety | Animal and plant safety/security<br>Food and water safety/security<br>Air safety |
| L3 | Epidemics/ Pandemics | Radiological / Nuclear | Radiological / Nuclear |
| L4 | Human<br>Animal<br>Plant | Nuclear meltdown<br>Industrial accident<br>technological accident<br>Cyber-catastrophe<br>Infrastructure failure | Nuclear meltdown<br>Industrial accident<br>technological accident<br>Cyber-catastrophe<br>Infrastructure failure |
| L3 | Extra-terrestrial | Explosives | Explosives |

| Pillar level L1 | **Fighting Crime and Terrorism** | | | |
|---|---|---|---|---|
| L2 | **Organised crime** | **Terrorism & radicalisation** | **Cybercrime** | **Other/horizontal and societal issues** |
| L3 | Counterfeit goods & documents | Terrorism financing | Child sexual abuse | Petty crime |
| L4 | Counterfeit pharmaceuticals<br>Counterfeit goods<br>Dangerous products<br>Currency<br>Falsified documents | | | |
| L3 | Environmental crime | Protection of public spaces | Online identity theft | Domestic violence and sexual violence |
| L4 | Illicit hunting and trading of wildlife<br>Illegal mining and logging<br>Illegal waste disposal and shipments | Drone attacks<br>Mass shootings | | |
| L3 | Trafficking of humans and goods | Radicalisation | Dark net (illegal markets/cryptocurrencies) | Disinformation & fake news |

| Pillar level L1 | **Fighting Crime and Terrorism** | | | |
|---|---|---|---|---|
| L4 | Illicit drugs production and trafficking<br>Firearms trafficking<br>Trafficking in human beings and human smuggling<br>Trafficking cultural goods | Societal issues<br>Terrorist content online<br>Foreign terrorist fighters | | |
| L3 | Economic crime, corruption and fraud | Explosives & explosive precursors | Digital forensics | Hate speech |
| L4 | VAT fraud<br>Money laundering<br>Corruption | | | |
| L3 | Cargo crime | CBRN threats | Non-cash payment fraud | Conventional forensics |
| L3 | Organised property crime | | Attacks against information systems | Travel intelligence (passenger Name record) |
| L3 | | | Threats related to encryption and 5G | Youth criminality |
| L3 | | | | Community policing |

| Pillar level L1 | **Resilience of Critical Infrastructure** | | | | |
|---|---|---|---|---|---|
| L2 | Transport | Energy | Health | Communication & information technology | Supply Chains and sensitive industries |
| L3 | Airports<br>Ports<br>Railways<br>Traffic control systems<br>Roads and highways | Electrical power<br>Oil and gas production<br>Storage facilities | Hospitals<br>Healthcare and blood supply facilities<br>Laboratories and pharmaceuticals<br>Search and rescue<br>Emergency services | Network information systems<br>Telecommunications<br>Broadcasting systems<br>Internet | Sensitive industrial plants<br>Security of supply<br>Food |
| L2 | Finance | Critical water infrastructure | Urban Built environments | Space | Other |
| L3 | Banking<br>Securities and investment<br>Cash distribution<br>Financial transactions outside of banks | Wastewater treatment<br>Dams<br>Supply and sanitation systems | Public spaces<br>Soft targets<br>Smart city assets<br>Buildings | Ground segments | Research facilities<br>Public response capabilities (police, civil protection)<br>Elections and democratic processes |