POLICY PAPER:

KRIZOVÁ PŘIPRAVENOST A ODOLNOST EVROPSKÉ UNIE: JAK PŘIPRAVIT (NEJEN) ČESKO NA MIMOŘÁDNÉ SITUACE?

AUTOŘI

Veronika Víchová	CENTRUM PRO INFORMOVANOU SPOLEČNOST
Andrea Michalcová	CENTRUM PRO INFORMOVANOU SPOLEČNOST

CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

V Centru pro informovanou společnost přinášíme a prosazujeme řešení pro bezpečnost Česka, která stojí na spolupráci státu, firem, občanské společnosti i každého z nás. Rozvíjíme schopnosti země čelit vnějším hrozbám, vlivu Ruska i budoucím krizím.

www.informedsociety.cz

TATO PUBLIKACE BYLA PŘIPRAVENA JAKO PODKLAD PRO NÁRODNÍ KONVENT O EU.

Národní konvent o Evropské unii je projekt koordinovaný Úřadem vlády ČR ve spolupráci s odbornými garanty jednotlivých kulatých stolů – experty na projednávaná témata. Národní konvent poskytuje místo pro diskuzi o aktuálních evropských tématech pro relevantní aktéry – představitele veřejné správy na národní i lokální úrovni, zástupce evropských institucí, odbornou veřejnost a další zainteresované osoby. V rámci Konventu jsou za tímto účelem pravidelně organizovány odborné kulaté stoly, jejichž výstupem jsou doporučení pro vládu ČR. Bližší informace o fungování Národního konventu o EU naleznete na webu Tvoříme Evropu.

CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

ÚVOD: ROSTOUCÍ TLAK NA EVROPSKOU BEZPEČNOST A PŘIPRAVENOST

Bezpečnostní prostředí Evropské unie a České republiky se v posledních třech letech zásadně proměnilo. Dříve výjimečné jevy se stávají novou normou a ukazují, že nejen státní aparát, ale i společnost jako celek musí být připraveny čelit narůstajícím a komplexním krizím.

Již dnes Rusko vede proti Evropě hybridní válku zahrnující dezinformace, nátlak na energetickou a dopravní infrastrukturu, kybernetické útoky a infiltraci extremistických a antisystémových skupin a vysocí představitelé NATO i členských států EU předpokládají další eskalaci napětí[1]. Ještě větší kapacity zneužívat klíčových zranitelností evropských demokratických společností má Čínská lidová republika. Tyto hrozby jsou stále častější, sofistikovanější a mohou v době krize amplifikovat chaos, snížit důvěru občanů ve stát a podpořit extremismus. Zejména v digitálním prostoru, na sociálních sítích, jako je TikTok nebo Telegram, nebo prostřednictvím zahraničních dezinformačních sítí může docházet k cílené manipulaci veřejnosti.

Vedle narůstající hrozby vojenského konfliktu čelí (nejen) Česká republika i dalším možným budoucím krizím konvenčního i hybridního charakteru. Patří mezi ně např. **uprchlické a migrační vlny** v důsledku válečných konfliktů nebo klimatických změn. Nová vlna uprchlíků by mohla ovlivnit sociální služby, školství, zdravotnictví i veřejné mínění. V případě silného polarizačního tlaku může také destabilizovat politické prostředí.

Silný dopad by rovněž mohly mít **klimatické změny a environmentální krize**. Extrémní sucha, vlny veder, přívalové deště, kůrovcové kalamity nebo znečištění vody a ovzduší mohou mít přímé dopady na zdraví obyvatel, zemědělskou produkci i dostupnost energií a vody. V kombinaci s dalšími krizemi (např. s výpadky sítí) nebo narůstajícími sabotážemi ze strany cizích státních či nestátních aktérů může jít o fatální ohrožení stability.

Celá Evropa má rovněž silnou zkušenost s COVID-19, který ukázal, jak je při **epidemiích a pandemiích** zranitelná infrastruktura zdravotnictví, školství a péče o zranitelné skupiny. S rostoucí globalizací a šířením antibiotické rezistence podle odborníků existuje možnost, že do 10 let dojde k další vážné epidemii nebo pandemii.[2]

V neposlední řadě čelí evropské státní i nestátní instituce a firmy stále rostoucímu počtu **kybernetických útoků a možným technologickým selháním**. Útoky na nemocnice, dopravní systémy nebo energetickou infrastrukturu mohou vést k výpadkům služeb, ztrátě důvěry občanů i ohrožení životů.

---

1 Russia could be ready to attack Nato within five years, says secretary general. *The Guardian* [online]. 2025 [cit. 2025-08-08]. Dostupné z: https://www.theguardian.com/world/2025/jun/09/nato-chief-russia-quantum-leap-defence

2 World Has 28% Risk of New Covid-Like Pandemic Within 10 Years. *Bloomberg* [online]. 2023 [cit. 2025-08-08]. Dostupné z: https://www.bloomberg.com/news/articles/2023-04-14/another-covid-like-pandemic-could-hit-the-world-within-10-years?embedded-checkout=true

Dopady těchto krizí budou širokospektrální. Občané mohou čelit nedostatku základních služeb (např. elektřina, voda nebo zdravotní péče), dezinformacím, chaosu a panice. Zasaženy budou především zranitelné skupiny, jako jsou senioři, děti, osoby s omezenou mobilitou nebo etnické a jazykové menšiny. České firmy se budou potýkat s výpadky energií, přerušením dodavatelských řetězců, absencí zaměstnanců, nebo regulačními zásahy (např. příděly nebo omezení výroby). Neschopnost reagovat v důsledku nepřipravenosti pro ně bude znamenat ekonomické ztráty a ohrožení pracovních míst.

Důsledky krizí ale pocítí i sám stát. Při kumulaci krizí hrozí přetížení složek integrovaného záchranného systému, výpadky rozhodovacích procesů, kolaps důvěry ve státní instituce a oslabení demokratické legitimity. Bez včasné koordinace může stát reagovat pomalu, nekoherentně a bez potřebného dopadu. Navíc je třeba otevřeně říci, že stát nebude schopen zajistit vše, v prvních hodinách a dnech krizí si občané, komunity i firmy musí umět pomoci sami. Z těchto důvodů je třeba chápat krizovou připravenost a odolnost ne jako technickou disciplínu, ale jako **strategickou investici do bezpečnosti, stability a důvěry ve stát**. Jak ukazují mimo jiné zkušenosti ze zemí, jako je Finsko, Švédsko nebo země Pobaltí, budování odolnosti není pouze otázkou dokumentů, ale také vzdělávání, praktických cvičení, školení, partnerství mezi sektory a schopnosti komunikovat s veřejností.

1. EVROPSKÝ RÁMEC KRIZOVÉ PŘIPRAVENOSTI: SILNÉ ZÁKLADY, NOVÁ STRATEGIE

Evropská unie v březnu 2025 představila ambiciózní unijní **Strategii unie připravenosti**[3], která má za cíl významně zvýšit civilní i vojenskou připravenost celé Unie. Strategie vychází z návrhů tzv. Niinistöho zprávy „Společně bezpečněji – posílení civilní a vojenské připravenosti a pohotovosti Evropy" z října 2024 a staví na stejných principech. Strategie přináší ucelený přehled oblastí, které je potřeba posílit, a konkrétních návrhů s cílem vytvořit Unii připravenosti, tedy připravenou a odolnou EU vůči všem přírodním a člověkem způsobeným krizím a katastrofám. Mezi klíčové principy strategie patří:

- **Integrovaný přístup:** Cílem není řešit každou hrozbu samostatně, ale připravovat se kontinuálně na všechny typy krizí, od pandemie, přes hybridní útoky až po přírodní katastrofy.
- **Celospolečenský přístup:** Zahrnuje všechny složky společnosti, včetně veřejného i soukromého sektoru a občanů, pro budování kultury odolnosti.
- **Meziresortní přístup:** Koordinace mezi resorty, členskými státy a EU, propojení civilních a vojenských kapacit.

Strategie obsahuje Akční plán se 30 klíčovými opatřeními zaměřenými na ochranu základních funkcí společnosti, přípravu obyvatelstva, tvorbu kritických zásob, systematickou krizovou koordinaci, civilně-vojenskou spolupráci, prediktivní schopnosti, partnerství s privátním sektorem a zapojení mezinárodních partnerů. Zahrnuje také doporučení pro členské státy, aby podpořily zásoby kritických materiálů a technologií a vybídly občany, aby měli doma zásoby a vybavení na minimálně 72 hodin a byli připraveni na potenciální výpadek proudu či jiných druhů energií.

Tato strategie má zásadní význam také pro Českou republiku, vypíchnout lze například:

- Zavedení evropské kultury připravenosti, například doporučené domácí zásoby, nebo krizová školení občanů, která mohou podpořit i národní odolnost.
- Aktivní implementace směrnic CER, NIS2 nebo Cyber Resilience Act, která je nyní v přípravné fázi, umožní českým institucím lépe chránit kritickou infrastrukturu.
- Zapojení do Unijního mechanismu civilní ochrany (UCPM), systému rescEU a spolupráce se Střediskem pro koordinaci odezvy na mimořádné události (ERCC) umožní koordinovanou reakci na přeshraniční krizové situace, jako jsou např. pandemie nebo energetické výpadky.
- Podpora propojování veřejného a privátního sektoru – zásadní témata jako sdílení zásob, krizová logistika nebo komunikace mohou být převzata přímo do národního přístupu ČR.

3 EU preparedness union strategy. *European Commission* [online]. 2025 [cit. 2025-08-08]. Dostupné z: https://commission.europa.eu/topics/preparedness_en?prefLang=cs

2. ZAHRANIČNÍ INSPIRACE: PŘÍKLADY DOBRÉ PRAXE V KRIZOVÉ PŘIPRAVENOSTI A ODOLNOSTI

Zkušenosti ze zemí, které čelí dlouhodobému bezpečnostnímu tlaku nebo geopolitickým rizikům, ukazují, že vysoká míra připravenosti nevzniká náhodou, ale je výsledkem systematické práce, důvěry veřejnosti a zapojení celé společnosti.

Finsko je považováno za evropského lídra v oblasti krizové připravenosti. Země systematicky rozvíjí koncepty tzv. **komplexní bezpečnosti**[4], které propojují státní instituce, soukromý sektor, obce, média i občanskou společnost. Každý resort i každá větší instituce má vlastní krizové plány, které se pravidelně aktualizují a testují v rámci meziresortních a mezioborových cvičení. Finsko má rovněž síť **regionálních center krizového řízení**[5] a decentralizované sklady zásob. Klíčovým prvkem je vysoká důvěra obyvatel ve stát a armádu[6], která posiluje ochotu spolupracovat a přijímat nezbytná opatření.

Estonsko patří mezi světové průkopníky v oblasti **kybernetické bezpečnosti** a digitální odolnosti. Po rozsáhlém kybernetickém útoku z roku 2007 investovalo do robustní infrastruktury a vzniklo Estonské centrum excelence pro kybernetickou obranu (CCDCOE), dnes působící v rámci struktur NATO. Země pravidelně organizuje kybernetická cvičení (např. Locked Shields) a prosazuje důslednou digitální gramotnost občanů i státních zaměstnanců. Estonský model spočívá v důvěře v e-government, decentralizaci dat a schopnosti rychlé obnovy systémů. V krizové komunikaci je kladen důraz na **rychlost, transparentnost a jednotnost sdělení**.

Litva v reakci na hrozby zejména z Ruska zavedla řadu praktických opatření. Vydala například **příručku "Co dělat v případě války nebo krize"** pro všechny domácnosti.[7] Tato brožura kombinuje rady pro přežití, ochranu před manipulacemi, a základní principy občanské odolnosti.

Podobnou publikaci do domácností distribuovalo také **Švédsko**.[8] To zároveň v roce 2017 obnovilo koncept **totální obrany**, který zahrnuje koordinaci mezi armádou, státními úřady, samosprávou, firmami a občany. Každý region a municipalita má zákonnou povinnost[9] připravit si své vlastní krizové plány

4 Comprehensive security. *The Security Committee, Ministry of Defense of Finland* [online]. 2025 [cit. 2025-08-08]. Dostupné z: https://turvallisuuskomitea.fi/en/comprehensive-security/

5 Wellbeing services counties will be responsible for organising health, social and rescue services. *Ministry of Social Affairs and Health of Finland* [online]. 2025 [cit. 2025-08-08]. Dostupné z: https://stm.fi/en/wellbeing-services-counties

6 OECD Survey on Drivers of Trust in Public Institutions 2024 Results - Country Notes: Finland. *OECD* [online]. 2024 [cit. 2025-08-08]. Dostupné z: https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/finland_596ba5da-en.html

7 If War or Crisis Comes: What Should I Do? *Ministry of National Defence of the Republic of Lithuania* [online]. 2024 [cit. 2025-08-08]. Dostupné z: https://www.iidraudimas.lt/content/uploads/2025/04/Jei-krize-arba-karas-kaip-elgtis-anglu-kalba.pdf

8 In case of crisis or war. *The Swedish Civil Contingencies Agency (MSB)* [online]. 2024 [cit. 2025-08-08]. Dostupné z: https://rib.msb.se/filer/pdf/30874.pdf

9 *The Swedish Act (2006:544) on Municipalities' and Regions' Measures Prior to and During Extraordinary Events in Peacetime and Heightened State of Alert.* 2006.

a počítat s různými scénáři, od blackoutu po válečný konflikt. Součinnost se soukromým sektorem je nedílnou součástí.

Tchaj-wan je příkladem společnosti, která čelí trvalé hrozbě napadení ze strany Číny. Vláda proto důsledně investuje do strategické komunikace, krizového řízení a sebeobrany občanů. Probíhají pravidelná **cvičení celonárodní mobilizace**[10], a to včetně simulací výpadku internetu nebo narušení energetických sítí. Zároveň Tchaj-wan rozvíjí systém **komunitní odolnosti**, v rámci kterého mají jednotlivé čtvrti nebo komunity vlastní zásoby a krizové týmy.[11]

10 What happens in Taiwan's military exercise to defend against China? *BBC* [online]. [cit. 2025-08-08]. Dostupné z: https://www.bbc.com/news/articles/cly21zrnk79o

11 Community Defense: Taiwan's Path to Civil Resilience. *Taiwan Business Topics* [online]. 2025 [cit. 2025-08-08]. Dostupné z: https://topics.amcham.com.tw/2025/03/community-defense-taiwans-path-to-civil-resilience/

3. KLÍČOVÉ ZRANITELNOSTI ČESKÉ REPUBLIKY

Česká republika v současnosti čelí několika zásadním rizikům, která mohou zásadně oslabit její schopnost zvládat krizové a mimořádné situace:

1) MEZIRESORTNÍ A MEZISEKTOROVÁ NESLADĚNOST KRIZOVÝCH PLÁNŮ A NÍZKÁ SCHOPNOST PŘENÉST SCÉNÁŘE DO PRAXE

Přestože Ministerstvo vnitra spravuje Katalog typových činností a typové plány, které stanovují scénáře pro krizové situace (např. povodeň, epidemie, zaručení dodávek energií), tyto dokumenty nejsou závazné pro soukromý a neziskový sektor. Kromě toho existuje systém hospodářské mobilizace podle zákona č. 241/2000 Sb., ale jeho znalost a praktická aplikace jsou velmi omezené. Scénáře zároveň dostatečně nereflektují současný a zejména budoucí možný stav, kdy Česko může čelit vícero krizím najednou. Hlavním problémem zůstává nízká schopnost tyto scénáře převádět do praxe a vytvořit o nich všeobecné povědomí a shodu, využívat je pro mezisektorová cvičení a udržovat aktualizovanou připravenost aktérů na všech úrovních.

2) NEDOSTATEČNÉ POVĚDOMÍ SOUKROMÉHO SEKTORU O ROLÍCH A POVINNOSTECH V KRIZOVÝCH STAVECH

Mnoho firem mimo rámec kritické infrastruktury si neuvědomuje své povinnosti během vyhlášení krizových stavů, jak je definuje Ústava ČR a krizová legislativa (např. stav ohrožení státu, nouzový stav, stav nebezpečí). Často nemají vypracované vlastní krizové plány, nejsou zapojeny do cvičení a netuší, jaká bude jejich role v případě nouze. Přitom právě soukromý sektor zajišťuje klíčové dodávky, logistiku, technologie a služby.

3) NÍZKÁ DŮVĚRA VEŘEJNOSTI VE SCHOPNOSTI STÁTU

Podle analýzy Ministerstva vnitra[12] důvěřuje schopnostem státu zvládat krize mezi 18-42% obyvatel, dle typu krize. Na vyšších příčkách se důvěra ve stát objevuje zejména při povodních nebo požárech, naopak na těch nejnižších se umístily různé typy hybridních útoků ze zahraničí (kybernetické útoky, dezinformace), uprchlická krize, sucho a válka. Nízká důvěra zvyšuje riziko iracionálních reakcí, jako je panika, nerespektování pravidel nebo šíření neověřených informací, což může dopady samotné krize ještě zvýšit.

12 Pod hladinou: Analýza a ponaučení z krizové komunikace během povodní. *Krizový informační tým Ministerstva vnitra* [online]. 2024 [cit. 2025-08-08]. Dostupné z: https://drive.google.com/file/d/19j2qm9Rv-yRgm9V97_zLCHqYvfYsDiM8/view?pli=1

4) SLABÁ PŘIPRAVENOST NA HYBRIDNÍ HROZBY A INFORMAČNÍ CHAOS

Ze zkušeností ze zahraničí jasně vyplývá, že ucelená strategická komunikace státu vůči veřejnosti je klíčová k získání důvěry obyvatelstva. Stát však nemá systémovou nadresortní strategii, jak během komplexní krize, ale i v běžném provozu, efektivně, jednotně a důvěryhodně komunikovat. Chybí kapacity pro monitoring informačního prostoru, včasnou reakci a přímé zapojení důvěryhodných osobností (např. starostů, lékařů, hasičů) napříč resorty. Zásadní jsou rozdíly v kapacitách a plánech jednotlivých resortů. Zatímco např. Ministerstvo vnitra nebo zdravotnictví již některými mimořádnými situacemi prošly a tyto zkušenosti byly schopny přetavit do praktických postupů a plánů, jiné se komunikaci nevěnují vůbec. Rychlé šíření paniky nebo nepřátelských narativů tak mohou zůstávat bez reakce.

5) NEREFLEKTOVANÉ ZRANITELNOSTI NA LOKÁLNÍ ÚROVNI

Obce a kraje jsou často první linií pomoci, např. při výpadku proudu, migraci, záplavách i při panice obyvatel. Přesto často nemají potřebné materiální vybavení, dostatečné metodické vedení, přístup k datům, plánům ani možnost účastnit se centrálních simulací.

4. CO JE POTŘEBA UDĚLAT?

Pro zvýšení krizové připravenosti a odolnosti ČR i EU navrhujeme tato opatření:

1) VYBUDOVAT PROFESIONÁLNÍ A ROBUSTNÍ SYSTÉM STRATEGICKÉ A KRIZOVÉ KOMUNIKACE

Posílení důvěry mezi státem a veřejností je základním předpokladem efektivního zvládání krizí. Ústřední orgány státní správy (zejména ministerstva vnitra, zdravotnictví, průmyslu a obchodu, obrany, či Úřad vlády nebo NÚKIB) by měly mít jasně vymezené a kapacitně posílené týmy pro strategickou a krizovou komunikaci, které by měly:

- Kontinuálně monitorovat informační prostor,
- Reagovat na dezinformace a hybridní hrozby,
- Vést proaktivní a koordinovanou komunikaci směrem k obyvatelstvu,
- Koordinovat komunikaci mezi resorty a zapojovat důvěryhodné aktéry, např. starosty, odborníky nebo složky IZS.

Role a odpovědnosti jednotlivých institucí by měly být jasně definovány ve strategickém dokumentu či kompetenčním rámci. Nabízí se rovněž posílení a koncepční uchopení občanského vzdělávání jako základu pro rozvoj občanských kompetencí klíčových pro úspěšné zvládnutí krizových stavů, jako je schopnost vyhodnotit relevantní a důvěryhodné informace a řídit se jimi, důvěřovat a respektovat pokyny krizových štábů a aktivně se zapojit do zvládání krizí dle svých možností a schopností.

2) LOKÁLNÍ CENTRA ODOLNOSTI

Ministerstvo školství, mládeže a tělovýchovy a Ministerstvo vnitra ve spolupráci s obcemi a občanským sektorem by měly vytvořit síť komunitních center připravenosti a odolnosti. Ta by mimo jiné sloužila k:

- Poskytování informací, školení a simulací,
- Distribuci základního vybavení pro krizové situace,
- Posilování důvěry mezi občany a institucemi skrze místní vazby.

3) JEDNOTNÝ RÁMEC SCÉNÁŘŮ KRIZOVÝCH SITUACÍ

Úřad vlády ve spolupráci s Ministerstvem vnitra, obrany, HZS a krajskými úřady by měl vytvořit prakticky využitelný rámec obsahující:

- popis typových krizí,
- odpovědnosti jednotlivých aktérů v rámci různých krizových stavů i mimo ně,

- harmonogramy cvičení,
- návody pro zapojení podniků, obcí i veřejnosti.

Tento rámec by měl reflektovat stávající typové plány a Katalog činností, ale rozšířit je o mezioborové a mezisektorové propojení a praktickou použitelnost.

4) PRAVIDELNÁ MEZIOBOROVÁ KRIZOVÁ CVIČENÍ

Klíčové resorty (zejména Ministerstva vnitra, obrany a průmyslu a obchodu) ve spolupráci s NÚKIB, kraji a Hospodářskou komorou by měly pořádat pravidelná cvičení zahrnující nejen složky IZS, ale také obce, podniky, školy, nemocnice nebo média. Je potřeba simulovat realistické scénáře, jako je blackout, migrační vlna nebo masový kybernetický útok.

5) PROPOJENÍ FIREM S KRIZOVÝM ŘÍZENÍM STÁTU A ZVÝŠENÍ POVĚDOMÍ O LEGISLATIVNÍCH POVINNOSTECH

Ministerstva průmyslu a obchodu, financí a vnitra ve spolupráci s NÚKIB a podnikovými asociacemi by měla:

- Zřídit krizové sektorové platformy pro sdílení zkušeností,
- Podporovat tvorbu krizových plánů i mimo rámec kritické infrastruktury,
- Zajistit osvětu o právech a povinnostech firem během různých stavů krizového řízení dle legislativy (např. stav ohrožení státu, nouzový stav),
- Poskytnout motivační nástroje pro firmy

ZÁVĚR

Bezpečnostní realita Evropy vyžaduje od členských států odpovědnou, systémovou a proaktivní přípravu na krize. Česká republika má potenciál stát se lídrem v oblasti civilní odolnosti. Má silnou občanskou společnost, schopný soukromý sektor i tradici solidarity. Aby však tento potenciál využila, musí urychleně vybudovat institucionální rámce, navázat partnerství a získat důvěru obyvatel. Evropa bude jen tak odolná, jak odolné budou její jednotlivé státy.

CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

www.informedsociety.cz