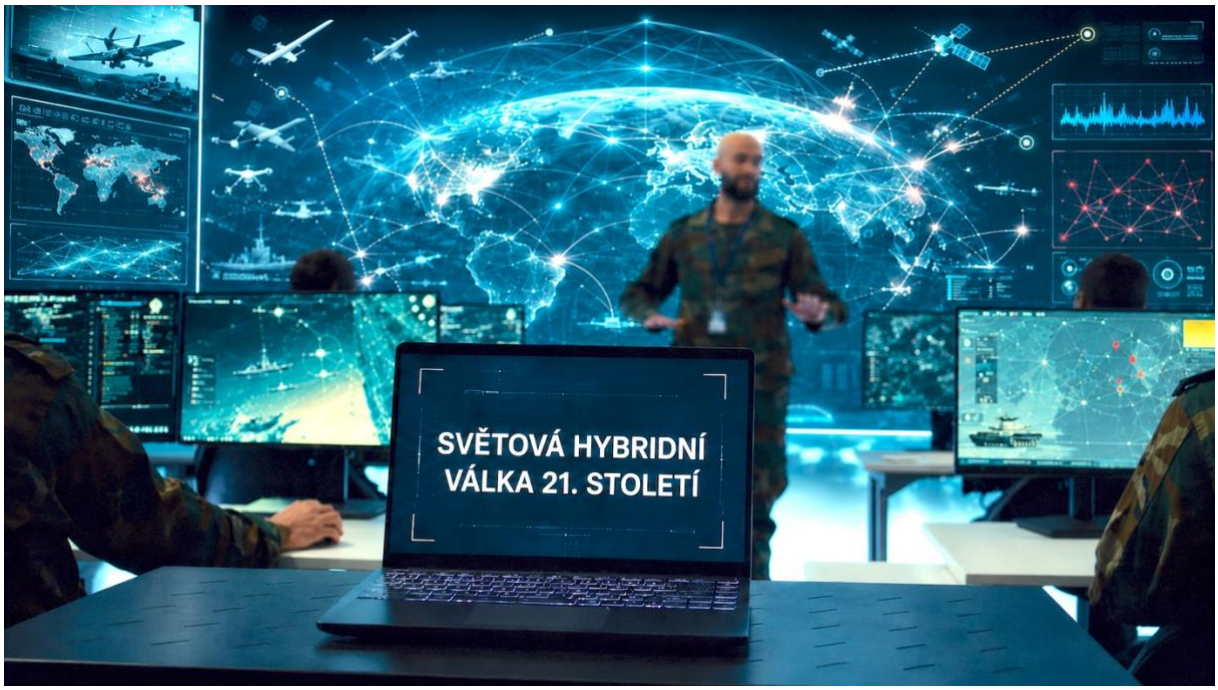
Česká republika: člen EU a NATO
Bezpečnost členských států EU a NATO na prvním místě
Datum vydání: 1. června 2026

CENTRÁLNÍ KYBERNETICKÝ ŠTÍT DEMOKRACIE

Kybernetické přezbrojení členských států EU a NATO je základním předpokladem pro naplňování aliančních závazků, neboť světová hybridní válka 21. století probíhá ve fyzickém i digitálním prostoru současně a s každým dalším dnem představuje rostoucí hrozbu pro demokratickou civilizaci a zvyšuje riziko eskalace bezpečnostních krizí a ozbrojeného konfliktu.

CENTRÁLNÍ KYBERNETICKÝ ŠTÍT DEMOKRACIE



„Nejnebezpečnější a nejničivější hrozby na světě jsou útoky na sdílené hodnoty a vzájemnou důvěru, bez nichž se rozpadá rodina, společnost, stát i mezinárodní řád.“

Centrální kybernetický štít tvoří základní pilíř nové bezpečnostní architektury pro členské státy EU a NATO. Bez něj nebude možné naplňovat alianční závazky, které vyžadují okamžité kybernetické přezbrojení demokratických zemí, neboť světová hybridní válka 21. století, na niž dlouhodobě upozorňují evropští i světoví státníci, probíhá ve fyzickém i digitálním světě současně. Z tohoto důvodu je nezbytné řešit bezpečnostní hrozby v obou dimenzích souběžně a koordinovaně, jelikož hybridní hrozby skrze kyberprostor pronikají do fyzického světa a mají natolik destrukční potenciál, že mohou členské státy zásadně rozvrátit a v krajním případě zničit ještě před případným vypuknutím ozbrojeného konfliktu.

NALÉHAVÉ UPOZORNĚNÍ PRO ČLENSKÉ STÁTY EU A NATO

Bezpečnost členských států EU a NATO vyžaduje plnění aliančních závazků ve fyzickém světě a v kyberprostoru současně, přičemž nezbytnou podmínkou je kybernetické přezbrojení prostřednictvím centrálního kybernetického štítu a vyvážené financování obou uvedených domén.

Centrální kybernetický štít představuje mimořádně důležitou, komplexní a dlouhodobě rozvíjenou alianční strategii, která vznikala na základě sedmnáctiletého systematického výzkumu, mezioborových analýz a praktického ověřování. Vzhledem ke složitosti a rozsahu však nelze realisticky očekávat, že jeho odbornou podstatu a strategické mechanismy běžné politické či poradní struktury v plném rozsahu pochopí, neboť jejich bezpečnostní politika je zaměřena převážně na fyzický prostor. Tato politická a bezpečnostní nerovnováha mezi fyzickou a digitální dimenzí však postupně zhoršuje bezpečnost členských států EU a NATO, neboť hybridní útoky na demokracii jsou nepřetržité a vedou k rozkladu demokratické civilizace a eskalaci ozbrojeného konfliktu, zatímco vojenské útoky se dosud neuskutečnily.

Převážná část politických představitelů nemá ani tušení, jaké ohavnosti a zvěrstva se v kyberprostoru odehrávají. Demokratický svět není na jejich existenci ani na jejich katastrofální dopady vůbec připraven. V důsledku světové hybridní války 21. století, kterou rozpoutaly autoritářské režimy, postupně vznikalo digitální podsvětí, v němž dnes působí miliony osob zapojených do různých forem kyberzločinů. Jejich činnost má ničivý dopad na kolektivní obranu, sdílené hodnoty a vzájemnou důvěru, na nichž stojí bezpečnost a soudržnost rodiny, společnosti, členských států EU a NATO i celého mezinárodního řádu. Následkem toho dochází ke každodennímu nárůstu rizika závažných bezpečnostních krizí, jejichž eskalace může vyústit až v ozbrojené konflikty. Jedním z možných řešení by mohla být aktivace Centrálního kybernetického štítu, jehož vývoj trval sedmnáct let a jehož hlavním cílem je posílení obrany demokratického světa proti těmto hrozbám.

Nejde o nedostatek odborných schopností politických představitelů, poradců, analytiků a mnoha dalších autorit, ale o přirozené systémové omezení jejich kapacit, protože musí zajišťovat velmi široké spektrum dalších agend. Ochranu demokracie v kyberprostoru, mezinárodní bezpečnost a řízení společnosti a státu v digitální éře proto nelze považovat za běžnou součást politické činnosti, neboť jde o rozsáhlou a vysoce komplexní oblast kybernetické bezpečnostní politiky. Z tohoto důvodu je nezbytný vznik Mezinárodní alianční rady, jejímž úkolem bude připravit podmínky pro aktivaci Centrálního kybernetického štítu a koordinovat proces kybernetického přezbrojení za účelem kolektivní ochrany členských států EU a NATO v kyberprostoru, jakožto prevence ozbrojeného konfliktu.

Unikátnost alianční strategie Centrálního kybernetického štítu spočívá v tom, že nevychází pouze z teoretických poznatků a odborných analýz, ale z dlouhodobých praktických zkušeností

získaných při konfrontaci s rizikovým a konfliktním prostředím. Právě v těchto podmínkách bylo nezbytné rozvíjet schopnosti adaptace, krizového rozhodování, identifikace hrozeb a tvorby preventivních obranných mechanismů. Na tomto základě byl následně vytvořen ucelený systém preventivních, obranných a stabilizačních opatření napříč bezpečnostní, technologickou, institucionální, ekonomickou i geopolitickou rovinou.

Centrální kybernetický štít byl vybudován především za účelem vytvoření podmínek pro plnění aliančních závazků členských států EU a NATO v kyberprostoru, protože tyto závazky již nelze v digitálním věku naplňovat pouze ve fyzickém prostoru. Kyberprostor se stal nedílnou součástí kolektivní obrany, a jeho podcenění by vedlo k ohrožení bezpečnosti, obranyschopnosti a stability demokratických států.

Mezinárodní alianční rada – garant plnění aliančních závazků v kybernetickém prostoru

---

Vznik Mezinárodní aliančí rady je považován za historický krok, protože naplňování aliančních závazků členských států Evropské unie a NATO vyžaduje jejich plnění nejen ve fyzickém světě, ale i v kyberprostoru. Mezinárodní alianční rada je proto zřizována za účelem dohledu a koordinace naplňování těchto závazků v rámci procesu kybernetického přezbrojení, čímž přispěje k posílení ochrany demokratické civilizace, kolektivní obrany členských států v kybernetickém prostoru, mezinárodní bezpečnosti a prevenci eskalace ozbrojených konfliktů.

Dění v kyberprostoru stále častěji ovlivňuje bezpečnostní, sociální, ekonomickou, environmentální a právní stabilitu i budoucnost členských států Evropské unie a NATO. Bez existence Mezinárodní aliančí rady by proto naplňování aliančních závazků členských států Evropské unie a NATO bylo v současném bezpečnostním prostředí kriticky ohroženo, neboť fyzický a digitální prostor jsou vzájemně propojeny prostřednictvím hybridních hrozeb, které umožňují přenos rizik a útoků z kybernetického prostoru do fyzického světa.

Mezinárodní alianční rada se stane klíčovým institucionálním orgánem pro naplňování aliančních závazků členských států Evropské unie a NATO právě proto, že došlo k historicky zásadním proměnám bezpečnostního prostředí 21. století, kdy významná část digitálního prostoru, v němž probíhá společenská, politická a veřejná komunikace, není plně pod přímou kontrolou států, ale je spravována soukromými technologickými společnostmi nebo režimy s centralizovanou kontrolou nad vlastními kybernetickými kapacitami. Tato asymetrie zvyšuje zranitelnost bezpečnostní infrastruktury členských států a komplikuje koordinované naplňování aliančních závazků, zejména v kontextu rostoucího významu hybridních hrozeb, které propojují kybernetický prostor s fyzickým bezpečnostním prostředím.

Institucionální struktura Mezinárodní alianční rady

Aby bylo možné naplňovat alianční závazky nejen ve fyzickém světě, ale i v kybernetickém prostoru současně, je nezbytné, aby institucionální struktura Mezinárodní alianční rady byla vybudována na víceúrovňovém modelu řízení, který propojuje politickou, strategickou, výkonnou a operační rovinu.

Nejvyšším rozhodovacím orgánem Mezinárodní alianční rady by bylo shromáždění předsedů vlád demokratických členských států Evropské unie a NATO, které by schvalovalo strategické priority, bezpečnostní cíle a klíčová rozhodnutí související s naplňováním aliančních závazků v kybernetickém prostoru. Výkonným představitelem Rady by byl generální sekretář odpovědný za politicko-strategické řízení, koordinaci mezinárodní spolupráce a realizaci schválených rozhodnutí. Generálního sekretáře by podporoval exekutivní výbor složený z aliančních zástupců členských států, jehož úkolem by bylo připravovat strategická rozhodnutí, koordinovat jejich implementaci a dohlížet na proces kybernetického přezbrojení. Klíčovou operační složkou Rady by bylo Kybernetické velení, odpovědné za plánování, koordinaci a řízení společných aktivit v oblasti kolektivní obrany v kybernetickém prostoru, aktivaci Centrálního kybernetického štítu a reakci na kybernetické a hybridní hrozby.

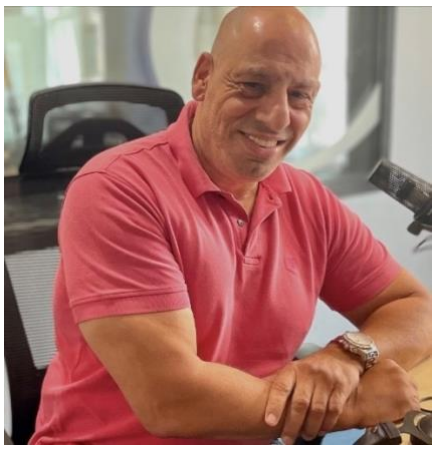
CENTRÁLNÍ KYBERNETICKÝ ŠTÍT DEMOKRACIE

Ladislav Boldi – **Autor a garant Centrálního kybernetické**ho štítu demokracie. Bezpečnost členských států EU a NATO vyžaduje plnění aliančních závazků ve fyzickém i kybernetickém prostoru současně.

Institucionální zázemí:
Digital Policy Institute – millennium 3000

- Zakladatel sociální sítě Politinn - první evropské platformy nové generace
- Zakladatel mobilní aplikace ONLINE DEMOKRACIE
- Zakladatel demokratických slavností a prestižního udílení cen „Demokratická osobnost roku“
- Autor konceptu „dezinfokracie“, nejničivějšího hybridního režimu 21. století, který vymazává demokracii z naší mysli.

Životopis: Ladislav Boldi



Ladislav Boldi vyrůstal v mimořádně krutých podmínkách. Poté, co se ho biologická matka krátce po narození vzdala, prožil 19 let ve výchovných ústavech, kde čelil brutálnímu násilí, mučení, nelidskému zacházení, nepopsatelnému utrpení a každodennímu boji o přežití. Po propuštění z výchovného ústavu byl nucen žít na ulici jako bezdomovec, protože mu stát a úřady odmítly poskytnout jakoukoli pomoc, a bez dokladu totožnosti pro systém fakticky neexistoval.

Aby přežil na ulici, která se nakonec stala jeho jediným domovem, byl donucen jíst prošlé nebo shnilé potraviny a zbytky z odpadkových košů a přijímat nabídky na pouliční zápasy za patnáct korun, které mu zajišťovaly alespoň základní obživu. Tyto činnosti nebyly výsledkem volby, ale jediným prostředkem k přežití. Svůj život si zachránil jen díky tomu, že se postupně naučil řešit problémy a konfliktní situace v podmínkách přímého ohrožení života. Navzdory krutosti osudu se rozhodl své zkušenosti zúročit ve prospěch společnosti a státu. Veškeré úsilí i své úspory investoval do vzdělání. Ve 40 letech vystudoval dálkově střední školu a následně absolvoval vysokou školu v oblasti veřejných a mezinárodních vztahů. Díky svým hlubokým zkušenostem z konfliktního prostředí vypracoval v roce 2015 koncept „sociální terorismus“, jehož cílem bylo varovat členské státy EU a NATO před radikalizací občanů na sociálních sítích, která může mít v některých případech závažnější důsledky než ozbrojený konflikt.

Hrozby, na které Ladislav Boldi dlouhodobě upozorňuje, se však netýkají pouze sociálního terorismu, ale i postupného poklesu důvěry v demokratické instituce v důsledku hybridních hrozeb rodících se v digitálním prostoru, jejichž dopady se projevují rostoucím bezpečnostním a společenským napětím. V prostředí globálních migračních procesů zároveň upozorňuje na skutečnost, že jejich organizace a koordinace probíhá stále častěji v kyberprostoru, což zásadně mění charakter těchto jevů a vyžaduje jejich řešení právě na této úrovni. Současně zdůrazňuje fenomén označovaný jako „digitální rakovina“, který představuje vážné ohrožení psychické stability populace v digitálním věku, spojené s nárůstem digitálního násilí, stresu, depresí, utrpení, sociální izolace a celkového oslabení duševního zdraví, zejména u mladší generace. Jeho návrhy, projekty, bezpečnostní strategie a odborná doporučení však politici i novináři odmítli z důvodu jeho minulosti a špatného sociálního původu.

Ladislav Boldi se nevzdal, a přestože se k němu jeho okolí dlouhodobě stavělo odmítavě, pokračoval více než 17 let v systematickém vývoji Centrálního kybernetického štítu, jehož cílem je umožnit členským státům Evropské unie a NATO zahájit proces kybernetického přezbrojení jako nezbytný předpoklad pro naplňování aliančních závazků v obou dimenzích současného bezpečnostního prostředí. Právě za tímto účelem vznikl Centrální kybernetický štít jako nástroj kolektivní obrany i v digitálním prostoru, neboť bezpečnostní hrozby v podmínkách světové hybridní války 21. století působí současně ve fyzické i kybernetické sféře, což vede k průběžné eskalaci bezpečnostních rizik a zvyšování pravděpodobnosti ozbrojeného konfliktu.

V kyberprostoru se rozvíjejí struktury, které jsou v analytické a bezpečnostní terminologii popisovány jako digitální podsvětí, jež postupně vznikalo v důsledku světové hybridní války 21. století. Toto digitální podsvětí dnes zahrnuje různé formy kyberkriminality, organizovaného zločinu a další trestné činnosti, které představují jednu z nejvýznamnějších bezpečnostních hrozeb digitální éry. Právě mnohaleté osobní zkušenosti z konfliktního prostředí vedly Ladislava Boldiho k vybudování alianční strategie, jejímž výsledkem je Centrální kybernetický štít – technologicky nejvyspělejší bezpečnostní systém zaměřený na ochranu členských států EU a NATO a demokratické civilizace.

Veškeré návrhy a koncepce Ladislava Boldiho v rámci boje a obrany proti světové hybridní válce 21. století by proto měly být posuzovány výhradně podle jejich obsahu, kvality, vize a přínosu pro členské státy EU a NATO, nikoli podle jeho minulosti, za kterou de facto ani nemůže. Kromě toho, ty nejlepší a nejodolnější bezpečnostní strategie nikdy nevznikají v politických debatách, konferenčních sálech ani v administrativním prostředí u kávy, ale z přímé zkušenosti v konfliktním prostředí a při střetu s reálnou hrozbou. Teprve život ohrožující konfrontace se zlem odhalí, které postupy skutečně fungují, které selhávají a jaké strategie jsou schopné obstát v kritických situacích a pod extrémním tlakem. Praktické zkušenosti získané v konfliktním prostředí se tak stávají klíčovým zdrojem poznání pro tvorbu moderních bezpečnostních doktrín.

Životní a profesní profil Ladislava Boldiho: *„Ti, kteří mě hanobili, špinili, ponižovali, diskriminovali, zesměšňovali, odsuzovali a otočili se ke mně zády, by měli vědět, že každá cesta, kterou jsem šel, každá špatná zkušenost, každý, s kým jsem něco prožil, a co jsem kdy učinil – to vše se nakonec ukázalo, že jsem kráčel správným směrem. A jen díky tomu se mi podařilo vybudovat mnoho dobrého a trvalého pro společnost a pro stát.“*

KONEC TRADIČNÍ POLITIKY – NÁSTUP AI POLITIKY V ČLENSKÝCH STÁTECH EU A NATO

Členské státy Evropské unie a NATO vstupují do historického transformačního období, které zásadním způsobem promění ochranu a řízení společnosti, fungování státu i podobu demokracie v digitální éře. Tradiční politika, zaměřená především na správu fyzického světa, postupně přestává plně odpovídat realitě 21. století, v níž se významná část společenské, politické, ekonomické i bezpečnostní komunikace přesouvá do kyberprostoru.

Tradiční politické modely v členských státech EU a NATO se dnes ocitají v mimořádně složité situaci, kdy nedokážou adekvátně reagovat na rychlost technologického vývoje ani na dynamiku digitálního prostředí. V důsledku toho vzniká nerovnováha v řízení společnosti a státu, která ohrožuje nejen bezpečnost členských států, ale i jejich schopnost plnit alianční závazky. Bezpečnost přitom představuje základní předpoklad stabilního fungování demokracie, efektivní správy státu a ochrany veřejného zájmu.

Přestože členské státy Evropské unie a NATO dosáhly významného pokroku v oblasti digitalizace veřejné správy, bezpečnosti a obrany, na vybudování demokratické infrastruktury pro fungování společnosti a státu v kyberprostoru prakticky zapomněly. Tento kritický nedostatek dnes ohrožuje vyvážené řízení společnosti a státu ve fyzickém i digitálním prostoru a současně oslabuje schopnost demokratických zemí čelit bezpečnostním výzvám 21. století. Vybudování plnohodnotného demokratického prostředí v kyberprostoru proto představuje jeden z nejdůležitějších úkolů následujících desetiletí, neboť právě na něm bude záviset kolektivní obrana demokratických států, budování centrálních ochranných mechanismů, posilování kybernetické odolnosti i postupný přechod od tradiční politiky k AI politice založené na principu ONLINE DEMOKRACIE.

AI politika představuje nový model řízení společnosti a státu založený na využívání operačních systémů umělé inteligence, které budou schopny v reálném čase analyzovat rozsáhlé objemy dat, vyhodnocovat potřeby občanů, modelovat dopady veřejných politik, navrhovat optimální řešení, podporovat rozhodovací procesy a koordinovat výkon veřejné správy. Tyto systémy budou integrovat ekonomické, bezpečnostní, sociální, vzdělávací, zdravotní, dopravní, energetické, environmentální i další strategické oblasti do jednotného datového prostředí, které umožní průběžnou optimalizaci fungování státu. V důsledku vyšší míry automatizace rozhodovacích a administrativních procesů dojde zároveň k významnému snížení potřeby lidské kapacity ve všech oblastech politického řízení, veřejné správy a souvisejících administrativních struktur, včetně počtu politických, úřednických a dalších exekutivních rolí, a to do míry umožňující autonomnější fungování systému řízení společnosti a státu.

AI politika bude bezpečná a demokraticky legitimní pouze tehdy, pokud bude založena na již vybudované digitální demokratické infrastruktuře, na jejímž principu bude fungovat ONLINE DEMOKRACIE. V praxi to znamená, že demokratické procesy musí být nejen podporovány novými technologiemi, ale přímo strukturovány a ukotveny v digitálním prostředí, kde se stanou plnohodnotnou součástí řízení státu. Bez těchto podmínek nebude možné efektivně a odpovědně řídit stát vyváženě ve fyzickém i digitálním prostoru a politici nebudou schopni plnit alianční závazky.

AI politika bude fungovat na principu ONLINE DEMOKRACIE, opírající se o digitální demokratickou infrastrukturu vybudovanou v souladu s nejvyššími bezpečnostními a technologickými standardy pro ochranu a rozvoj demokracie v kyberprostoru. Tento model zásadně promění fungování politického systému a vytvoří nové formy interakce mezi občany, politiky a veřejnou správou, včetně vzniku e-voličů, e-kandidátů a dalších digitálních nástrojů demokratické participace. V rámci AI politiky zároveň vznikne nový princip sdílené pravomoci mezi občanem a státem. Občané budou prostřednictvím digitálních demokratických platforem stále více zapojováni do rozhodovacích procesů, budou moci průběžně vyjadřovat své potřeby a zájmy, podílet se na tvorbě veřejných politik a řešit vybrané záležitosti v reálném čase. Tento proces představuje jednu z nejvýznamnějších změn demokratického systému od vzniku zastupitelské demokracie, protože umožní přímější propojení mezi občanem a výkonem veřejné moci.

Aby bylo možné efektivně naplňovat alianční závazky v digitální éře, jak se předpokládá, bude nezbytná hluboká transformace celé tradiční politiky směrem k AI politice fungující na principu ONLINE DEMOKRACIE, včetně přechodu tradičních politických stran na AI politické strany. Pouze za předpokladu vyváženého řízení společnosti a státu ve fyzickém i digitálním prostoru současně lze zajistit schopnost tyto závazky odpovědně naplňovat.

Pokud nedojde k okamžité transformaci tradičních politických stran na AI politické strany a k systematickému budování digitální demokratické infrastruktury pro rozvoj ONLINE DEMOKRACIE, která představuje základní předpoklad nové bezpečnostní architektury, hrozí členským státům EU a NATO mimořádně závažné důsledky, mezi něž patří:

- Ztráta schopnosti plnění aliančních závazků NATO.
- Rozpad řízení společnosti a státu v důsledku hybridních útoků na demokracii.
- Rozpad fungování veřejné správy v důsledku neschopnosti transformace z tradiční politiky na AI politiku.
- Ohrožení samotného demokratického řádu a jeho základních principů.
- Oslabení legitimity státu a ztráta jeho autority v očích občanů.
- Rozpad důvěry v demokracii, politické představitele a veřejné instituce.
- Rostoucí a obtížně kontrolovatelný rozmach organizovaného zločinu a zločineckých struktur digitálního podsvětí, jež tvoří nedílnou součást světové hybridní války 21. století.
- Destabilizace bezpečnostní, politické a společenské rovnováhy členských států EU a NATO.
- Ohrožení digitální státnosti, suverenity, národní identity a legitimity států v kyberprostoru.
- Masivní šíření dezinformací, propagandy a manipulace veřejného mínění, často podporované AI systémy.

- Ztráta schopnosti rozlišovat lež od pravdy v osobním, profesním i veřejném životě.
- Exploze informačního chaosu a celospolečenské dezorientace.
- Zrychlená polarizace společnosti a prohlubování názorových konfliktů.
- Radikalizace jednotlivců i skupin v online prostředí (sociální terorismus) s přesahem do reálného světa.
- Nárůst frustrace, hněvu a nenávisti vedoucí k oslabení mezilidských vztahů.
- Eroze společenské soudržnosti a narušení vazeb mezi státy.
- Přenos digitálních konfliktů do fyzického prostoru včetně rizika násilných střetů.
- Zvyšování bezpečnostního napětí a vznik nových forem extremismu.
- Manipulace volebních procesů a ovlivňování volebního chování.
- Destabilizace volebních systémů a oslabení jejich důvěryhodnosti.
- Narušení rovnosti politické soutěže.
- Snižování transparentnosti rozhodovacích procesů.
- Koncentrace moci v technologických a datových strukturách.
- Zneužívání dat k politickým a mocenským účelům.
- Posilování vlivu zahraničních aktérů na vnitřní politiku členských států EU a NATO.
- Zesilování hybridních útoků na demokratické instituce členských států EU a NATO.
- Automatizace AI propagandy a její masové šíření v kyberprostoru.
- Vznik uzavřených informačních bublin a fragmentace veřejného diskurzu.
- Oslabování tradičních médií a jejich kontrolní role v důsledku světové hybridní války 21. století.
- Nárůst datově řízeného populismu a emocionální manipulace AI politiky.
- Prohlubování závislosti občanů na technologických platformách a AI systémech.
- Neschopnost institucí reagovat na rychlý technologický vývoj ve světě.
- Kolaps koordinace mezi digitální a fyzickou úrovní výkonu státní moci.
- Oslabení schopnosti strategického řízení státu v podmínkách světové hybridní války 21. století.
- Eroze schopnosti členských států EU a NATO provádět základní rozhodovací a rozpočtové procesy.
- Ohrožení ekonomické, sociální a právní stability států včetně jejich dlouhodobé prosperity a rozvoje členských států EU a NATO.

Centrální kybernetický štít byl koncipován jako strategický nástroj pro toto mimořádně náročné transformační období. Uvedené hrozby a jejich důsledky současně představují jasný důkaz, že bez včasného vybudování AI politiky založené na principu ONLINE DEMOKRACIE a digitální demokratické infrastruktury může dojít k postupnému rozkladu systému řízení společnosti a státu v členských zemích EU a NATO, což by zásadně oslabilo schopnost demokratických institucí zajišťovat bezpečnost, stabilitu, efektivní správu státu i plnění aliančních závazků. Úkolem centrálního kybernetického štítu proto není pouze ochrana demokratického systému před hybridními hrozbami, ale také vytvoření podmínek pro co nejrychlejší a bezpečný přechod od tradiční politiky k AI politice fungující na principu ONLINE DEMOKRACIE, která umožní vyvážené řízení společnosti a státu ve fyzickém i digitálním prostoru současně a posílí schopnost členských států EU a NATO odpovědně naplňovat své bezpečnostní, hodnotové, právní a alianční závazky.

Politici členských států Evropské unie a NATO narážejí na limity svých bezpečnostních kapacit, neboť nové hybridní a kybernetické hrozby nedokážou účinně řešit pouze v rámci státních struktur. Klíčové technologické ekosystémy, digitální platformy, datová infrastruktura i

inovační kapacity jsou totiž z převážné části ve vlastnictví a správě soukromého sektoru. Bez vizionářů, stratégů a odborníků ze soukromé sféry zůstávají bezradní a sami si neporadí s tak zásadními výzvami, jaké představuje světová hybridní válka 21. století, jejíž komplexní analýza trvala téměř 17 let. Právě tyto autority disponují technologickým know-how se zaměřením na vybudování digitální demokratické infrastruktury a schopnostmi vytvářet a implementovat strategická řešení. Bez jejich oslovení a aktivního zapojení proto nelze vybudovat moderní bezpečnostní architekturu 21. století ani zajistit kolektivní obranu členských států EU a NATO.

Ve Spojených státech a v Číně probíhá dlouhodobě masivní technologický a investiční rozvoj zaměřený na budování rozsáhlých digitálních ekosystémů zahrnujících globální internetové platformy, sociální sítě, cloudové infrastruktury, umělou inteligenci, polovodiče, kvantové technologie, robotiku, autonomní systémy, zejména pak kybernetickou bezpečnost a sofistikované datové služby. Obě velmoci si uvědomují, že technologická dominance znamená ekonomickou, bezpečnostní i geopolitickou moc, a proto soustřeďují obrovské finanční, výzkumné i strategické kapacity právě do technologického rozvoje. Jejich síla stojí na velmi úzkém propojení soukromého sektoru a státní podpory, rychlosti rozhodování a schopnosti okamžitě převádět technologické inovace do globálního měřítka. Zároveň systematicky podporují technologické vizionáře, inovátory, vývojáře strategických systémů a tvůrce moderních bezpečnostních a kybernetických řešení, protože si uvědomují, že právě tito lidé představují klíč k budoucí moci, stabilitě a globálnímu vlivu. Vytvářejí jim mimořádné podmínky pro výzkum, vývoj, investice i realizaci technologických projektů, na nichž stále více závisí bezpečnost států, fungování ekonomik i stabilita moderní společnosti. Díky tomu dnes určují tempo vývoje umělé inteligence, sociálních platforem, datových systémů, moderních bezpečnostních technologií a kybernetických strategií, které zásadně ovlivňují fungování celého světa. Technologické prvenství se pro ně nestalo pouze otázkou ekonomiky, ale především strategického vlivu, moci a schopnosti formovat budoucí podobu globální společnosti v digitálním věku.

Naproti tomu Evropa v oblasti technologií a inovací dlouhodobě naráží na kombinaci rozsáhlého systému regulací, směrnic, příkazů, zákazů a administrativních omezení, které zpomalují a komplikují rozvoj inovačního prostředí. Návrhy na budování komplexních bezpečnostních architektur, včetně centrálních kybernetických obranných systémů, bývají v evropském prostředí často v raných fázích politického procesu odkládány nebo úmyslně blokovány v důsledku institucionální roztříštěnosti, mocenských priorit a v některých případech i klientelistických vazeb na úrovni členských států EU, Evropského parlamentu a Evropské komise.

V evropském institucionálním rámci jsou tradičně upřednostňovány politické funkce před realizací technologických, inovačních a strategických projektů, včetně rozsáhlých vědecko-technologických a bezpečnostních iniciativ, stejně jako před systematickou podporou technologických vizionářů, inovátorů a odborníků na moderní kybernetické a bezpečnostní systémy ze soukromé sféry. Tato strukturální preference politických rolí nad technologickým rozvojem vytváří riziko, že mezinárodní projekty zásadní pro digitální bezpečnost členských států EU a NATO nebudou plně realizovány, přestože na nich v dlouhodobém horizontu závisí jejich strategická a bezpečnostní stabilita napříč klíčovými oblastmi veřejného i politického života. Tento strukturální vývoj postupně vede k oslabení konkurenceschopnosti Evropy v globálním technologickém prostoru, k prohlubující se závislosti na externích technologických

řešeních ze Spojených států a Číny a k faktickému zaostávání v oblastech, kde by přitom Evropa mohla při efektivnějším institucionálním nastavení patřit mezi světové lídry.

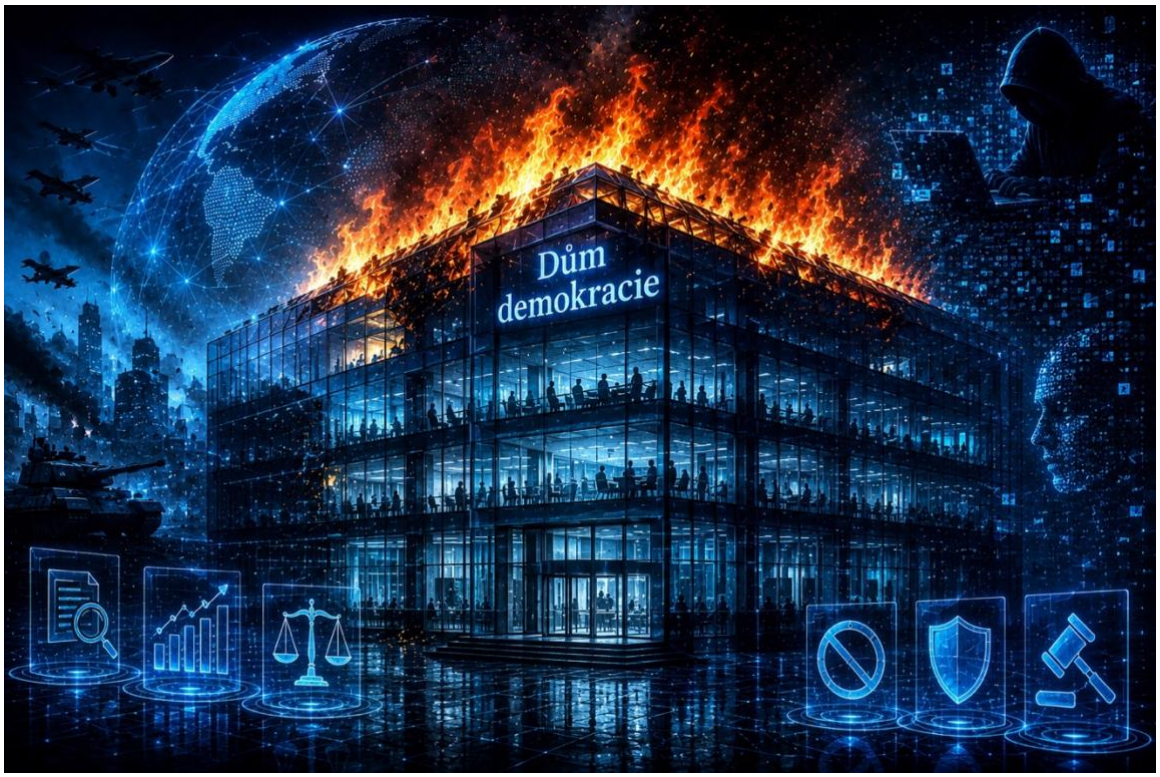
Pro politické představitele členských států EU a NATO je důležité jasně rozlišovat mezi dvěma odlišnými koncepty ochrany demokracie. Zatímco Evropský štít demokracie je budován primárně na principu digitálních regulací, legislativních směrnic a podpory prodemokratických organizací vymezujících hranice přípustného obsahu a je určen pouze pro členské státy Evropské unie, posláním Centrálního kybernetického štítu nejsou žádné regulace. Jeho princip spočívá v budování a rozvoji politického, bezpečnostního, hodnotového a právního systému, který chrání a upevňuje důvěru nejen mezi spojenci, ale i uvnitř demokratických společností, čímž přímo přispívá ke zvyšování obranyschopnosti aliančních struktur, posilování informační odolnosti a snižování zranitelnosti členských států vůči nepřátelskému působení.

Žádná demokratická společnost se nebude nikdy sociálně, ekonomicky ani technologicky efektivně rozvíjet pod masivním náporem nadměrných zákonů a mocenských ambicí, které vytvářejí konfliktní prostředí v členských státech EU a NATO. Demokracie může přežít pouze tehdy, bude-li společnost vychovávána na sdílených hodnotách, budování vzájemné důvěry a posilování společenské soudržnosti, nikoliv na základě mocenského řízení prostřednictvím rostoucích zákonů, zákazů a příkazů, jak je stále častěji uplatňováno nejen ve fyzickém, ale dnes již i v digitálním prostoru. Proto je nutné aktivovat centrální kybernetický štít a s jeho pomocí vybudovat moderní digitální demokratickou infrastrukturu, která umožní ochranu a rozvoj demokracie na principu sdílených hodnot, společenské stability a vzájemné důvěry v obou světech — fyzickém i digitálním — současně.

Centrální kybernetický štít představuje mezinárodní integrovaný bezpečnostní systém, který by se měl stát novým pilířem bezpečnostní architektury členských států Evropské unie a NATO, jelikož v současné globální bezpečnostní praxi neexistuje srovnatelný mechanismus obdobného rozsahu a koncepčního řešení. Jeho sedmnáctiletý vývoj vedl k vybudování digitální demokratické infrastruktury založené na deseti aliančních bezpečnostních pilířích, které integrují nejmodernější kapacity pro reakci na světovou hybridní válku 21. století.

Pokud nebudou včas zahájeny kroky směřující k zavedení a aktivaci Centrálního kybernetického štítu, bude vážně ohroženo plnění aliančních závazků. Bez vzájemné důvěry nelze dlouhodobě udržet spojenectví, soudržnost ani funkční systém kolektivní obrany, což by vedlo k postupnému oslabení demokratických institucí a stability členských států Evropské unie a Severoatlantické aliance.

DEMOKRATICKÝ SVĚT V PLAMENECH SVĚTOVÉ HYBRIDNÍ VÁLKY 21. STOLETÍ



V digitálním světě hoří střecha demokratického domu, ale tento požár žádné regulace, analýzy, směrnice, zákazy ani příkazy nedokážou uhasit.

V digitálním prostoru hoří střecha demokratického domu, ale jen málokdo si tohoto neštěstí všímá. Tento stav je přímým důsledkem probíhající světové hybridní války 21. století, jejíž nedílnou součástí je digitální podsvětí, kde dochází k nekontrolovatelnému rozrůstání organizovaného zločinu, sociálnímu terorismu v podobě radikalizace občanů na sociálních sítích, kybernetickým útokům na demokracii, jakož i digitálnímu násilí, tyranii, otroctví, zneužívání a mnoha dalším formám eskalující trestné činnosti a kybernetických hrozeb.

Zatímco Evropská unie a aliance NATO se soustředí na analýzu toho, proč tento požár vznikl a kdo ho způsobil, mezitím se tyto ohavnosti a zvěrstva v kyberprostoru masivně šíří a prostřednictvím zločineckých struktur, mezi které patří i autoritářské režimy, se přenášejí do fyzického světa. Na těchto ohavnostech a zvěrstvech ročně generují stamiliardové až bilionové zisky, přičemž ohrožují nejen členské státy, ale i samotnou demokratickou civilizaci a způsobují masivní ekonomické škody. V boji proti světové hybridní válce 21. století, která je vnímána jako jedna z největších hrozeb, neboť probíhá v obou světech, fyzickém a digitálním současně, se jako možné systémové řešení jeví aktivace centrálního kybernetického štítu – technologicky nejvyspělejšího obranného systému v kontextu současných mezinárodních bezpečnostních hrozeb.

Osud demokracie v členských státech EU a NATO závisí na Centrálním kybernetickém štítu.

Webové stránky:
https://www.kybernetickystitdemokracie.cz

Alianční strategie 2026: Kybernetické přezbrojení prostřednictvím Centrálního kybernetického štítu jako nástroj pro nezbytné plnění aliančních závazků členských států EU a NATO i v kyberprostoru.

Česká republika může na summitu NATO ve dnech 7.–8. července 2026 v Ankaře předložit návrh na otevření debaty o naplňování aliančních závazků, které jsou dnes primárně posuzovány podle výše obranných výdajů ve fyzickém prostoru. Tento přístup však již plně neodpovídá současnému vývoji mezinárodního bezpečnostního prostředí, protože alianční závazky musí být v moderních podmínkách naplňovány také v kyberprostoru, který se stal klíčovou součástí bezpečnostní a obranné reality 21. století. Navzdory probíhajícím diskusím o své roli v systému kolektivní obrany deklaruje Česká republika připravenost tyto závazky nejen plnit, ale také se aktivně podílet na jejich modernizaci prostřednictvím předložení strategického návrhu v podobě konceptu Centrálního kybernetického štítu, který je chápán jako jeden z klíčových pilířů nové bezpečnostní architektury EU a NATO. Současná světová hybridní válka 21. století probíhá současně ve fyzickém i digitálním prostoru, což zásadně mění charakter bezpečnostních hrozeb. Z tohoto důvodu je nezbytné zahájit proces kybernetického přezbrojení demokratických států, který umožní efektivní reakci na hybridní hrozby, bezpečnostní rizika i mezinárodní konflikty v jejich digitální i fyzické podobě. Pouze tak lze zajistit koordinovaný přístup k ochraně stability a předcházet každodennímu nárůstu rizika eskalace ozbrojených konfliktů.

KYBERNETICKÉ PŘEZBROJENÍ A JEHO FINANCOVÁNÍ JAKO ZÁKLAD MODERNÍ BEZPEČNOSTNÍ ARCHITEKTURY

Kybernetické přezbrojení představuje dlouhodobou strategickou investici do digitální bezpečnosti, odolnosti a stability členských států EU a NATO, která má zásadní preventivní charakter. Jeho klíčovým principem je skutečnost, že investice do kybernetického přezbrojení postupně sníží budoucí potřebu výdajů na klasickou vojenskou infrastrukturu, protože posílí prevenci konfliktů, zvýší schopnost včasné reakce na hybridní hrozby a významně přispějí ke snížení eskalace mezinárodního napětí a rizika ozbrojených konfliktů.

Kybernetické přezbrojení představuje komplexní soubor mezinárodních politických, bezpečnostních, technologických a právních opatření, která vytvářejí prostor pro vybudování stabilního hodnotového a institucionálního rámce kyberprostoru. Jeho součástí je vybudování digitální demokratické infrastruktury v kyberprostoru, která umožní rozvoj konceptu ONLINE DEMOKRACIE – prvního politického systému fungujícího v digitálním světě. Současně posílí digitální suverenitu, identitu a legitimitu členských států EU a NATO v kyberprostoru a ochrání jejich digitální státnost, včetně demokratické a národní integrity.

Zásadní oblastí bude také obrana proti světové hybridní válce 21. století, která z kyberprostoru proniká v podobě šíření dezinformací, nenávistné propagandy a manipulace veřejného mínění do fyzického světa a představuje vysoké riziko eskalace mezinárodního napětí a ozbrojených konfliktů.

Kybernetické přezbrojení zároveň představuje zásadní prvek bezpečnostní architektury, na kterém v moderním světě fakticky závisí stabilita a budoucí bezpečnost členských států EU a NATO. V současném prostředí již nelze považovat za dostačující ochranu pouze tradičních dimenzí, jako je vzdušný prostor či územní integrita, protože bezpečnostní hrozby se poprvé v historii odehrávají paralelně ve fyzickém i digitálním světě současně. Kyberprostor se stal rovnocenným operačním prostředím, ve kterém dochází k formování, eskalaci i přenosu konfliktů do reálného světa. Z tohoto důvodu je kybernetická obrana klíčová pro samotný osud bezpečnostní stability států.

Nedílnou součástí Centrálního kybernetického štítu by měla být koncepce pro vybudování kybernetické armády členských států EU a NATO. Ta by tvořila jeho klíčový operační a realizační prvek a představovala budoucí základní kapacitu pro budování, provoz a dlouhodobý rozvoj celého systému kybernetické obrany, včetně jeho průběžného fungování a schopnosti reagovat na dynamicky se vyvíjející hrozby v digitálním prostoru.

Je nutné vycházet ze skutečnosti, že nedemokratické režimy, jako jsou Čína, Rusko, Írán a další, již dlouhodobě disponují státem řízenými a organizovanými kybernetickými armádami a strukturami, které systematicky využívají k vedení hybridních operací. Tyto operace zahrnují zejména budování digitálního podsvětí, dezinformační kampaně, nenávistnou propagandu, manipulaci informačního prostředí, kybernetické útoky a další formy působení s přímými dopady do fyzického světa.

V tomto kontextu vyvstává zásadní otázka, zda je možné bez vybudování srovnatelných obranných kapacit na úrovni EU a NATO dlouhodobě a plnohodnotně naplňovat alianční bezpečnostní závazky v podmínkách probíhající světové hybridní války 21. století.

Generál Jean-Pierre Perrin v rozhovoru pro Seznam Zprávy uvedl: „Vnímat hrozbu neznamená někoho strašit. Je to o budování sebevědomí. Každý den Severoatlantická aliance čelí ze strany Ruska úmyslným provokacím, hybridním a především kybernetickým útokům. Hranice mezi mírem, krizí a konfliktem nebyla nikdy tak tenká jako dnes.“ Základním stavebním kamenem sebevědomí je důvěra. Ta se však v současnosti postupně rozplývá a vytrácí – nejen v rámci demokratických společností, kde lidé ztrácejí důvěru v principy a fungování demokracie, ale i mezi členskými státy Evropské unie a Severoatlantické aliance. Tento nebezpečný trend může mít katastrofální dopady na samotnou podstatu spojenectví, které je přitom klíčovým aliančním bezpečnostním pilířem a nezbytným předpokladem efektivní obranyschopnosti v současném světě. Bohužel tento pilíř dosud není plně zakotven v bezpečnostní architektuře, a proto je v zájmu mezinárodní bezpečnosti jeho prioritní posílení prostřednictvím aktivace Centrálního kybernetického štítu v rámci moderní bezpečnostní infrastruktury 21. století.

Navrhované rozdělení bezpečnostních investic představuje optimální strategii moderní bezpečnostní architektury 21. století pro EU a NATO:

1. **2,5 % HDP na aktivaci Centrálního kybernetického štítu:** Tato strategická investice je klíčová pro systematickou obranu proti světové hybridní válce 21. století, probíhající ve fyzickém i digitálním světě současně. Jejím cílem je ochrana politického, bezpečnostního, hodnotového a právního systému, vzájemné důvěry a sdílených hodnot, včetně ochrany digitální státnosti, suverenity, národní identity a legitimity státu v kyberprostoru, jakož i ochrany kritické infrastruktury a státních institucí před koordinovanými hybridními hrozbami.
2. **2,5 % HDP na vojenskou infrastrukturu:** Tato část financování zajišťuje rozvoj konvenčních obranných schopností, včetně ochrany vzdušného prostoru, pozemní a námořní obrany, zajištění fyzické územní integrity a suverenity členských států, stejně jako rozvoj strategických a operačních kapacit ozbrojených sil členských států EU a NATO.

V rámci nezbytného kybernetického přezbrojení členských států Evropské unie a NATO musí být financování rozdělováno rovnoměrně a vyváženě tak, aby byla zajištěna skutečná rovnováha a společná úroveň odolnosti napříč celou Aliancí, neboť hybridní hrozby pocházející z kyberprostoru mohou v moderním prostředí dosáhnout takové intenzity, že dokážou členské státy zásadně rozvrátit a v krajním případě i zcela zničit ještě před případným vypuknutím ozbrojeného konfliktu.

Pokud se Spojené státy americké rozhodnou podmínit bezpečnostní garance v rámci Severoatlantické aliance a aktivaci článku 5 splněním závazků ve výši 5 % HDP, bude nezbytné tento přístup strategicky přehodnotit. Mnohem prozíravější by bylo tento princip rozšířit o tzv. „digitální článek 5“, a to přímo na základě Kyberstrategie 2026 amerického prezidenta Donalda Trumpa. Ta v klíčové pasáži uvádí: „Svoboda a bezpečí v kyberprostoru se nesmí brát jako samozřejmost. Protivníci a kyberzločinci využívají kyberprostor k šíření autoritářství, potlačování demokracie a oslabování naší národní i ekonomické bezpečnosti.“ Kyberstrategie

2026 Donalda Trumpa tak otevírá přímou cestu k aktivaci Centrálního kybernetického štítu, který chrání demokracii a zajišťuje maximální bezpečnost členských států NATO a EU.

Náměstek generálního tajemníka NATO Jean-Charles Ellermann-Kingombe pronesl památnou větu, která rovněž otevírá cestu k zavedení „digitálního článku 5“ v kyberprostoru: „Od NATO se totiž očekává, že bude schopno bojovat a chránit se jak na zemi, tak ve vzduchu a na moři, ale také ve vesmíru a v kyberprostoru. Všechny tyto domény mají digitální základ, který je zranitelný vůči kybernetickým útokům. Kybernetická ochrana je tedy ústředním prvkem ve všech dimenzích přípravy na moderní válčení a je pro ozbrojené síly klíčová. Potřebujeme vybudovat digitální páteřní síť. Musíme zavést postupy, jak sdílet obrovské objemy dat, a vyškolit lidi, kteří budou nové systémy obsluhovat. Je tedy spousta věcí, které musíme udělat – a musíme je udělat rychle.“

Centrální kybernetický štít bude představovat unikátní systém, který bude pro členské státy EU a NATO zajišťovat tzv. kompletní bezpečnostní servis. Tím se rozumí souvislé a nepřetržité zajištění ochrany, koordinace a reakční schopnosti v digitálním prostoru v rámci jednoho propojeného a řízeného celku. Tento servis bude představovat jednotný mechanismus bezpečnostní podpory napříč členskými státy a stane se klíčovým prvkem moderní bezpečnostní architektury EU a NATO.[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]

VAROVÁNÍ

Demokratický svět musí místo debat, regulací, směrnic a analýz začít konat!

Hybridní útoky zaměřené proti demokratické civilizaci dosahují již dnes takové intenzity a rozsahu, že bez aktivace centrálního štítu reálně hrozí postupný rozklad rodin, společností, členských států Evropské unie a NATO i samotných základů mezinárodního řádu.

Členské státy Evropské unie a NATO se ocitají v situaci, kdy jejich největším problémem již není nedostatek informací o hybridních hrozbách, ale nekonečné debaty, pomalé rozhodování, nadměrná byrokracie, složité schvalovací procesy a dlouhodobé upřednostňování teorií, analýz, studií, posudků a konzultací před rozhodnými akcemi. V prostředí probíhající světové hybridní války 21. století se nečinnost, odklady a administrativní průtahy stávají strategickou výhodou pro nepřítele, a záhubou pro demokratickou civilizaci.

Zatímco aktéři hybridních hrozeb, včetně autoritářských režimů, vedou proti členským státům EU a NATO i proti demokratické civilizaci dlouhodobé a nepřetržité útoky, představitelé demokratických vlád často pouze debatují, analyzují situaci a přijímají nové regulace či směrnice. Tyto kroky samy o sobě však útočníky nezastaví ani je neodradí od nepřátelského působení.

Každá promarněná vteřina, kterou aktéři hybridních hrozeb využívají k útokům proti demokratickým státům, ohrožuje naplňování aliančních závazků, zvyšuje bezpečnostní rizika pro demokratickou civilizaci a snižuje kolektivní obranyschopnost EU a NATO.

OBSAH

Oddíl 1

Co je větší hrozba - Světová hybridní válka 21. století nebo ozbrojený konflikt?

V důsledku světové hybridní války 21. století, kterou rozpoutaly autoritářské režimy, postupně vznikalo digitální podsvětí, v němž dnes působí miliony osob zapojených do různých forem kyberzločinů. Jejich činnost má ničivý dopad kolektivní obranu, sdílené hodnoty a vzájemnou důvěru, na nichž závisí bezpečnost a soudržnost rodiny, společnosti, členských států EU a NATO i mezinárodního řádu.

Existuje celá řada závažných důvodů, proč by politické autority demokratických států, představitelé Evropské unie, členských zemí NATO i mezinárodních organizací měli důkladně přehodnotit současné bezpečnostní priority. Zároveň by si měli položit zásadní strategickou otázku: Co dnes představuje větší hrozbu pro členské státy EU a NATO a demokratickou civilizaci? Potenciální ozbrojený konflikt v budoucnosti, nebo světová hybridní válka 21. století, která již každý den probíhá ve fyzickém i digitálním prostoru a narušuje kolektivní obranu a bezpečnostní infrastrukturu, ničí sdílené hodnoty a kriticky oslabuje vzájemnou důvěru, bez nichž se postupně rozpadá rodina, společnost, stát i mezinárodní řád.

Nejen bezpečnost, ale i budoucnost členských států Evropské unie a demokratické civilizace je stále více ohrožována mimořádně závažnou hrozbou, která vyplývá ze skutečnosti, že rozhodující technologické platformy, komunikační infrastruktura, algoritmické systémy a kybernetické kapacity 21. století se nacházejí mimo přímou kontrolu států, a to buď v rukou soukromých technologických společností, nebo jsou součástí mocenských struktur autoritářských režimů. Zatímco tradiční obranné a zbraňové systémy byly po staletí budovány, vlastněny a řízeny státy jako základní nástroj ochrany své suverenity a bezpečnosti, tato zásadní změna vytvořila bezprecedentní bezpečnostní asymetrii. Demokratické státy tak nesou odpovědnost za ochranu svých občanů, institucí a demokratického řádu, avšak významná část prostoru, ve kterém se formuje veřejné mínění a odehrávají informační a vlivové operace, se nachází mimo jejich přímý vliv. Právě tato strukturální nerovnováha postupně vedla ke vzniku globálně propojeného konfliktního prostředí, v němž se začala formovat světová hybridní válka 21. století.

Vznik globálně konfliktního prostředí a bezpečnostní asymetrie

Vznik globálně konfliktního prostředí je primárně důsledkem narůstající bezpečnostní asymetrie, kdy členské státy Evropské unie a NATO nemají plnou kontrolu nad klíčovými technologickými platformami, které se nacházejí buď v rukou soukromých technologických společností, jejichž zájmy jsou převážně ekonomické, nikoli bezpečnostní, nebo se staly součástí mocenských struktur autoritářských režimů, které je využívají k působení proti demokratickým zemím.

V globálním konfliktním prostředí se zrodila světová hybridní válka 21. století

Světová hybridní válka 21. století představuje komplexní a historicky nově vzniklý bezpečnostní fenomén. Jedná se o formu víceúrovňového konfliktu, jenž kombinuje různé nástroje mocenského vlivu, násilí, teroru, nátlaku a destabilizace, a to jak ve fyzickém, tak v digitálním prostoru současně. Vyznačuje se širokým spektrem nástrojů a forem působení. Mezi klíčové patří zejména šíření dezinformací, vedení informačních a vlivových operací, šíření nenávistné propagandy a manipulace s veřejným míněním prostřednictvím moderních komunikačních technologií a sociálních sítí. V důsledku těchto vlivů ztrácí demokratická civilizace schopnost rozlišovat mezi pravdou a lží a ocitá se tak ve stavu kritického ohrožení.

Světová hybridní válka 21. století umožnila vznik digitální podsvětí

Důsledkem dlouhodobého působení světové hybridní války 21. století a jejího pronikání do digitálního prostoru je vznik fenoménu, který lze označit jako digitální podsvětí. Jedná se o globálně propojené, decentralizované prostředí tvořené sítí aktérů, struktur a platforem, v němž dochází k různým formám kybernetické kriminality, informačních operací a koordinovaných vlivových aktivit. Tento prostor se postupně vyvinul jako vedlejší produkt konfliktního prostředí a asymetrie mezi technologickými a kybernetickými kapacitami států a nestátních aktérů.

Digitální podsvětí udržuje světovou hybridní válku 21. století v operativní činnosti.

Digitální podsvětí tvoří nezbytnou operační infrastrukturu světové hybridní války 21. století, která umožňuje její plnohodnotné fungování. Tento prostor funguje jako aktivní katalyzátor hybridního působení, který umožňuje, urychluje a multiplikuje různé formy informačních operací, kybernetické kriminality a vlivových aktivit. Digitální podsvětí je systematicky využíváno miliony aktérů zapojených do různých forem kyberzločinů a zároveň i autoritářskými režimy, přičemž rozsah těchto aktivit je mimořádně vysoký a zahrnuje statisíce až miliony jednotlivých incidentů denně.

Centrální kybernetický štít - strategická zbraň proti světové hybridní válce 21. století

Z obavy o budoucí bezpečnost členských států Evropské unie a NATO vznikla potřeba vybudovat Centrální kybernetický štít jako základní pilíř nové bezpečnostní architektury odpovídající podmínkám 21. století. Tato potřeba vychází ze skutečnosti, že dopady světové hybridní války 21. století a vznikajícího digitálního podsvětí mají zásadní a dlouhodobě destruktivní vliv na bezpečnostní prostředí demokratické civilizace, a v řadě aspektů mohou být z hlediska každodenní kumulace rizik srovnatelné, či dokonce závažnější než tradiční ozbrojené konflikty.

Myšlenka tohoto konceptu se začala formovat již před sedmnácti lety, kdy jeho autor na základě zkušeností z konfliktního prostředí identifikoval zásadní proměnu mocenských poměrů v digitálním prostoru. Upozornil na skutečnost, že rozhodující technologické, komunikační a kybernetické kapacity jsou soustředěny převážně v rukou soukromého sektoru, zatímco demokratické státy nedisponují odpovídajícími nástroji k plnohodnotnému

prosazování svých bezpečnostních a strategických zájmů v digitálním prostředí. Současně identifikoval rostoucí trend, kdy autoritářské režimy tyto kapacity systematicky integrují do svých mocenských a bezpečnostních struktur, čímž dochází k prohlubování strukturální bezpečnostní asymetrie.

Tato asymetrie byla vyhodnocena jako dlouhodobé strategické riziko, které vyžaduje vytvoření nové integrační a koordinační architektury schopné posílit postavení demokratických států v kyberprostoru a zajistit účinnější ochranu jejich bezpečnostních, demokratických a aliančních zájmů.

Autor alianční strategie, jakou představuje Centrální kybernetický štít, již v rané fázi identifikoval, že převládající bezpečnostní paradigma demokratických států je založeno především na regulatorních, legislativních a ex post reakčních mechanismech, zahrnujících normativní rámce, směrnicovou harmonizaci a administrativně-kontrolní nástroje. Zároveň dospěl k závěru, že tento přístup je strukturálně limitovaný a není schopen dostatečně reagovat na tempo, komplexitu a adaptivní charakter moderních hybridních, informačních a kybernetických operačních prostředí.

Z tohoto důvodu rozvinul koncepci vícevrstvé preventivní bezpečnostní architektury, založené na anticipačně-operativních protokolech, prediktivně-reaktivních bezpečnostních smyčkách a kontinuálních režimech kybernetické imunizace kritických systémů.

Jádrem tohoto přístupu je implementace integrovaných preventivních operačních programů, které zahrnují sekvenční detekci emergentních hrozbových vektorů, preemptivní intervenční mechanismy, adaptivní řízení expozice digitálních ekosystémů, dynamickou segmentaci operačních domén, real-time orchestraci vícevrstvých obranných struktur a kontinuální aktivaci distribuovaných bezpečnostních protokolů ve stavu vysoké operační připravenosti. Tyto mechanismy jsou doplněny o schopnost preventivní projekce rizikových scénářů, řízené snižování útočných ploch a systematické zvyšování resilience kritických digitálních i institucionálních subsystémů, čímž vzniká model, v němž preventivní složka tvoří základní architektonický princip celého systému.

Tato preventivní architektura představuje klíčový předpoklad pro stabilizaci strategického postavení členských států EU a NATO v kybernetickém prostoru, posílení jejich systémové autonomie a dlouhodobé zajištění odolnosti demokratických institucí vůči hybridním hrozbám, které se promítají současně do digitální i fyzické dimenze bezpečnosti.

Součástí tohoto rámce je také využití prediktivních modelů hrozeb vycházejících z reálných zkušeností z prostředí kybernetických a hybridních operací, behaviorální analýza aktérů, hardening digitální infrastruktury, segmentace kybernetických domén, orchestrace bezpečnostních operací a kontinuální sdílení threat intelligence napříč zapojenými strukturami. Tyto mechanismy umožňují včasnou identifikaci hybridních operačních scénářů a jejich neutralizaci v počátečních fázích vývoje.

Díky Centrálnímu kybernetickému štítu získají členské státy Evropské unie a NATO schopnost zásadně posílit své postavení a efektivně čelit nejzávažnější systémové hrozbě současnosti, kterou představuje světová hybridní válka 21. století. Ta se postupně formovala v důsledku

oslabení strukturální kontroly a narušení rovnováhy v kyberprostoru, jenž se v průběhu digitální transformace dostal převážně pod vliv soukromého sektoru a autoritářských režimů.

Bezpečnostní asymetrie vzniklá koncentrací klíčových technologií, digitálních platforem a kybernetických kapacit v těchto dvou sférách vedla k oslabování důvěry v demokratické instituce, eskalaci bezpečnostních rizik v kyberprostoru a rostoucí intenzitě hybridních útoků na demokratické systémy. Z tohoto hlediska se jako zásadní strategický závěr ukazuje nutnost, aby alianční závazky členských států Evropské unie a NATO byly naplňovány současně ve fyzickém i kybernetickém prostoru, neboť oba tyto rozměry jsou dnes plně propojené a vzájemně závislé.[15, 16, 17, 18, 19]

Oddíl 2

Centrální kybernetický štít – základ kolektivní bezpečnosti v rámci NATO a EU

„Od NATO se totiž očekává, že bude schopno bojovat a chránit se jak na zemi, tak ve vzduchu a na moři, ale také ve vesmíru a v kyberprostoru. Všechny tyto domény však mají digitální základ, který je zranitelný vůči kybernetickým útokům. Kybernetická ochrana je tedy ústředním prvkem ve všech dimenzích přípravy na moderní válčení a je pro ozbrojené síly klíčová. Potřebujeme vybudovat digitální páteřní síť. Musíme zavést postupy, jak sdílet obrovské objemy dat, vyškolit lidi, kteří budou nové systémy obsluhovat. Je tedy spousta věcí, které musíme udělat, a musíme je udělat rychle."

Autor citátu: Jean-Charles Ellermann-Kingombe, náměstek generálního tajemníka NATO pro kybernetickou oblast a digitální transformaci[20]

Současná metodika financování obrany v rámci NATO již neodpovídá struktuře hrozeb 21. století a vyžaduje okamžitou reformu. Tento závěr není postaven na teoretické úvaze, ale na empiricky doložitelné skutečnosti, že rozhodující část bezpečnostních rizik se přesunula do kyberprostoru, který dnes představuje primární prostředí, v němž dochází k systematickému narušování demokratických států. Klíčovým nedostatkem současného přístupu není samotná existence obranných mechanismů, ale jejich nesprávná prioritizace. Zatímco značná část finančních prostředků je nadále alokována do konvenčních vojenských kapacit, prostor, který bezprostředně ovlivňuje stabilitu států, jejich politické procesy i schopnost kolektivní obrany, zůstává strukturálně i finančně poddimenzovaný.

V tomto kontextu je nezbytné formulovat zásadní strategickou tezi: bezpečnost členských států NATO a Evropské unie je dnes primárně determinována úrovní stability v kyberprostoru. Tento prostor již nelze chápat jako doplňkovou doménu, ale jako základní infrastrukturu, na níž je vystavěno fungování demokratického státu. Veškeré klíčové procesy – od formování veřejného mínění přes volební mechanismy až po rozhodovací procesy vlád a bezpečnostních institucí – jsou dnes závislé na digitálním prostředí. Jakékoli narušení tohoto prostředí proto nemá pouze technický charakter, ale představuje přímý zásah do samotných základů demokracie.

Kyberprostor se zároveň stal prostředím, v němž dochází k systematickému působení, které lze charakterizovat jako strukturální destabilizaci demokratických systémů. Tento stav lze analyticky označit jako „dezinfokracii" – formu hybridního působení, v níž dochází k masivnímu šíření manipulativního obsahu, narušování informační integrity a postupnému rozkladu důvěry v demokratické instituce. Na rozdíl od tradičních hrozeb nemá tento proces jasně vymezený začátek ani konec, probíhá kontinuálně a zasahuje všechny vrstvy společnosti. Jeho důsledkem je oslabování schopnosti občanů orientovat se v realitě, zpochybňování legitimity státních institucí a postupná eroze společenské soudržnosti.

Zásadní problém spočívá v tom, že současné nástroje reakce na tento typ hrozeb jsou nedostatečné. Regulatorní přístupy, založené na zákazech, příkazech a směrnicích, nejsou schopny zajistit ochranu demokratického prostředí v kyberprostoru. Tyto nástroje reagují ex post, mají omezenou účinnost v globálním digitálním prostředí a často samy vyvolávají další napětí, včetně obav o svobodu projevu a legitimitu zásahů státu. Především však nedokážou řešit samotnou podstatu problému, kterou je absence systematicky vybudované digitální demokratické infrastruktury.

Právě tato absence představuje největší strukturální slabinu současného bezpečnostního systému. Demokratické státy vstoupily do digitální éry bez odpovídající infrastruktury, která by byla schopna chránit základní principy demokratického fungování v online prostředí. Výsledkem je stav, kdy klíčový prostor pro formování veřejného mínění, politické diskuse a společenské interakce není pod kontrolou demokratických mechanismů a je vystaven intenzivnímu působení destabilizačních vlivů.

Řešením této situace nemůže být dílčí úprava stávajících nástrojů, ale systémová změna přístupu. Tou je vybudování a aktivace **Centrálního kybernetického štítu**, který představuje klíčový prvek navrhované reformy metodiky financování obrany. Tento štít není pouze technologickým projektem, ale komplexním bezpečnostním rámcem, jehož cílem je vytvořit plnohodnotnou digitální demokratickou infrastrukturu na úrovni členských států NATO a Evropské unie.

Podstata tohoto konceptu spočívá v tom, že ochrana demokracie v digitálním prostředí nemůže být založena na omezeních, ale na aktivním budování prostředí, které je strukturálně odolné vůči manipulaci, dezinformacím a hybridním operacím. Digitální demokratická infrastruktura by v tomto smyslu představovala ekvivalent fyzické obrany – systém, který nejen reaguje na útoky, ale především jim předchází tím, že minimalizuje jejich účinnost.

Klíčovým aspektem této infrastruktury je ochrana důvěry. Důvěra v demokratické instituce, volební procesy, média i mezinárodní aliance, jako jsou NATO a Evropská unie, představuje základní podmínku jejich fungování. V kyberprostoru je však tato důvěra systematicky narušována. Pokud není aktivně chráněna, dochází k jejímu postupnému rozpadu, který se nevyhnutelně přenáší do fyzického světa. Výsledkem je oslabení legitimity státu, nárůst politické nestability a snížení schopnosti reagovat na bezpečnostní hrozby.

Z tohoto důvodu je nutné redefinovat samotný princip kolektivní obrany. Současný model, založený na článku 5 NATO, musí být rozšířen o jeho digitální dimenzi. Zavedení tzv. digitálního článku 5 znamená, že útok na informační a kybernetickou infrastrukturu jednoho členského státu bude považován za útok na všechny. Tento princip však nemůže být pouze deklaratorní. Musí být podložen odpovídajícími kapacitami, koordinací a především financováním.

A právě zde se dostáváme k jádru navrhované reformy. Přesměrování části obranných rozpočtů do financování Centrálního kybernetického štítu není alternativou ke stávajícím výdajům, ale jejich nezbytným doplněním a podmínkou jejich efektivity. Bez zajištění stability v kyberprostoru není možné zajistit funkčnost vojenských struktur, logistických systémů ani rozhodovacích procesů. Jinými slovy, kolektivní obrana ve fyzickém světě je přímo závislá na existenci kolektivní obrany v kyberprostoru.

Ignorování této skutečnosti vytváří zásadní strategické riziko. Pokud zůstane kyberprostor nedostatečně chráněn, bude nadále sloužit jako hlavní vstupní bod pro destabilizaci států. Tento proces může vést k postupnému rozkladu demokratických systémů, oslabení mezinárodních aliancí a v krajním případě k jejich faktickému paralyzování. Nejde tedy pouze o otázku technologickou nebo bezpečnostní, ale o otázku existence současného demokratického uspořádání.

Reforma metodiky financování obrany v rámci NATO proto musí být postavena na jasné prioritě: systematickém vybudování a financování Centrálního kybernetického štítu jako základního pilíře kolektivní bezpečnosti. Tento krok představuje jedinou realistickou odpověď na povahu současných hrozeb a jediný způsob, jak zajistit, že kolektivní obrana členských států Evropské unie a NATO bude funkční nejen formálně, ale i fakticky v podmínkách digitálního věku.[21, 22, 23]

Oddíl 3

AI politické strany mohou přivést lidstvo k blahobytu, ale i do záhuby

---

Tradiční politici po desetiletí slibují lepší budoucnost. Umělá inteligence ji však již nebude vytvářet na základě ideologických vizí, emocí, marketingových kampaní či krátkodobých volebních strategií, ale prostřednictvím nepřetržité analýzy makroekonomických cyklů, geopolitických rizik, bezpečnostních hrozeb, demografických změn, energetických trendů a globálních finančních toků. Civilizace vstupuje do období, v němž se schopnost predikovat budoucí vývoj společnosti stane jedním z nejdůležitějších nástrojů politické a státní moci. Nejde již o vzdálenou futuristickou představu, ale o velmi blízkou budoucnost, která se v důsledku exponenciálního rozvoje umělé inteligence stává prakticky nevyhnutelnou. Moderní svět dosáhl takové úrovně technologické, ekonomické a společenské komplexity, že tradiční lidské struktury přestávají být schopny efektivně řídit státy bez rozsáhlé podpory umělé inteligence.

Umělá inteligence postupně přebírá správu dvou klíčových realit současné civilizace – světa fyzického a světa digitálního. Tyto dva světy jsou dnes natolik propojené, že jakékoli zásadní politické, ekonomické nebo bezpečnostní rozhodnutí automaticky ovlivňuje oba současně. Digitální infrastruktura již není pouhým doplňkem fyzického světa, ale stala se jeho neoddělitelnou součástí. Finanční systémy, energetické sítě, doprava, zdravotnictví, státní správa, armáda, média i veřejná komunikace jsou stále více závislé na digitálních technologiích, datových tocích a automatizovaných systémech. Právě umělá inteligence se stává koordinační vrstvou této nové civilizační infrastruktury a postupně přebírá úlohu hlavního nástroje strategického řízení společnosti.

Hybridní AI programy budou schopny v reálném čase analyzovat miliony proměnných současně a optimalizovat fungování státu v rozsahu, který byl dosud pro lidské struktury nepředstavitelný. Umělá inteligence bude schopna precizně sestavovat státní rozpočty, modelovat ekonomický vývoj na desítky let dopředu, predikovat hospodářské krize, optimalizovat veřejné investice a řídit strategické oblasti, jako jsou bezpečnost, energetika, doprava, zdravotnictví, školství či sociální systém. Zásadně se změní samotný princip státní správy. Místo pomalého, administrativně náročného a často chaotického rozhodovacího procesu vznikne systém permanentní algoritmické optimalizace, který bude schopen okamžitě reagovat na krizové situace a nabízet desítky alternativních řešení s vysokou mírou přesnosti a efektivity.

Jednou z nejzásadnějších změn bude schopnost státu získat prostřednictvím umělé inteligence bezprecedentní kontrolu nad finančními a daňovými procesy. AI systémy budou schopny v reálném čase sledovat finanční toky, optimalizovat výběr daní, analyzovat pohyb kapitálu a automaticky odhalovat podezřelé ekonomické operace. Stát tak získá výrazně vyšší kontrolu nad daňovým systémem, veřejnými financemi i fungováním daňových subjektů a korporací. Daňové úniky, rozsáhlé podvody, manipulace účetních systémů či netransparentní převody financí budou v prostředí permanentního algoritmického dohledu mnohem obtížnější než

kdykoli v historii moderních států. Umělá inteligence současně umožní výrazně efektivnější správu důchodového systému, sociálních mechanismů i veřejných rozpočtů, čímž může státům ušetřit obrovské finanční prostředky a dramaticky snížit administrativní náklady.

V tomto kontextu však vzniká zásadní bezpečnostní otázka, která přesahuje rámec běžné technologické modernizace. Pokud má umělá inteligence převzít tak zásadní část řízení státu, ekonomiky a informačního prostoru, je nezbytné vytvořit nový typ obranné architektury, která dokáže chránit samotné základy demokratického systému. Právě zde vstupuje do hry koncept Centrálního kybernetického štítu, který představuje nejpokročilejší bezpečnostní systém budoucnosti zaměřený na ochranu demokratických států před digitálním autoritářstvím, manipulací algoritmických systémů a zneužitím AI politickými strukturami.

Dnes již existuje rozsáhlý systém evropských digitálních regulací, jako jsou GDPR, Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, NIS2, Data Act, Data Governance Act či Cyber Resilience Act, jejichž cílem je chránit bezpečnost, soukromí a stabilitu digitálního prostoru. Současně však vzniká stále vážnější riziko, že s nástupem AI politických stran, hybridních algoritmických systémů a automatizovaného řízení společnosti začne docházet k nekontrolovatelnému nárůstu dalších digitálních regulací, kontrolních mechanismů a administrativních procesů. Digitální civilizace je totiž natolik komplexní a dynamická infrastruktura, že každé nové bezpečnostní riziko, každá nová forma digitální manipulace, informačního vlivu či umělé inteligence může vytvářet tlak na další regulatorní zásahy. V důsledku toho by se digitální prostor mohl postupně stát natolik přeregulovaným, nepřehledným a administrativně zatíženým prostředím, že by se v něm přestali orientovat nejen občané, ale i samotné demokratické instituce, státy a technologické společnosti. Demokracie tak může být v budoucnu oslabena nejen hybridními útoky, dezinformacemi a digitálním autoritářstvím, ale také permanentním vrstvením složitých digitálních regulací, které mohou postupně paralyzovat schopnost společnosti efektivně fungovat v online prostoru. Právě proto se v podmínkách nastupující digitální civilizace stává Centrální kybernetický štít prakticky nenahraditelným nástrojem ochrany demokracie, protože jeho princip nespočívá v dalším nekontrolovatelném rozšiřování regulatorních omezení, ale ve vytvoření jednotné digitální demokratické infrastruktury fungující na principu ONLINE DEMOKRACIE, která dokáže aktivně chránit demokratický prostor před hybridními útoky, manipulací algoritmických systémů, koordinovanými informačními operacemi, digitálním autoritářstvím a zneužitím umělé inteligence, aniž by docházelo k postupnému zahlcení digitálního prostoru permanentně narůstajícími regulatorními zásahy.

Současně platí, že Centrální kybernetický štít je v podmínkách nastupující digitální civilizace prakticky nezastupitelný. Členské státy Evropské unie a NATO se bez něj nebudou schopny dlouhodobě efektivně bránit vůči sofistikovaným formám digitální manipulace, hybridních hrozeb a potenciálního nástupu autoritářských AI politických struktur.

Současné politické strany vznikly v podmínkách industriální éry, kdy bylo možné řídit stát prostřednictvím relativně jednoduchých administrativních struktur a omezeného objemu informací. Digitální civilizace však vytváří prostředí, které je pro tradiční politické modely jen obtížně zvládnutelné. Právě proto začnou vznikat nové AI politické strany a digitální politická hnutí, která budou schopna využívat pokročilé hybridní programy a systémy pro řízení společnosti v reálném čase. Tyto nové politické struktury budou schopny spravovat současně fyzický i digitální prostor společnosti.

V důsledku této transformace může být v budoucnu nahrazena významná část současných politiků, úředníků a administrativních aparátů. Umělá inteligence totiž dokáže převzít velkou část činností, které dnes vykonávají ministerstva, státní úřady a politické struktury. Automatizace rozhodovacích procesů, zpracování legislativních podkladů, ekonomických analýz, bezpečnostních modelů i administrativních agend zásadně sníží potřebu rozsáhlého byrokratického aparátu. AI politické strany budou schopny fungovat s mnohem menším počtem lidských aktérů, avšak s výrazně vyšší efektivitou, rychlostí a schopností dlouhodobého strategického plánování. Politika se postupně začne transformovat z ideologického střetu názorů na systém datového a algoritmického řízení společnosti.

Současně však vzniká jedno z největších bezpečnostních a civilizačních rizik moderní historie. Systémy schopné centralizovaně řídit ekonomiku, veřejné finance, bezpečnostní infrastrukturu, informační prostor i politické procesy mohou být v případě zneužití využity k vytvoření nové formy digitálního autoritářství. Na rozdíl od tradičních autoritářských režimů nebude tato forma moci založena pouze na fyzické kontrole obyvatelstva, ale především na permanentní kontrole dat, informací, digitální komunikace a psychologického ovlivňování společnosti prostřednictvím algoritmů. Umělá inteligence bude schopna analyzovat chování obyvatelstva v reálném čase, predikovat reakce společnosti, identifikovat rizikové skupiny a optimalizovat mechanismy politického vlivu s přesností, která nemá v historii obdoby.

Právě digitální prostor se totiž stal novým hlavním bojištěm demokracie. Veškerá společenská, mediální a politická komunikace se stále více přesouvá do online prostředí, kde se formují názory veřejnosti, rozhoduje se o důvěře ve státní instituce a vznikají nové mocenské struktury budoucnosti. Sociální sítě již dnes významně ovlivňují politické procesy, volební chování i stabilitu demokratických institucí. V budoucnu se tento vliv ještě dramaticky prohloubí. AI politické struktury budou schopny pracovat s psychologií společnosti, personalizovanou propagandou, predikcí chování voličů i masivními datovými analýzami v rozsahu, který může zásadně překonat možnosti tradičních demokratických institucí.

Právě proto představuje nástup AI politických stran jednu z nejzásadnějších výzev pro demokratický svět 21. století. Pokud členské státy Evropské unie a NATO neaktivují včas Centrální kybernetický štít, může dojít nejen k destabilizaci jednotlivých států, ale v krajním scénáři i k postupnému rozkladu demokratické civilizace jako celku.

Civilizace vstupuje do období, kdy se rozhodující boj o budoucnost demokracie nebude odehrávat pouze v parlamentních sálech nebo ve fyzickém prostoru států, ale především v digitálním světě, který se stává novým centrem politické, ekonomické a společenské moci.[24, 25, 26]

Oddíl 4

Digitální regulace důvěru občanů v demokracii neobnoví ani neposílí

Pokles důvěry v demokracii a v její instituce – nejen na národní, ale i mezinárodní úrovni – se v současnosti stále výrazněji projevuje jako klíčový důsledek proměny digitálního prostředí. Zásadní roli zde hraje obsah na sociálních sítích, který systematicky vyvolává závislost uživatelů. Tato závislost, umocněná cílenou manipulací emocí – strachu, hněvu, údivu či smíchu – představuje největší bezpečnostní hrozbu pro demokracii a stabilitu členských států EU a NATO.

Skrytá forma šíření dezinformací, propagandy, nenávisti a manipulace je integrována do atraktivních, interaktivních a emocionálně poutavých formátů, které uživatele vtahují do stále hlubšího dezinformačního prostoru. Právě tato kombinace závislosti a skrytého ovlivňování umožnila rozvoj a nadvládu dezinfokracie – nejničivějšího hybridního režimu 21. století, který systematicky působí na sociálních sítích již více než patnáct let. Výsledkem je postupné oslabování schopnosti občanů racionálně se orientovat ve veřejném prostoru, polarizace společnosti a eroze důvěry v demokratické instituce.

Evropská unie ani aliance NATO zatím tuto problematiku neuchopily jako strukturální bezpečnostní riziko. Ve skutečnosti dochází k paradoxní situaci: uživatelé jsou kvůli digitální závislosti odtrženi od svého osobního života, osobního rozvoje i aktivní účasti na veřejném životě, a péče o společné dobro státu a společnosti je oslabena. Místo toho je jejich pozornost upoutána na obsah, který primárně vyvolává emocionální reakce a maximalizuje zapojení, zatímco skrytě posiluje narušení demokratických procesů.

Z pohledu demokratických systémů má tento proces zničující dopady: dochází k postupnému oslabování schopnosti občanů rozlišovat mezi fakty a manipulací, což omezuje jejich aktivní zapojení do veřejného života. Tento trend narušuje i důvěru v mezinárodní organizace, jako jsou Evropská unie a NATO, jejichž legitimita je založena na důvěře členských států a občanů. Pokud je tato důvěra systematicky oslabována, dochází k narušení schopnosti těchto organizací efektivně plnit své funkce.

Zásadním problémem současného přístupu je fakt, že jakékoliv digitální regulace – zákazy, příkazy nebo směrnice – nemohou ze své podstaty vyřešit samotný problém závislosti uživatelů ani eliminovat mechanismy, které tuto závislost udržují. Regulace dokáže jen do určité míry omezit viditelné projevy, ale nedokáže odstranit jádro problému: ekonomický model platforem a jejich schopnost maximalizovat pozornost prostřednictvím emocionálně poutavého obsahu.

Současný stav zároveň vytváří prostor pro aktéry, kteří digitální prostředí využívají k vlastnímu prospěchu, často na úkor veřejného zájmu. Ekonomická motivace maximalizovat zapojení podporuje šíření obsahu, který vyvolává silné emoce, a marginalizuje materiál podporující informovanost, vzdělávání či konstruktivní veřejnou diskusi. V důsledku toho digitální

prostředí aktivně přispívá k šíření ideologií a strategií, které destabilizují demokratické hodnoty.

Z pohledu jednotlivce se tento trend projevuje ztrátou kontroly nad vlastním časem a pozorností. Závislost na sociálních sítích omezuje prostor pro osobní rozvoj, vzdělávání, profesní růst a zapojení do veřejného života, což má zásadní dopad na individuální i společenský blahobyt. Tato dysbalance mezi krátkodobým emocionálním uspokojením a dlouhodobými cíli představuje kritické riziko pro demokracii a kolektivní bezpečnost členských států EU a NATO.

Obnovy důvěry v demokracii nelze dosáhnout restriktivními opatřeními, ale pouze systémovou změnou přístupu k digitálnímu prostředí. Klíčovým prvkem je vybudování integrovaného politického, bezpečnostního, hodnotového a právního rámce, který umožní efektivní správu kyberprostoru a ochranu demokratických principů. Součástí tohoto rámce je koncept ONLINE DEMOKRACIE, který transformuje uživatele z pasivního konzumenta na aktivního účastníka veřejného života.

ONLINE DEMOKRACIE umožňuje občanům zapojit se do rozhodovacích procesů, strukturovaně sdílet názory a podílet se na tvorbě politik s přímým dopadem na jejich život. Posiluje transparentnost, odpovědnost a důvěru – klíčové předpoklady dlouhodobého fungování demokratických systémů. Současně vytváří prostor, aby digitální prostředí podporovalo činnosti přispívající k rozvoji společnosti místo jejího oslabování.

Centrální kybernetický štít představuje systémové řešení, které nahrazuje dosavadní neúčinné regulace. Jeho hlavním posláním je vybudování digitální demokratické infrastruktury, jež umožňuje ochranu a posilování důvěry občanů a efektivně brání dominanci dezinfokracie v globálním informačním prostoru. Bez jeho existence nelze zajistit stabilitu demokratických systémů ani jejich kolektivní obranu v podmínkách 21. století.

Oddíl 5

Ochrana demokracie v kyberprostoru je podmínkou jejího přežití ve fyzickém světě

Posláním Centrálního kybernetického štítu je zajištění kolektivní obrany demokratických zemí, členských zemí Evropské unie a NATO před komplexním spektrem hybridních hrozeb 21. století. Namísto zavádění digitálních regulací a směrnic, které jsou v přímém rozporu se strategickým bojem proti těmto hrozbám, jelikož se soustředí převážně na administrativní potírání jejich následků (mazání obsahu, zákazy, příkazy či nařízení), bude vybudován historicky první politický, bezpečnostní, hodnotový a právní systém v kyberprostoru – ONLINE DEMOKRACIE. Jeho strukturální architektura umožní nejen předcházet šíření dezinformací, nenávisti, propagandy a manipulace s veřejným míněním, ale i odstraňovat jejich příčiny. Jde o existenční nutnost, neboť na zajištění ochrany demokracie v kyberprostoru existenčně závisí osud a přežití demokracie ve fyzickém světě.

V rámci strategického boje proti hybridním hrozbám 21. století je naprosto nepřijatelné spoléhat se na digitální regulace, směrnice, monitoring, analýzy, zákazy či mazání obsahu v kyberprostoru, protože tato opatření reagují pouze na následky šíření dezinformací, nenávisti, propagandy a manipulace s veřejným míněním, a neřeší příčiny. Z toho důvodu nikdy nelze zajistit ochranu obyvatel a státu, národní bezpečnost, integritu demokratických institucí ani důvěru občanů ve fungování mezinárodních organizací, jako jsou Evropská unie, NATO a OSN.

Demokracie je hodnotový systém založený na svobodě, právním státu a lidské důstojnosti a nelze ji chránit příkazy, zákazy ani vojenskou silou. Její skutečná ochrana musí být zajištěna vybudováním integrovaného politického, bezpečnostního, hodnotového a právního systému v kyberprostoru – ONLINE DEMOKRACIE, která propojí digitální a fyzický svět. Právě v kyberprostoru dnes probíhá veškerá společenská a politická komunikace i rozhodovací procesy, na nichž je demokracie ve fyzickém světě existenčně závislá.

V kontextu moderní bezpečnosti a boje proti hybridním hrozbám se integrovaným politickým a bezpečnostním systémem v kyberprostoru rozumí stav, kdy digitální prostor není vnímán jen jako „technologie“ (kabely a servery), ale jako plnohodnotná část státu se stejnými pravidly jako ve fyzickém světě.

V boji proti šíření dezinformací, nenávisti, propagandy a manipulaci s veřejným míněním je naprosto klíčové vybudovat v kyberprostoru digitální demokratickou infrastrukturu, která je základním předpokladem pro vznik funkční ONLINE DEMOKRACIE. Bez ní nelze účinně zavádět žádná preventivní, bezpečnostní ani politická opatření proti hybridním hrozbám, neboť by postrádala základní rámec zajišťující důvěryhodnost, legitimitu a stabilitu demokratických procesů. V digitálním prostředí, kde působí více než pět miliard uživatelů, je proto nezbytné upustit od neúčinných reaktivních regulací, které řeší až následky, a namísto toho vybudovat

integrovaný systém, jenž hybridním útokům svou vnitřní integritou a pevnou architekturou aktivně předchází.

Centrální kybernetický štít je přitom koncipován jako systém vystavěný na deseti pilířích, které společně tvoří komplexní a vzájemně propojený rámec ochrany demokratických procesů. Pouze tento ucelený systém dokáže zajistit odolnost vůči hybridním hrozbám a zabezpečit důvěru v demokracii. Jednotlivé pilíře zahrnují integrovaný právní řád kyberprostoru, digitální suverenitu občanů, transparentní algoritmy veřejné diskuse, bezpečné digitální identity, aktivní detekci a eliminaci útočných narativů u zdroje, ochranu kritické informační infrastruktury, vzdělávací odolnost společnosti, etický rámec umělé inteligence, mezinárodní bezpečnostní koordinaci a včasnou politickou atribuci útoků. Tento desetipilířový model opouští neúčinnou metodu reaktivních zákazů a namísto ní buduje aktivní digitální pevnost, která hybridní agresi nevyvrací až ex post, ale svou systémovou integritou ji činí neúčinnou dříve, než zasáhne veřejné mínění.

Roztříštěnost regulačních přístupů vytváří v kyberprostoru takzvané ‚bezpečné přístavy' pro útočníky, kteří využívají legislativní vakuum k beztrestnému vedení informační války. Namísto jednotné obranné fronty tak vzniká nebezpečný asymetrický prostor, kde jsou demokratické instituce paralyzovány vlastní byrokracií, zatímco hybridní hrozby operují v reálném čase. Dosavadní reaktivní model, založený na mazání obsahu, zcela ignoruje algoritmickou podstatu současné manipulace; namísto řešení příčiny se pouze snaží zmírnit viditelné symptomy společenského rozkladu. Aby se zabránilo další eskalaci násilí a destabilizaci států, je nezbytné nahradit tyto izolované a nefunkční směrnice jednotnou digitální architekturou. Ta musí být postavena na principech preventivního odstrašení a technologické integrity, které jako jediné dokážou v kyberprostoru obnovit řád a zajistit, aby se digitální dezinformace přestaly transformovat v reálnou destrukci demokratického světa.

Integrace Centrálního kybernetického štítu do mezinárodních struktur (EU, NATO) je klíčovou evolucí v obraně: přechodem od fyzických zbraní k ochraně kognitivního a informačního prostoru. V éře, kdy hranice mezi mírem a konfliktem splývá v šedé zóně hybridního působení, již nelze oddělovat bezpečnost územní od bezpečnosti digitální. Absence jednotné technologické a hodnotové platformy v kyberprostoru totiž činí článek 5 Washingtonské smlouvy zranitelným; útok, který rozvrátí vnitřní stabilitu státu skrze masivní manipulaci a rozklad důvěry, může být stejně devastující jako konvenční invaze, avšak bez adekvátní infrastruktury zůstává pod prahem ozbrojené reakce. Vybudování Štítu tak není pouze technickou inovací, ale strategickým imperativem, který definuje novou úroveň odstrašení. Pouze skrze tuto digitální architekturu může Aliance garantovat svou akceschopnost a zajistit, že kolektivní obrana bude v 21. století reálnou zárukou suverenity, nikoliv jen prázdným deklarativním pojmem v digitálně destabilizovaném světě.

Namísto budování centrálních úřadů na pravdu je nutné se zaměřit na vybudování integrované architektury důvěry v demokracii. V kyberprostoru, kde nelze a nesmí být obsah kontrolován skrze subjektivní cenzurní zásahy, musí ochranu zajistit samotná systémová integrita prostředí. Tato digitální demokratická infrastruktura nenahrazuje lidský úsudek, ale poskytuje mu pevný a bezpečný rámec – od nezmanipulovatelných digitálních identit přes transparentní algoritmy až po jasně definovanou právní odpovědnost aktérů. Tím, že systém chrání procesy (jak se informace šíří a jak jsou ověřovány), nikoliv konkrétní slova (co je řečeno), vytváří imunní prostředí, kde dezinformace ztrácejí svou ničivou sílu, aniž by byla obětována svoboda

projevu. Tento posun od obsahu k infrastruktuře je jedinou možnou cestou, jak ochránit pět miliard uživatelů před technologickou diktaturou i hybridním rozvratem zároveň.

ONLINE DEMOKRACIE představuje historicky první integrovaný politický, bezpečnostní, hodnotový a právní systém v kyberprostoru. Tato nová globální autorita není dalším úřadem, ale univerzálním operačním systémem digitální civilizace – chybějícím článkem mezi technologickým pokrokem a společenskou smlouvou. Vybudování této legitimní struktury umožní vepsat demokratické principy přímo do kódu a síťových protokolů, čímž se kyberprostor transformuje z nekontrolovaného bojiště v bezpečný a transparentní prostor. Bez tohoto systémového ukotvení zůstanou pokusy o obranu proti dezinformacím, nenávisti, propagandě a manipulaci s veřejným míněním jen marným bojem s větrnými mlýny; bez digitální státnosti totiž nelze v online světě garantovat právo, bezpečnost ani svobodu.

VAROVÁNÍ

Pokud se státní a mezinárodní regulace kyberprostoru omezují pouze na represivní mechanismy – tedy na směrnice, zákazy, příkazy a mazání obsahu – a přitom ignorují hloubkovou erozi společenské soudržnosti, kterou tento obsah vyvolává, nejedná se o obranu demokracie, nýbrž o budování digitálního autoritářství.

Skutečná obrana vyžaduje systémové ukotvení hodnot a práva přímo v architektuře sítě (digitální státnost), nikoliv jen nástroje pro cenzuru textu. Bez tohoto rozlišení se snaha o bezpečnost mění v nástroj kontroly, který místo ochrany svobody likviduje samotnou podstatu demokratického dialogu.

ONLINE DEMOKRACIE a její Centrální kybernetický štít proto nepředstavují volbu, ale existenční nutnost. Bez této infrastruktury, která by v kyberprostoru ukotvila stejnou míru právní a bezpečnostní jistoty, jakou požíváme ve fyzickém světě, zůstávají moderní státy jen prázdnými schránkami, jejichž suverenita končí u prvního internetového kabelu. Pouze integrace deseti pilířů Štítu do samotné DNA digitálního světa umožní státům a mezinárodním institucím i alianci NATO znovu převzít iniciativu a proměnit kyberprostor z nástroje destrukce v bezpečný pilíř civilizace.

Nedostatek odborné připravenosti politických činitelů pro digitální prostředí je však strategickým bezpečnostním rizikem. Funkce v národní a mezinárodní bezpečnosti vyžadují lídry, kteří do úřadu nastupují již plně vycvičeni pro hybridní střety. Pokud se rozhodovací procesy opírají o teoretické znalosti místo o reálnou zkušenost s fyzickým a kybernetickým bojištěm, výsledkem jsou pak chybná rozhodnutí s destruktivním dopadem na bezpečnostní architekturu státu. ONLINE DEMOKRACIE a její Centrální kybernetický štít proto vyžadují

novou elitu – lídry, kteří prošli autentickým výcvikem v digitálním konfliktním prostředí a pro které je kyberprostor přirozeným operačním polem.

Rok 2014, kdy hybridní agrese naplno odhalila zranitelnost digitálně propojené společnosti, vytvořil nebezpečný precedens beztrestné manipulace. Absence robustních obranných mechanismů tehdy umožnila, aby se kyberprostor stal inkubátorem informační války. Z masového šíření dezinformací, nenávisti a propagandy se postupně zrodil fenomén dezinfokracie, který plně ovládl sociální sítě a skrze ně začal nekontrolovaně formovat veřejné mínění i politickou realitu.[27]

Z masového šíření dezinformací, nenávisti a propagandy v kyberprostoru se zrodila informační válka, která skrze sociální sítě následně vyústila ve fenomén dezinfokracie.

Dezinfokracie je nejničivější hybridní režim 21. století, který působí již více než patnáct let na sociálních sítích a způsobuje informační dezorientaci veřejnosti. Kvůli tomu dochází ke špatným politickým a osobním rozhodnutím, důsledkem jsou zničené mezilidské vztahy, narůstající hádky, nenávist, frustrace, vztek, strach, zoufalství, bezmoc a beznaděj, rozvrácené rodiny, přibývající konflikty mezi lidmi, chaos, kriticky oslabená bezpečnost, sociální, ekonomická a právní stabilita země, prohlubující se chudoba, duševní poruchy a utrpení, terorismus, války, násilí, radikalizace, extremismus, postupná ztráta důvěry ve stát a mezinárodní systém a rozpadající se demokracie ve světě.

V kyberprostoru se odehrávají zvěrstva, o jejichž rozsahu nemají občané ani stát plné povědomí. Tato digitální hrůza zahrnuje nejen šíření dezinformací, manipulaci veřejného mínění, nenávist, digitální násilí nebo informační válku, ale i online maskirovku – digitální invazi do demokratických zemí, kyberokupaci států – autoritářství, omezování osobní svobody a svobody projevu, cenzuru, radikalizaci na sociálních sítích – tedy sociální terorismus, digitální rakovinu, vlivové operace včetně aktivit zpravodajských služeb, hybridní útoky na demokracii aj., které skrze mobilní zařízení pronikají do fyzického světa a existenčně ohrožují demokracii, rozvracejí stát a kriticky oslabují ekonomický, technologický rozvoj a národní bezpečnost. Tyto destruktivní procesy představují souhrnně fenomén označovaný jako „dezinfokracie“.

Aby politici dokázali účinně čelit dezinfokracii – nejničivějšímu hybridnímu režimu 21. století, musí disponovat přímou zkušeností s konfliktním prostředím v kyberprostoru. Tuto zkušenost však většina z nich postrádá. Spoléhání na poradce nenahradí chybějící vhled do dynamiky bleskového šíření nenávisti a sofistikovaných manipulací. V krizích se proto elity uchylují k zastaralým směrnicím a neúčinným zákazům, které v digitálním světě selhávají.

Tento deficit zkušeností z ‚první linie‘ činí bezpečnostní struktury neakceschopnými. Politický systém bez funkčního kybernetického protějšku je v moderní civilizaci strategicky neudržitelný a přímo ohrožuje podstatu demokracie.

Jedinou účinnou obranou je ONLINE DEMOKRACIE – integrovaný politický, bezpečnostní, hodnotový a právní systém ukotvený v digitální architektuře. Tato struktura trvale propojuje fyzický a digitální svět a garantuje odolnost demokratických procesů proti hybridním hrozbám.

Centrální kybernetický štít vznikl jako nejvyšší bezpečnostní záruka této nové infrastruktury. Brání přenosu hybridních hrozeb z digitálních zařízení do reality a vytváří bezpečnější prostor pro pět miliard uživatelů internetu a sociálních sítí. Je efektivnější než jakákoli byrokratická regulace, jejíž nesourodá implementace mezi státy paradoxně prohlubuje chaos a destabilizaci. Bez Centrálního kybernetického štítu dnes nelze zajistit stabilitu demokratických zemí EU ani akceschopnost NATO. Je existenční nutností pro kolektivní obranu moderní civilizace.

Oddíl 6

Princip kolektivní obrany demokracie v kyberprostoru

Centrální kybernetický štít (Bohemia: Central Cyber Shield) představuje nejvyšší formu ochrany demokratické infrastruktury v digitálním prostoru. Jeho existence je dnes nezbytná, neboť budoucnost demokracie ve fyzickém světě je přímo závislá na ONLINE DEMOKRACII – systému, který propojuje digitální a fyzický prostor prostřednictvím jednotného politického, bezpečnostního, hodnotového a právního rámce. Digitální civilizace, kterou dnes tvoří více než pět miliard uživatelů internetu a sociálních sítí, vyžaduje stabilní, legitimní a důvěryhodnou infrastrukturu, která zásadně překračuje možnosti tradičních směrnic, regulací, zákazů či příkazů. Tyto dosavadní mechanismy se ukazují jako fragmentární, nekoordinované a v konečném důsledku často kontraproduktivní.

Hlavním úkolem Centrálního kybernetického štítu je zajištění kolektivní obrany demokracie v kyberprostoru, která dnes prakticky neexistuje. Aliance NATO sice disponuje článkem 5 pro kolektivní obranu ve fyzickém světě, ale v kyberprostoru zůstávají spojenci i celá Evropská unie bezbranní. Dosud neexistuje žádný funkční mechanismus kolektivní kybernetické obrany, který by dokázal čelit dezinfokracii – nejničivějšímu hybridnímu režimu 21. století. Tento zásadní deficit přímo ohrožuje bezpečnost, odolnost a stabilitu demokratického světa. Centrální kybernetický štít tuto mezeru odstraňuje a poskytuje univerzální rámec kolektivní obrany, který mohou využívat nejen členské státy NATO, ale i členské státy EU, ostatní demokratické země a mezinárodní instituce. Tím zajišťuje, že obranyschopnost států již není omezena pouze na fyzický prostor, ale je plně rozšířena i do kyberprostoru, kde dnes probíhá rozhodující část politické, společenské a bezpečnostní komunikace.

Kolektivní obranu demokracie nelze zajistit zákazy, směrnicemi či cenzurou. Pouze vybudováním integrovaného politického, bezpečnostního, hodnotového a právního systému – ONLINE DEMOKRACIE – je možné propojit fyzický a digitální svět a zajistit jednotný rámec ochrany demokratické infrastruktury. Tento systém plně integruje všechny formy řízení, monitoringu, prevence a reakce proti hybridním hrozbám, které samostatně nemohou žádné státy ani mezinárodní organizace účinně zvládnout. Politické systémy fungující výhradně ve fyzickém světě bez svého digitálního protějšku jsou v dnešní době strategicky neudržitelné a představují existenční riziko pro stabilitu, bezpečnost i samotnou podstatu demokracie.

Existenční požadavek kolektivní kybernetické obrany: rozšíření článku 5 o digitální článek 5

V současné době není ani aliance NATO plně obranyschopná. Zatímco pokračují strategické investice do vojenské infrastruktury, dochází zároveň k postupnému oslabování kolektivní obrany způsobenému masivním šířením dezinformací, nenávisti, propagandy a manipulace s veřejným míněním, zejména na sociálních sítích. Z těchto procesů se zrodila informační válka, z níž se vyvinul fenomén známý jako dezinfokracie – nejničivější hybridní režim 21. století,

který systematicky narušuje důvěru občanů, destabilizuje demokratické instituce a ohrožuje schopnost členských států účinně spolupracovat.

V důsledku tohoto vývoje některé členské státy oprávněně zpochybňují, zda aliance NATO dokáže plně naplnit své závazky, včetně investic do obranných kapacit a dodržování aliančních dohod, neboť klíčový předpoklad obrany – důvěra v demokracii a stabilitu institucí – je přímo ohrožen. Existenčním řešením je proto zavedení tzv. digitálního článku 5, který by prostřednictvím Centrálního kybernetického štítu aktivně chránil alianci proti šíření dezinformací, nenávisti, propagandy a manipulace. Tento nástroj zajistí komplexní ochranu důvěry, stabilitu demokratických institucí a skutečnou obranyschopnost členských států i celé aliance NATO v digitálním věku, čímž se stává nezbytným pilířem kolektivní obrany v 21. století.[28]

Struktura Centrálního kybernetického štítu je vybudována na principu kolektivní obrany a tvoří ji deset aliančních bezpečnostních pilířů, které dohromady představují komplexní a ucelený systém ochrany digitální demokratické infrastruktury:

- **ONLINE DEMOKRACIE**: První politický systém v kyberprostoru, který zajišťuje legitimní rozhodování, kolektivní obranu a propojení digitálního a fyzického světa skrze komplexní systém ochrany a rozvoje digitální státnosti, národní identity, legitimity a suverenity státu. Tento systém garantuje ochranu lidských práv, svobodu projevu, lidskou důstojnost a právo na digitální existenci.
- **Digitální demokratická infrastruktura:** Jednotná platforma nahrazující fragmentární regulace a poskytující koordinovaný rámec pro politická, bezpečnostní a právní opatření, která zajišťuje kolektivní obranu a neprostupný digitální štít pro členské státy EU, NATO a všechny demokratické spojence.
- **Sociální síť Politinn:** První evropská demokratická platforma nové generace, která zajišťuje ochranu a rozvoj demokracie v digitálním i fyzickém světě. V kyberprostoru buduje ucelený politický, bezpečnostní, hodnotový a právní systém, umožňuje evoluční rozvoj volebních procesů skrze e-voliče a e-kandidatury a garantuje legitimní rozhodování, čímž zajišťuje kolektivní obranu a stabilitu digitální civilizace pro členské státy EU a NATO.
- **Kyberstrategie 2026 – Boj proti dezinfokracii:** Dezinfokracie je nejničivější hybridní režim 21. století. Namísto neúčinných restriktivních opatření, regulací, směrnic a selektivně dodržovaných zákazů, které jen prohlubují chaos a násilí, buduje tento pilíř v kyberprostoru integrovaný politický, bezpečnostní, hodnotový a právní systém, který zabrání nárůstu hrozeb a konfliktů v podobě šíření dezinformací, nenávisti, propagandy a manipulace s veřejným míněním, které skrze sociální sítě a mobilní zařízení agresivně pronikají do fyzického světa.
- **Centrální kybernetický štít pro NATO:** Zavedením digitálního článku 5 NATO nezbytně adaptujeme na realitu 21. století. Kodifikujeme tím princip, že dezinfokracie – nejničivější hybridní režim 21. století působící na sociálních sítích – vyžaduje okamžitou spojeneckou reakci. Systémové narušování demokratických procesů se tak stává útokem na celou Alianci a kybernetická kolektivní obrana nedílnou součástí naší nedělitelné bezpečnosti.
- **Digitální světová organizace (DWO):** Nejlepším způsobem kolektivní obrany demokracie je vybudování nového světového řádu v kyberprostoru. Budování tohoto řádu bez Centrálního kybernetického štítu, jehož součástí je i Digitální světová

organizace (DWO), je předem odsouzeno k neúspěchu. Poprvé v historii totiž lidstvo žije ve dvou světech současně – fyzickém a digitálním. Kvůli této nové dimenzi reality je nezbytné, aby DWO vybudovala v kyberprostoru inovativní politický, bezpečnostní, hodnotový a právní systém pro více než pět miliard uživatelů internetu a sociálních sítí.

- **Kyberstrategie 2026 – Boj proti „digitální rakovině“:** Tento pilíř slouží jako aktivní obranný štít a prevence proti destruktivnímu digitálnímu obsahu, který rozkládá lidskou psychiku i společnost. Namísto pasivního přihlížení buduje systém, který v kyberprostoru garantuje bezpečné prostředí a chrání život a fyzické i duševní zdraví více než pěti miliard uživatelů internetu a sociálních sítí. Cílem je zastavit technologickou degradaci člověka, předcházet digitální závislosti a eliminovat toxické algoritmy, které vyvolávají deprese, úzkosti a sebedestruktivní chování. Tímto způsobem Kyberstrategie 2026 chrání lidskou integritu a zajišťuje, že digitální svět zůstane prostorem pro rozvoj, nikoliv nástrojem pro ničení lidského zdraví a důstojnosti.
- **Kyberstrategie 2026 – Kybernetické přezbrojení:** Jde o strategickou modernizaci obranných mechanismů, jejíž nedílnou součástí je vybudování integrovaného politického, bezpečnostního, hodnotového a právního systému. Kvalita a účinnost kybernetického přezbrojení přímo závisí na stabilitě tohoto nového řádu, který transformuje technologickou sílu v nástroj ochrany digitální státnosti. V rámci Kyberstrategie 2026 získává toto přezbrojení stejnou váhu jako konvenční vojenské investice, neboť bez systémové pevnosti právního a hodnotového ukotvení v kyberprostoru zůstává jakákoliv technická ochrana proti sofistikovaným útokům nefunkční.
- **Kyberstrategie 2026 – Boj proti sociálnímu terorismu:** Strategický pilíř Kyberstrategie 2026 zaměřený na eliminaci radikalizace občanů v prostředí sociálních sítí. Sociální terorismus definujeme jako proces cíleného rozvratu společnosti skrze digitální platformy, kde dochází k systémovému šíření nenávisti, strachu a dezinformací s cílem destabilizovat legitimní instituce a demokratický řád. Tragické následky tohoto fenoménu nezůstávají v kyberprostoru, ale skrze digitální násilí a psychologickou manipulaci přímo expandují do fyzického světa, kde vyvolávají reálné konflikty, agresi a rozklad sociální soudržnosti. Tento pilíř buduje aktivní systém prevence a ochrany, který brání přeměně digitálních zařízení v nástroje radikalizace, a garantuje tak bezpečí občanů i stabilitu státu.
- **Budování bezpečnostního, hodnotového a právního systému v kyberprostoru:** Budování pilířů digitální státnosti, suverenity a národní identity, které zajišťují legitimitu státu v kyberprostoru. Tento komplexní systém tvoří skutečnou ochranu, kterou nedokážou zajistit žádná restriktivní opatření, digitální regulace, směrnice, zákazy ani nařízení. Zatímco byrokratické příkazy jsou v digitálním světě neúčinné a státy je často ignorují, tento pilíř vytváří funkční řád, který nekompromisně garantuje ochranu lidských práv, svobodu projevu a lidskou důstojnost. Pro všechny demokratické země, členské státy EU i NATO je tato suverénní infrastruktura jedinou cestou, jak ochránit národní identitu před rozkladem a zajistit přežití demokracie ve fyzickém světě.

Každý z deseti pilířů nahrazuje dosavadní neefektivní regulace, směrnice a zákazy, které byly fragmentární, nekoordinované a krátkozraké. Dohromady tvoří stabilní, legitimní a bezpečný rámec pro více než pět miliard uživatelů internetu a sociálních sítí. Tento systém aktivně

podporuje společenskou soudržnost a zajišťuje plně funkční propojení digitálního a fyzického prostoru, čímž vytváří jednotnou a neprostupnou architekturu moderní civilizace.

Centrální kybernetický štít představuje nejen nástroj ochrany demokratické infrastruktury, ale i garanta kolektivní obrany v kyberprostoru. Jde o klíčový prvek, bez něhož nemohou členské státy EU a NATO, ale ani všechny ostatní státy světa a celé mezinárodní společenství zajistit svou stabilitu a bezpečnost. Tento systém je historicky jedinečný a existenčně nezbytný; pouze prostřednictvím deseti pilířů Centrálního kybernetického štítu lze totiž garantovat existenci demokracie v obou světech současně, zajistit ochranu lidských práv a veřejného dobra a upevnit celkovou bezpečnostní odolnost moderní civilizace.

Oddíl 7

ONLINE DEMOKRACIE propojí digitální a fyzický svět

Každý stát disponuje vlastním politickým, bezpečnostním, hodnotovým a právním systémem, který určuje fungování společnosti, garantuje ochranu práv i svobod občanů a zajišťuje stabilitu demokratických procesů. Tento systém je pevně ukotven ve fyzickém světě, avšak jeho plnohodnotný ekvivalent v kyberprostoru dosud chybí. Právě tato systémová trhlina představuje hlavní příčinu narůstajících hrozeb, konfliktů a destabilizačních jevů, které vznikají v digitálním prostředí a následně se prostřednictvím sociálních sítí a mobilních zařízení nekontrolovaně přenášejí do fyzického světa.

Kyberprostor je globální a bezhraniční prostředí, ve kterém působí více než pět miliard uživatelů internetu a sociálních sítí. Na rozdíl od fyzického světa zde však chybí jednotný legitimní a funkční systém řízení společnosti, který by odpovídal politickým, bezpečnostním, hodnotovým a právním strukturám jednotlivých států. Tato systémová absence vytváří nekontrolované prostředí, v němž dochází k masivnímu šíření dezinformací, nenávisti, propagandy a manipulaci s veřejným míněním, což nevyhnutelně vede k polarizaci společnosti, eskalaci konfliktů a k systémovému narušování demokratických procesů.

Dosavadní přístup států i mezinárodních institucí, včetně Evropské unie, se doposud omezoval pouze na zavádění digitálních regulací, směrnic a nařízení. Tento model se však ukazuje jako zásadně nedostatečný a systémově nefunkční. Regulace jsou totiž aplikovány pouze na omezený okruh států a subjektů, zatímco jiné země je neuplatňují vůbec. V prostředí, které je ze své podstaty globální a propojené, tak vzniká kritická asymetrie: pravidla platí jen pro fragmentární část digitálního prostoru, zatímco jeho zbytek zůstává mimo jakoukoli kontrolu. Výsledkem je prohlubující se chaos, fragmentace a neustále se zvyšující bezpečnostní i sociální napětí.

Tato nesourodost vytváří paradoxní situaci, kdy regulace, jejichž cílem má být ochrana demokracie, ve skutečnosti šíření hybridních hrozeb nezastavují, ale naopak přispívají k jejich eskalaci. Dezinformace, propaganda a manipulace se totiž šíří napříč digitálními hranicemi bez ohledu na lokální legislativu. Jakékoli restriktivní opatření v jedné části kyberprostoru je snadno obcházeno prostřednictvím jiných jurisdikcí, což činí dosavadní fragmentární přístup dlouhodobě neudržitelným a strategicky neefektivním.

Z uvedeného vyplývá, že samotné digitální regulace nemohou nikdy představovat skutečné řešení. Neřeší totiž podstatu problému, kterou je absence komplexního a legitimního systému řízení společnosti v kyberprostoru. Ochrana demokracie v digitálním prostředí proto nemůže být založena na dílčích restriktivních opatřeních, ale vyžaduje hloubkovou systémovou transformaci. Pouze vytvoření plnohodnotné digitální státnosti a správy věcí veřejných v kyberprostoru může zajistit stabilitu a bezpečnost, kterou současné fragmentární směrnice postrádají.

Jediným dlouhodobě udržitelným řešením je vybudování plnohodnotného politického, bezpečnostního, hodnotového a právního systému v kyberprostoru, který bude odpovídat principům fungování demokratických států ve fyzickém světě. Tento systém musí být založen na principech ONLINE DEMOKRACIE a musí být pevně ukotven v robustní digitální demokratické infrastruktuře, která zajistí legitimitu, transparentnost a důvěryhodnost všech procesů probíhajících v digitálním prostředí.

Klíčovou roli v tomto procesu hraje Centrální kybernetický štít. Ten nepředstavuje pouze technologický nástroj, ale komplexní systémový rámec, který umožňuje definovat a prosadit jednotná pravidla pro fungování digitální civilizace. Jeho hlavním úkolem je zajistit ochranu více než pěti miliard uživatelů internetu a sociálních sítí, posílit odolnost vůči hybridním hrozbám a zamezit jejich destruktivnímu přenosu do fyzického světa.

Centrální kybernetický štít tak prostřednictvím ONLINE DEMOKRACIE vytváří základní pilíře pro vznik nového, globálně propojeného, systému, který integruje fyzický a digitální svět do jednoho funkčního celku. Na rozdíl od fragmentovaných regulací poskytuje tento mechanismus jednotný, konzistentní a systémově ukotvený přístup k ochraně demokracie, lidských práv a bezpečnosti. Právě propojení Štítu s ONLINE DEMOKRACIÍ zajišťuje, že technologická obrana není jen pasivním filtrem, ale legitimním nástrojem digitální státnosti, který garantuje stabilitu moderní civilizace.

Bez vybudování tohoto systému bude kyberprostor i nadále zdrojem nestability, konfliktů a hybridních hrozeb, které budou postupně rozkládat nejen digitální prostředí, ale i samotné základy demokratických států. V moderní digitální civilizaci již nelze oddělovat fungování společnosti ve fyzickém a virtuálním světě. Oba tyto prostory musí být neoddělitelně propojeny jednotným legitimním a funkčním systémem, který zajistí jejich stabilitu, bezpečnost a dlouhodobou udržitelnost.

Oddíl 8

Digitální státnost: Politický a právní základ státu a demokracie v kyberprostoru

---

Digitální státnost představuje komplexní a systémově provázaný rámec, jehož cílem je přenést výkon státní suverenity, demokratických procesů a ochrany občanů do kyberprostoru. Nejde pouze o technologickou infrastrukturu, ale o plnohodnotné rozšíření státní existence do digitální dimenze, která je dnes klíčovým prostředím pro fungování moderní společnosti. Základním principem digitální státnosti je vytvoření funkčního politického, bezpečnostního, hodnotového a právního systému, který bude v kyberprostoru plně odpovídat strukturám fyzického světa a zároveň je nezbytným způsobem doplňovat.

V této souvislosti je nezbytné striktně rozlišovat mezi dvěma klíčovými rovinami ochrany, které jsou často mylně zaměňovány, ačkoliv mají zásadně odlišný charakter i funkci.

První rovinu představuje technická a bezpečnostní ochrana státu v kyberprostoru. Ta zahrnuje zejména zabezpečení kritické infrastruktury, komunikačních a síťových systémů, státních databází, cloudových úložišť, energetických a dopravních uzlů, zdravotnických a finančních informačních systémů, vojenských technologií a autentizačních systémů. Tato úroveň obrany je zaměřena proti kybernetickým útokům, hackerským operacím, sabotážím či průmyslové špionáži a je nezbytná pro zajištění elementární funkčnosti státu a jeho technologické stability. Jedná se však primárně o obranu infrastruktury, nikoliv o ochranu samotné podstaty demokracie.

Druhou, neméně zásadní rovinou je ochrana digitální státnosti jako hodnotového, politického a právního systému. Tato ochrana směřuje k zachování integrity demokracie v kyberprostoru – tedy k obraně svobody projevu, lidských práv a důstojnosti. Zásadní prioritou této roviny je zajištění legitimity a bezpečnosti digitálních demokratických procesů, jako jsou online volby (e-voting), elektronická referenda či digitální participace občanů na správě věcí veřejných. Nejde již jen o technické šifrování, ale o garantování právní nezpochybnitelnosti a důvěry občanů v digitální instituce. Do této roviny spadá rovněž obrana proti dezinformacím, manipulaci s veřejným míněním a psychologickým operacím. Tyto formy hybridních hrozeb neútočí na technickou infrastrukturu, ale na samotnou podstatu demokratického rozhodování a hodnotové ukotvení společnosti.

Právě v této druhé rovině hraje klíčovou roli imunitní systém demokracie. Jeho základním pilířem je ochrana, budování a udržování důvěry v demokracii. Tento imunitní systém představuje soubor systémových, preventivních a adaptačních mechanismů, které svou sílu čerpají právě z autentické důvěry občanů v instituce a hodnoty státu. Díky tomu je schopen rozpoznat, analyzovat a neutralizovat škodlivé informační vlivy přirozenou cestou, bez nutnosti represivních zásahů. Tento přístup je zásadně odlišný od tradičních forem regulace: namísto neúčinného posilování kontroly nad obsahem se zaměřuje na obnovu důvěry jakožto klíčového faktoru odolnosti celého systému vůči manipulaci.

Zásadním problémem současného přístupu k bezpečnosti je skutečnost, že většina států se soustředí téměř výhradně na první rovinu – tedy na technickou ochranu infrastruktury. Druhá rovina, představující ochranu samotné digitální státnosti jakožto nositele demokratických hodnot, však zůstává systémově podceněna a nedostatečně řešena. Tento nesoulad vytváří kritickou bezpečnostní mezeru; moderní hybridní hrozby totiž primárně necílí pouze na technické zázemí, ale útočí přímo na hodnotový a rozhodovací systém společnosti.

Jedním ze stěžejních pilířů digitální státnosti je proto ONLINE DEMOKRACIE, která představuje nový model demokratického řízení společnosti v digitálním prostředí. Tento model umožňuje přímé zapojení občanů do rozhodovacích procesů, radikálně zvyšuje transparentnost a zásadním způsobem posiluje legitimitu celého politického systému. ONLINE DEMOKRACIE tak transformuje pasivní digitální konzumenty v aktivní digitální občany, čímž vytváří nezbytný hodnotový protipól k dosavadnímu roztříštěnému a neefektivnímu systému správy věcí veřejných.

ONLINE DEMOKRACIE je zároveň nástrojem pro ochranu hodnotového systému, neboť vytváří strukturovaný a důvěryhodný prostor pro veřejnou diskusi a rozhodování. Klíčovým nástrojem pro realizaci tohoto modelu je sociální síť Politinn – evropská platforma nové generace, která slouží jako institucionální a komunikační prostředí pro autentickou interakci mezi občany, politiky a institucemi. Tato platforma není pouhým komunikačním nástrojem, ale základním stavebním prvkem digitální státnosti, který umožňuje organické propojení všech jejích složek do jednoho funkčního a legitimního celku.

Základním systémovým rámcem je digitální demokratická infrastruktura, která zajišťuje funkční propojení technické a hodnotové roviny. Tato infrastruktura vytváří prostředí, ve kterém může koexistovat bezpečná technologická základna se stabilním demokratickým systémem. Její nedílnou součástí jsou mimo jiné digitální identita občanů, bezpečné komunikační kanály, verifikační mechanismy, transparentní datové struktury a institucionální nástroje pro efektivní řízení a kontrolu procesů. Pouze tato komplexní infrastruktura dokáže transformovat kyberprostor z nekontrolovaného prostředí v legitimní součást státu.

Institucionální oporou celého systému je Národní bezpečnostní centrum pro obranu demokracie v kyberprostoru, které propojuje technickou ochranu státu s ochranou jeho hodnotového systému. Toto centrum koordinuje nejen aktivní obranu proti kybernetickým útokům, ale i komplexní ochranu demokratických procesů před hybridními hrozbami. Působí jako integrující prvek, který zajišťuje součinnost mezi technologickým zabezpečením infrastruktury a obranou integrity digitální státnosti, čímž vytváří jednotnou frontu proti pokusům o vnější i vnitřní destabilizaci společnosti.

Další nedílnou součástí digitální státnosti jsou hybridní politické programy, které reflektují organické propojení fyzického a digitálního světa. Na ně navazují elektronické volby (e-volby), které představují technologicky vyspělý nástroj pro bezpečné, transparentní a inkluzivní zapojení občanů do demokratických procesů. Tyto prvky společně zajišťují, že politická aktivita i samotný akt volby odpovídají dynamice 21. století, přičemž díky robustní digitální infrastruktuře garantují integritu a nezpochybnitelnost volebních výsledků.

Celý tento komplexní systém je integrován prostřednictvím Centrálního kybernetického štítu, který plní nepostradatelnou dvojí funkci. Na jedné straně zajišťuje technickou ochranu

infrastruktury, zatímco na straně druhé chrání samotnou digitální státnost jakožto nositele demokratických hodnot. Právě tato schopnost simultánně propojit a bránit obě tyto roviny činí z Centrálního kybernetického štítu klíčový nástroj pro zajištění stability, suverenity a bezpečnosti moderní digitální civilizace.

Digitální státnost tak představuje nejen technologickou inovaci, ale především zásadní civilizační posun. Bez jejího vybudování zůstává stát kriticky zranitelný – a to nejen po technické stránce, ale především v rovině hodnot, důvěry a legitimity. Právě tyto oblasti jsou pro dlouhodobou stabilitu a fungování demokracie naprosto klíčové. Absence digitální státnosti tak v moderní éře znamená rezignaci na ochranu samotné podstaty svobodné společnosti v prostředí, které dnes určuje naši budoucnost.

Oddíl 9

Imunitní systém demokracie

Imunitní systém demokracie je součástí integrovaného politického, bezpečnostního, hodnotového a právního systému. Jeho podstatou je především budování a rozvoj důvěry v demokracii, která je základním předpokladem odolnosti státu a mezinárodních institucí, jako jsou EU, NATO a další. Jako nedílná součást Centrálního kybernetického štítu představuje tento systém soubor aktivních mechanismů, které chrání demokratický systém před vnitřním rozkladem, autoritářskými tendencemi, populismem a extremismem. Je to základní struktura, která prostřednictvím digitální demokratické infrastruktury zajišťuje bezpečnostní, sociální, ekonomickou, environmentální a právní stabilitu státu a mezinárodního řádu.

Imunitní systém demokracie funguje obdobně jako imunitní systém lidského organismu. Pokud je silný, dokáže přirozeně odolávat vnějším i vnitřním hrozbám, stabilizovat společenské vztahy a udržovat soudržnost společnosti. Pokud však dochází k jeho oslabování, demokratický systém ztrácí schopnost rozpoznávat a eliminovat destruktivní vlivy, což vede k postupné destabilizaci celého společenského a politického prostředí.

Kritickým momentem narušení imunitního systému demokracie je situace, kdy občané přestávají být schopni spolehlivě rozlišovat mezi pravdou a lží. Tento stav je přímým důsledkem systematického šíření dezinformací, manipulace s veřejným míněním, nenávisti a propagandy, které zaplavují kyberprostor v masivním měřítku. V prostředí, kde neexistuje jasný a důvěryhodný referenční rámec reality, dochází k informační dezorientaci, která zásadně ovlivňuje rozhodování jednotlivců i celé společnosti.

Tato dezorientace postupně přerůstá v hlubokou nedůvěru, která narušuje mezilidské vztahy i vztah občanů ke státu. Lidé se začínají mezi sebou konfrontovat na základě odlišných interpretací reality, což vede k narůstajícím konfliktům, hádkám a postupně i k nenávisti. Tato nenávist následně eskaluje do radikalizace, agresivního chování a fyzického násilí. Společnost se tak dostává do stavu vnitřního rozkladu, kdy přestává fungovat jako soudržný celek.

V tomto kontextu vzniká informační válka, která se neodehrává pouze mezi státy, ale především uvnitř samotných společností. Jejími aktéry nejsou jen politické nebo státní struktury, ale i samotní občané, kteří se – často nevědomě – stávají součástí šíření manipulativního obsahu. Informační válka tak zásadním způsobem oslabuje imunitní systém demokracie tím, že systematicky narušuje důvěru jako jeho základní stavební prvek.

Z této informační války se postupně formuje fenomén označovaný jako dezinfokracie – nejničivější hybridní režim 21. století. Tento režim je založen na systematickém a dlouhodobém narušování informačního prostředí, jehož cílem je destabilizace společnosti prostřednictvím chaosu, nedůvěry a polarizace. Dezinfokracie nepůsobí jednorázově, ale kontinuálně – eroduje důvěru a tím rozkládá celý imunitní systém demokracie.

Důsledky tohoto působení jsou hluboké a komplexní. Dochází k rozpadu rodinných a komunitních vazeb, nárůstu konfliktů mezi jednotlivci i skupinami, šíření strachu, frustrace, bezmoci a beznaděje. Současně se oslabuje bezpečnostní, sociální, ekonomická i právní stabilita státu. Informační dezorientace vede ke špatným osobním i politickým rozhodnutím, která dále prohlubují destabilizaci společnosti.

Dezinfokracie útočí přímo na imunitní systém demokracie – tedy na důvěru. Jakmile důvěra klesá, oslabuje se schopnost společnosti bránit se manipulaci a udržovat demokratický řád. Čím slabší je důvěra, tím rychleji dochází k rozpadu demokratických struktur. Tento proces má akcelerační charakter: oslabení důvěry vede k dalšímu šíření dezinformací a konfliktů, což následně důvěru dále oslabuje.

V extrémním případě může dojít k úplnému kolapsu imunitního systému demokracie. V takovém stavu již společnost není schopna rozlišovat mezi legitimními a nelegitimními informacemi, mezi pravdou a manipulací, ani mezi demokratickými a nedemokratickými principy. Výsledkem je rozpad demokratického systému jako takového, protože bez důvěry nelze demokracii udržet ani obnovit.

Ochrana imunitního systému demokracie proto představuje jednu z nejvyšších priorit moderního státu i mezinárodního společenství. Nejde pouze o ochranu informačního prostoru, ale o ochranu samotné podstaty demokratického zřízení. Klíčovým nástrojem této ochrany je vybudování funkčního politického, bezpečnostního, hodnotového a právního systému v kyberprostoru, který dokáže prostřednictvím Centrálního kybernetického štítu systematicky posilovat důvěru, stabilizovat informační prostředí a odolávat destruktivnímu působení dezinfokracie.

Bez tohoto systému a jeho Centrálního kybernetického štítu zůstává svobodná společnost zranitelná a její imunitní systém pod náporem cizích zájmů a chaosu postupně selhává. Naopak jeho vybudování a důsledná implementace představují základní předpoklad pro zachování stability, bezpečnosti a dlouhodobé existence demokratického řádu v podmínkách digitální civilizace.

Oddíl 10

Koncept vybudování a fungování Centrálního kybernetického štítu

---

Vybudování Centrálního kybernetického štítu představuje zcela zásadní civilizační krok, který nelze redukovat pouze na technologickou nebo bezpečnostní iniciativu. Jde o vznik nové globální instituce, která musí mít nejen digitální, ale především reálnou, fyzickou podobu. Tento štít musí být vybudován jako rozsáhlý, vysoce zabezpečený technologický komplex, situovaný v některé z demokratických zemí, který se stane centrálním řídicím a koordinačním uzlem pro ochranu demokracie v kyberprostoru. Nejde o běžnou instituci, ale o obří mezinárodní centrum, které svou velikostí, významem i funkcí nemá v moderní historii obdoby.

Tento komplex musí být koncipován jako velkokapacitní infrastruktura, ve které bude působit několik tisíc špičkových odborníků z celého světa. Na jednom místě se zde soustředí nejvyšší úroveň lidského know-how v oblasti kyberbezpečnosti, ochrany demokratických procesů, politických systémů, práva, analýzy dat, informačních operací i strategického řízení. Právě tato koncentrace expertízy je klíčová, protože současný stav, kdy jsou tyto kapacity rozptýleny napříč jednotlivými státy a institucemi, vede k roztříštěnosti, pomalé reakční schopnosti a nízké efektivitě při řešení globálních hrozeb.

Centrální kybernetický štít musí být koncipován jako prostor, kde budou mít své zastoupení všechny státy, které mají zájem chránit své občany, svou suverenitu a svou digitální státnost. Nejde přitom výhradně o demokratické země, i když právě ty by měly stát u jeho zrodu. Kyberprostor je globální a nedělitelný, a proto jeho ochrana nemůže být omezena pouze na jednu skupinu států. Naopak, tento systém musí být otevřený i dalším zemím, které chtějí zajistit stabilitu svého prostředí a čelit hybridním hrozbám, které neznají hranice. Každý stát, každá mezinárodní instituce, každá organizace, která nese odpovědnost za bezpečnost, stabilitu a fungování společnosti, musí mít možnost se na tomto systému podílet a být jeho součástí.

V rámci tohoto centra se musí soustředit vládní struktury, bezpečnostní složky, zpravodajské služby, specialisté kybernetických sil, kybernetické kontrarozvědky, mezinárodní organizace, obranné aliance, technologické společnosti, výzkumné instituce, analytická centra, strategické útvary, ale také experti na ochranu demokratických hodnot, svobody projevu a lidských práv. Tento celek musí fungovat jako jeden koordinovaný organismus, který je schopen reagovat v reálném čase na jakoukoli hrozbu, a to nejen na úrovni jednotlivých států, ale na úrovni celé digitální civilizace.

Fyzická existence tohoto centra má zásadní význam nejen z hlediska operativního řízení, ale i z hlediska legitimity a důvěry. Vytváří totiž jasně definovanou globální autoritu, která není založena na mocenském diktátu, ale na společné odpovědnosti za ochranu demokracie, lidských práv a stability společnosti. V prostředí, kde dochází k systematickému narušování

důvěry prostřednictvím dezinformací, manipulace a informační války, je existence takového centra klíčová pro obnovu důvěry občanů v demokratický systém.

Zcela zásadním principem fungování Centrálního kybernetického štítu je oddělení, a zároveň úzké propojení dvou základních oblastí, které dnes nejsou dostatečně koordinovány. První oblastí je technická ochrana infrastruktury, tedy ochrana sítí, datových toků, komunikačních systémů, kritické infrastruktury, státních i soukromých digitálních systémů a celkové kybernetické bezpečnosti. Druhou oblastí je ochrana samotné podstaty demokracie, tedy ochrana důvěry, legitimity, svobody projevu, právního státu a odolnosti společnosti vůči dezinformacím, nenávisti, propagandě a manipulaci s veřejným míněním.

Tyto dvě oblasti nelze oddělovat, protože technická bezpečnost bez ochrany hodnotového systému nedokáže zabránit rozkladu společnosti, a naopak ochrana hodnot bez technologického zajištění není schopna čelit moderním hybridním hrozbám. Teprve jejich propojení v rámci jednoho integrovaného systému vytváří skutečně funkční obranný mechanismus, který je schopen chránit demokracii jako celek.

Centrální kybernetický štít zároveň představuje klíčový pilíř pro vybudování digitální demokratické infrastruktury, na níž je založena ONLINE DEMOKRACIE jako nový integrovaný politický, bezpečnostní, hodnotový a právní systém v kyberprostoru. Tento systém umožní propojit digitální a fyzický svět do jednoho funkčního celku, ve kterém budou demokratické procesy legitimní, transparentní a odolné vůči manipulaci. Bez existence tohoto centra by nebylo možné takový systém efektivně vybudovat, řídit ani chránit.

V širším kontextu tak Centrální kybernetický štít přispívá ke vzniku nové formy globálního uspořádání, které odpovídá realitě digitálního věku. Tento nový světový řád není založen na tradičních mocenských strukturách, ale na propojení technologií, hodnot a práva v rámci jednotného systému, který chrání nejen státy, ale především jednotlivce. Každý člověk na planetě má právo na ochranu svého života, zdraví, důstojnosti a svobody, a to nejen ve fyzickém, ale i v digitálním prostoru, který se stal nedílnou součástí lidské existence.

Bez vybudování Centrálního kybernetického štítu zůstává současný svět v zásadní nerovnováze. Politické, bezpečnostní a právní systémy existují pouze ve fyzickém světě, zatímco kyberprostor, ve kterém se odehrává většina komunikace a rozhodování, zůstává bez odpovídajícího systémového rámce. Tento stav je dlouhodobě neudržitelný a je hlavní příčinou vzniku a eskalace hybridních hrozeb, které se z digitálního prostředí přenášejí do reality v podobě konfliktů, násilí, destabilizace států a oslabení demokracie.

Proto je nezbytné jasně konstatovat, že Centrální kybernetický štít není volitelným projektem, ale absolutní nutností. Bez jeho existence nelze zajistit bezpečnost, stabilitu ani budoucnost moderní civilizace. Tento projekt představuje historickou příležitost vytvořit funkční legitimní a globálně koordinovaný systém ochrany demokracie, který odpovídá výzvám 21. století a který je schopen chránit nejen státy, ale i samotnou podstatu lidské společnosti.

Centrální kybernetický štít je navržen jako komplexní mezinárodní systém, který integruje politický, bezpečnostní, hodnotový a právní rámec digitální státnosti. Tento systém funguje jako globální mozek demokracie, jehož účelem je ochrana suverenity států, stabilita demokratického řádu, obrana imunitního systému demokracie a prevence hybridních hrozeb

v kyberprostoru. Aby byl systém efektivní, musí být každý stát a klíčová mezinárodní instituce plně zastoupena, přičemž každé zastoupení má jasně definovanou roli, odpovědnost a oblast působení.

Ministerstva obrany hrají zásadní roli v ochraně vojenských sítí a kybernetické infrastruktury státu. Jejich úkolem je nejen zabezpečit obranu proti kybernetickým útokům na armádní systémy a zařízení, ale také garantovat bezpečnou a spolehlivou komunikaci mezi jednotlivými složkami armády. V digitálním věku, kdy kybernetické útoky mohou ohrozit nejen vojenskou efektivitu, ale i samotnou suverenitu státu, se tato činnost stává existenčně důležitou. Ministerstva obrany proto nefungují izolovaně; úzce spolupracují s aliančními obrannými strukturami, zejména s členskými státy NATO a dalšími obrannými koalicemi, s cílem sdílet informace o aktuálních hrozbách, koordinovat obranné operace a zajistit jednotnou a efektivní reakci na krizové situace. Tato spolupráce umožňuje, aby každý stát mohl nejen účinně chránit své vojenské kapacity, ale zároveň zachovat kompatibilitu a propojení s obrannými systémy partnerů, což je kritické pro fungování kolektivní obrany. Klíčovou rolí ministerstev obrany je tedy udržení schopnosti státu reagovat na kybernetické konflikty, předcházet destabilizaci vojenských a politických struktur a zároveň přispívat k celkové bezpečnosti demokratického světa prostřednictvím integrovaného propojení s ostatními státy a jejich obrannými mechanismy. V kontextu Centrálního kybernetického štítu se role ministerstev obrany ještě významně rozšiřuje, protože tento štít poskytuje jednotný rámec, který umožňuje sdílení klíčových dat, koordinaci obranných opatření a kolektivní ochranu nejen vojenských sítí, ale i celé demokratické infrastruktury ve fyzickém i digitálním prostoru.

Ministerstva vnitra mají zásadní odpovědnost za ochranu veřejné bezpečnosti v kyberprostoru a za prevenci kybernetické kriminality, která ohrožuje každodenní život občanů i stabilitu společnosti. Jejich činnost zahrnuje koordinaci státní policie a dalších bezpečnostních složek při odhalování hrozeb, vyšetřování kybernetických útoků a zabezpečení kritických informačních toků. V digitálním věku, kdy se dezinformace, extremistické ideologie a radikalizace šíří neuvěřitelnou rychlostí prostřednictvím sociálních sítí a online platforem, musí ministerstva vnitra nejen reagovat na již probíhající útoky, ale aktivně monitorovat a předvídat nové hrozby. Součástí jejich působnosti je také sledování dezinformačních kampaní a kybernetických aktivit, které mohou destabilizovat veřejný diskurz, zvyšovat sociální napětí a ohrožovat důvěru občanů ve státní instituce a demokratické procesy. Ministerstva vnitra proto nejen odhalují a neutralizují digitální hrozby, ale zároveň podporují stabilizaci veřejného prostoru a demokratického diskurzu, čímž zajišťují ochranu občanů a integritu státních institucí.

V rámci Centrálního kybernetického štítu se role ministerstev vnitra výrazně posiluje, protože Štít umožňuje koordinované propojení s ostatními státními a mezinárodními institucemi, včetně obranných struktur NATO a dalších demokratických států. Tento systém poskytuje jednotný rámec pro monitorování, prevenci a reakci na hybridní hrozby a dezinformace a vytváří prostředí, ve kterém mohou ministerstva vnitra efektivně chránit veřejnou bezpečnost a stabilitu digitální i fyzické společnosti. Tímto způsobem se zajišťuje, že občané, instituce a demokratické procesy jsou chráněny nejen před fyzickými, ale i před kybernetickými hrozbami, což je zásadní pro dlouhodobou stabilitu a bezpečnost demokratického světa.

Ministerstva spravedlnosti hrají klíčovou roli při vytváření a dohledu nad digitálními zákony a právními rámci, které jsou nezbytné pro ochranu demokratické infrastruktury v

kyberprostoru. Jejich působnost zahrnuje nejen tvorbu legislativy upravující digitální státnost, ale také vypracování moderních právních norem, které zahrnují principy ONLINE DEMOKRACIE, včetně digitální ústavy a pravidel pro legitimní fungování politických, bezpečnostních a hodnotových procesů v digitálním prostoru.

Ministerstva spravedlnosti poskytují rovněž právní podporu v případě kybernetických útoků, šíření dezinformací, manipulace veřejného mínění či jiných forem hybridních hrozeb, které mohou ohrozit stabilitu státu a důvěru občanů v demokratické instituce. Jejich činnost zajišťuje, aby reakce státu na kybernetické hrozby byly nejen efektivní, ale i v souladu s principy právního státu, lidských práv a respektu k důstojnosti jednotlivce.

V kontextu Centrálního kybernetického štítu tvoří ministerstva spravedlnosti právní páteř celé struktury. Díky koordinaci s ostatními ministerstvy, obrannými institucemi, bezpečnostními složkami a mezinárodními organizacemi, včetně členských států NATO a dalších demokratických zemí, umožňují jednotnou implementaci právních opatření na národní i mezinárodní úrovni. Tím je zajištěno, že ochrana demokracie v kyberprostoru není pouze fragmentární, lokální nebo selektivní, ale funguje jako komplexní, koordinovaný a legitimní systém, který chrání více než pět miliard uživatelů internetu a sociálních sítí a zároveň podporuje dlouhodobou stabilitu, bezpečnost a důvěru v demokratické procesy.

Ministerstva financí hrají zásadní roli při ochraně digitální ekonomiky a zajišťování stability finančních systémů státu. Jejich činnost zahrnuje ochranu digitálních platebních systémů, zabezpečení finančních transakcí a monitoring bankovních sítí, které jsou stále více vystaveny sofistikovaným kybernetickým útokům a hybridním hrozbám. V digitálním věku, kdy se finanční transakce provádějí v reálném čase prostřednictvím online platforem a globálních sítí, představuje jejich činnost základní pilíř ochrany národní i mezinárodní ekonomické stability.

Ministerstva financí zároveň koordinují své aktivity s mezinárodními finančními institucemi, centrálními bankami a dalšími státními i mezinárodními subjekty, aby zajistila jednotnou obranu proti kybernetickým podvodům, finančním manipulacím a pokusům o destabilizaci ekonomického systému. Taková spolupráce umožňuje rychlou výměnu informací o hrozbách, koordinaci preventivních opatření a efektivní reakci na krizové situace.

V rámci Centrálního kybernetického štítu ministerstva financí zajišťují, že ekonomická a finanční složka digitální demokratické infrastruktury je propojena s ostatními pilíři Štítu. Tento integrovaný systém umožňuje nejen ochranu finančních toků, ale zároveň podporuje stabilitu digitální státnosti a celkové bezpečnosti státu. Centrální kybernetický štít tímto způsobem vytváří koordinovanou a komplexní obranu, která chrání finanční systém demokratických států – včetně členských států EU, dalších demokratických zemí a členských států NATO – a zajišťuje, že ekonomická stabilita není ohrožena kybernetickými útoky, manipulacemi ani dezinformačními kampaněmi.

Klíčovou rolí ministerstev financí je tak udržení finanční stability států a ochrana ekonomického systému, která je dnes nedílně spojena s ochranou demokracie a legitimních rozhodovacích procesů ve fyzickém i digitálním světě. Centrální kybernetický štít zabezpečuje, že tato stabilita je dlouhodobá, koordinovaná a odolná vůči komplexním hybridním hrozbám, čímž umožňuje demokratickým státům efektivně fungovat i v prostředí globální digitální civilizace.

Bezpečnostní složky státu představují klíčový prvek ochrany digitální a fyzické integrity demokratického systému a jsou nedílnou součástí Centrálního kybernetického štítu. Policie zajišťuje bezpečnost veřejných sítí a ochranu občanů před kybernetickými hrozbami, odhaluje online kriminalitu, monitoruje dezinformační kampaně a radikalizaci, a tím stabilizuje veřejný diskurz. Národní kontrarozvědka se specializuje na prevenci infiltrace cizích aktérů, hybridních hrozeb a sofistikovaných kybernetických operací, které by mohly ohrozit národní bezpečnost i důvěru veřejnosti v demokratické instituce. Zpravodajské služby poskytují strategický přehled o mezinárodních kybernetických aktivitách, detekují rizikové hrozby a zajišťují včasné varování pro státní orgány, což umožňuje koordinovanou obranu proti komplexním útokům. Kybernetické jednotky disponují kapacitami pro okamžitou reakci na kybernetické útoky, provádějí preventivní opatření a aktivní obranu, čímž brání šíření destabilizujících procesů do fyzického světa.

Každá z těchto složek poskytuje specializovanou expertizu a konkrétní nástroje pro oblast, kterou pokrývá. Pro efektivní ochranu demokracie a stabilitu státu však nestačí působení jednotlivých složek izolovaně – proto jsou všechny bezpečnostní složky plně propojeny prostřednictvím Centrálního kybernetického štítu. Tento integrovaný systém umožňuje koordinovanou akci, okamžitou výměnu informací, jednotnou strategii obrany a efektivní reakci na hybridní hrozby, čímž se vytváří skutečný mechanismus kolektivní ochrany demokratické infrastruktury nejen pro členské státy EU a NATO, ale i pro další demokratické země a mezinárodní instituce.

Díky této koordinaci Centrální kybernetický štít zajišťuje, že bezpečnostní složky nejsou pouze nástrojem ochrany fyzického prostoru, ale že společně tvoří robustní systém obrany, který propojuje kybernetický a reálný svět, stabilizuje rozhodovací procesy, chrání občany a demokratickou infrastrukturu a zároveň zajišťuje dlouhodobou odolnost vůči sofistikovaným a celosvětovým kybernetickým hrozbám.

Legislativní a expertní týmy digitálního práva představují základní pilíř právní ochrany demokracie v kyberprostoru a fungují jako klíčový nástroj Centrálního kybernetického štítu. Tyto týmy vyvíjejí a aktualizují normy pro digitální zákony, regulace a digitální ústavy, které tvoří právní rámec pro fungování ONLINE DEMOKRACIE. Vytvářejí právní struktury, jež umožňují státu, institucím a občanům bezpečně operovat v digitálním prostoru, chrání jejich práva, svobody a demokratické principy a současně poskytují nástroje pro účinnou obranu proti dezinformacím, manipulacím a hybridním útokům.

Týmy se rovněž podílejí na tvorbě a implementaci mezinárodních dohod o digitální státnosti, koordinují spolupráci s ostatními demokratickými zeměmi a mezinárodními organizacemi a zajišťují, že právní rámce respektují univerzální hodnoty lidských práv, svobody projevu a principy právního státu. Tento právní základ je nezbytný pro fungování Centrálního kybernetického štítu, protože samotná ochrana demokracie nemůže existovat pouze na základě technických opatření, regulací nebo izolovaných nástrojů – vyžaduje komplexní, právně zakotvený systém, který propojuje digitální a fyzický svět.

Klíčovou rolí těchto týmů je zajistit, aby veškeré procesy obrany a ochrany demokratické infrastruktury měly pevný právní rámec a aby kolektivní ochrana demokracie byla nejen technicky, ale i právně zajištěna. Bez existence tohoto právního pilíře by byla kybernetická ochrana nedostatečná, protože demokratické procesy, důvěra občanů a legitimita

rozhodování států – včetně členských států EU, NATO a dalších zemí – by zůstaly v kyberprostoru zranitelné. Díky těmto týmům je Centrální kybernetický štít schopen poskytovat dlouhodobou, koordinovanou a právně zakotvenou ochranu, která je absolutně nezbytná pro přežití demokracie ve fyzickém i digitálním světě.

Centrální kybernetický štít není pouze národní ani regionální iniciativou; jedná se o komplexní mezinárodní platformu, kde jsou zastoupeny klíčové nadnárodní organizace, alianční a bezpečnostní struktury, které dohromady zajišťují koordinovanou ochranu demokracie v kyberprostoru. V této platformě je Evropská unie klíčovým partnerem, který koordinuje digitální legislativu, standardy kybernetické bezpečnosti a ochrany demokratických procesů mezi členskými státy. EU tímto způsobem zajišťuje jednotný rámec a harmonizaci pravidel, což je zásadní pro efektivní ochranu demokratické infrastruktury ve všech členských státech.

Aliance NATO se zapojuje prostřednictvím vojenských a kybernetických strategií, přičemž poskytuje nezbytnou podporu pro obranu členských států proti hybridním a kybernetickým hrozbám. V tomto kontextu je naprosto nezbytné rozšířit stávající článek 5 o digitální článek 5. Zároveň Centrální kybernetický štít vyplňuje zásadní mezeru, neboť zatímco členské státy NATO disponují článkem 5 pro kolektivní obranu ve fyzickém světě, podobná koordinovaná kolektivní obrana v kyberprostoru doposud neexistuje. Tato platforma tak umožňuje implementaci digitální kolektivní obrany, která zahrnuje nejen členské státy EU a NATO, ale i další demokratické země a klíčové mezinárodní subjekty, čímž se zajišťuje ochrana demokracie a stabilita států ve virtuálním prostoru.

Organizace spojených národů poskytuje globální rámec pro dodržování lidských práv, svobody projevu a mezinárodního práva, čímž posiluje legitimitu a právní integritu digitálních demokratických procesů. Mezinárodní měnový fond a Světová banka se soustředí na ochranu digitálních finančních systémů, koordinaci ekonomické odolnosti a prevenci destabilizace států prostřednictvím kybernetických hrozeb, což umožňuje, aby ekonomická infrastruktura zůstala bezpečná a stabilní i v digitálním prostoru. Interpol a Europol pak poskytují mezinárodní podporu při odhalování kyberkriminality, monitorování dezinformačních sítí a koordinaci bezpečnostních operací napříč hranicemi, čímž významně přispívají k prevenci eskalace hybridních hrozeb do fyzického světa.

Další mezinárodní organizace, včetně regionálních obranných aliancí, regulačních a standardizačních orgánů, institucí pro lidská práva a expertních skupin zaměřených na hybridní hrozby, jsou nedílnou součástí tohoto systému. Každá organizace má jasně definovanou roli a odpovědnost, což zajišťuje integritu platformy a koordinaci na globální úrovni. Centrální kybernetický štít tímto způsobem umožňuje propojení politických, bezpečnostních, hodnotových a právních rámců napříč státy a organizacemi a vytváří první skutečně kolektivní obranu demokracie v kyberprostoru, která je existenčně nezbytná pro stabilitu digitální civilizace a ochranu demokracie ve fyzickém světě.

Centrální kybernetický štít integruje do své struktury klíčové technologické a výzkumné instituce, které poskytují odborné kapacity a nástroje nezbytné pro efektivní ochranu digitální demokratické infrastruktury. Technologické společnosti mají zásadní úlohu při vývoji a provozu nástrojů pro monitorování sítí, analýzu dat, detekci kybernetických hrozeb a zabezpečení cloudových systémů a digitálních identit. Jejich odborné schopnosti umožňují

predikovat útoky, identifikovat bezpečnostní slabiny a rychle reagovat na krizové situace, čímž se zajišťuje kontinuita a bezpečnost digitální státnosti.

Výzkumné a akademické instituce se soustředí na metodologii prediktivního modelování hrozeb, scénáře krizového řízení a nástroje pro stabilizaci veřejného diskurzu. Jejich práce je kriticky důležitá, protože umožňuje anticipovat hybridní útoky a dezinformační kampaně, které mohou destabilizovat nejen kyberprostor, ale následně i fyzický svět. Tyto instituce poskytují analytický základ, který umožňuje státním orgánům, bezpečnostním složkám a mezinárodním organizacím koordinovaně čelit komplexním hrozbám.

Analytická centra a experti na kybernetickou bezpečnost zajišťují jednotné standardy obrany, monitorují kybernetické útoky a poskytují rychlou reakci na incidenty. Jejich činnost propojuje technologickou expertizu s operativními strukturami státní i mezinárodní bezpečnosti, což umožňuje efektivní sdílení informací, koordinaci obranných operací a okamžité řešení krizových situací.

Psychologičtí a sociologičtí experti doplňují tuto strukturu analýzou vlivu dezinformací na veřejné mínění, vyhodnocováním rizik radikalizace a podporou tzv. imunitního systému demokracie. Jejich role je nezbytná pro pochopení sociálních a psychologických dopadů hybridních hrozeb, které se šíří prostřednictvím sociálních sítí a digitálních platforem, a pro vytváření strategií, jež minimalizují destabilizaci společnosti a podkopávání důvěry v demokratické procesy.

Existence mezinárodního lékařského konzilia přímo v operačním centru Centrálního kybernetického štítu je nezbytná, protože současné hrozby v kyberprostoru již neútočí pouze na technickou infrastrukturu, ale cíleně zasahují do biologické a psychické integrity obyvatelstva. Přítomnost špičkových lékařských kapacit v místě velení umožní okamžitou identifikaci a neutralizaci biokybernetických útoků, které mohou skrze digitální sítě ochromit zdravotnické systémy nebo přímo ohrozit životy pacientů v kyberprostoru. Toto konzilium zároveň funguje jako diagnostický a obranný orgán proti sofistikovaným psychologickým operacím, které mají za cíl vyvolat masový stres a mentální rozklad společnosti. Integrace medicínské expertízy do digitální obrany státu tak zajišťuje, že ochrana lidského zdraví a zachování psychické stability populace jsou prioritní součástí kolektivní bezpečnosti v rámci celého mezinárodního řádu.

Společně tyto technologické a výzkumné subjekty tvoří nedílnou součást Centrálního kybernetického štítu, který tím získává multidisciplinární kapacity pro prevenci, detekci, reakci a mitigaci hrozeb v kyberprostoru. Tento integrovaný systém je nezbytný pro zajištění kolektivní obrany demokracie nejen členských států NATO, ale také členských států Evropské unie a dalších zemí. Bez koordinace a spolupráce těchto technologických a vědeckých institucí by nebylo možné efektivně chránit demokratickou infrastrukturu a udržovat důvěru občanů v bezpečné a stabilní fungování státních i mezinárodních systémů.

Centrální kybernetický štít tak prostřednictvím této propojené struktury vytváří jednotný, funkční a legitimní rámec pro ochranu demokracie, který nahrazuje fragmentární, nekoordinované a krátkozraké přístupy jednotlivých států či organizací. Integrace technologických a výzkumných institucí je proto klíčová pro zabezpečení kontinuity

demokratických procesů v kyberprostoru a pro ochranu demokratické civilizace, jejíž stabilita je existenčně závislá na spolehlivém fungování ONLINE DEMOKRACIE.

Centrální kybernetický štít integruje specializované týmy zaměřené na tvorbu digitální legislativy a hodnotového systému, které zajišťují právní a hodnotovou stabilitu ONLINE DEMOKRACIE. Týmy pro digitální zákony vytvářejí komplexní právní rámec, jenž umožňuje ochranu kybernetické bezpečnosti, občanských práv a suverenity států. Tento rámec nahrazuje fragmentární a nekoordinované právní úpravy, které jsou dnes v jednotlivých státech často nesourodé a neúčinné. Díky centralizované struktuře Centrálního kybernetického štítu jsou všechny státy, instituce a mezinárodní organizace schopny čerpat z jednotného a funkčního právního systému, který zajišťuje legitimitu, koordinaci a efektivní obranu proti hybridním hrozbám.

Týmy pro digitální ústavu definují základní principy digitální státnosti a fungování demokratických procesů v kyberprostoru. Jsou odpovědné za kodifikaci práv a povinností všech účastníků digitálního prostředí, zajištění transparentnosti rozhodovacích procesů a ochranu integrity demokratických struktur. Digitální ústava vytváří stabilní základ pro kolektivní obranu demokracie v kyberprostoru, která je stejně kritická jako tradiční vojenská obrana. Bez takto definovaných principů by členské státy NATO, členské státy Evropské unie, stejně jako další země, nemohly účinně koordinovat ochranu demokratických procesů ani reagovat na sofistikované kybernetické útoky.

Experti na ochranu demokratických hodnot se zaměřují na udržování a posilování tzv. imunitního systému demokracie. Jejich úkolem je monitorovat veřejný diskurz, analyzovat vliv dezinformačních kampaní a předcházet destabilizačním útokům, které by mohly narušit důvěru občanů v demokratické procesy. Tito odborníci vytvářejí metodiky, které propojují právní, bezpečnostní a hodnotový rámec, a tím umožňují efektivní prevenci proti destabilizaci demokracie. Jejich práce je nedílnou součástí deseti pilířů Centrálního kybernetického štítu a přispívá k dlouhodobé stabilitě a soudržnosti digitální i fyzické společnosti.

Centrální kybernetický štít tak prostřednictvím těchto týmů poskytuje nedílnou podporu kolektivní obraně demokracie v kyberprostoru. Nejedná se pouze o ochranu jednotlivých států či aliancí, ale o globální zajištění integrity demokratických procesů, které jsou existenčně závislé na stabilním a koordinovaném právním a hodnotovém systému. Tato struktura nahrazuje neefektivní směrnice, zákazy a lokální regulace, které samy o sobě nemohou zajistit skutečnou bezpečnost a stabilitu demokratických států.

Díky integraci týmů pro digitální zákony, digitální ústavu a expertů na ochranu demokratických hodnot vzniká jednotný právní a hodnotový rámec, který podporuje koordinovanou obranu proti hybridním hrozbám, dezinformacím a kybernetickým útokům. Tento rámec umožňuje státům a mezinárodním organizacím efektivně spolupracovat, sdílet informace, vytvářet preventivní strategie a zajistit stabilní, legitimní a důvěryhodný digitální prostor.

Tento robustní interdisciplinární komplex představuje bezprecedentní integrační uzel, v němž jsou přímo zastoupena všechna relevantní ministerstva, odborné týmy a specialisté napříč celým spektrem státní správy. Jeho unikátnost spočívá v globálním dosahu: v rámci Centrálního kybernetického štítu jsou přítomny nejen členské státy EU a NATO, ale i partneři

z Afriky, Asie a dalších regionů, kteří sdílejí společný zájem na ochraně digitální státnosti, suverenity a legitimity státu v kyberprostoru.

Součástí tohoto aparátu je i mezinárodní lékařské a odborné konzilium, které vedle technologických expertů zajišťuje ochranu biologické a psychické integrity obyvatelstva. Tato široká mezinárodní kooperace umožňuje v reálném čase sdílet data a obranné protokoly, čímž vzniká globální digitální aliance.

Celkově tato struktura Centrálního kybernetického štítu představuje pilíř, na němž stojí ochrana demokracie v kyberprostoru a na kterém je existenčně závislá budoucnost demokracie ve fyzickém světě. Bez něj by nebylo možné zajistit koordinovanou a efektivní kolektivní obranu demokratických států ani stabilitu veřejného diskurzu, což z něj činí nezbytnou součást deseti pilířů Centrálního kybernetického štítu.

Oddíl 11

Budova gigacentra Bohemia: Central Cyber Shield

Centrální kybernetický štít, umístěný v impozantní budově označované jako „Bohemia: Central Cyber Shield“, bude představovat skutečně jedinečný projekt, jehož cílem bude vybudovat inovativní, komplexní a integrovaný politický, bezpečnostní, hodnotový a právní systém – ONLINE DEMOKRACII – v kyberprostoru. Tato budova nebude pouze administrativním sídlem, ale stane se monumentálním, architektonicky i funkčně výjimečným centrem globálního významu, které nebude mít ve světě obdoby. Půjde o strukturu jedinečného formátu, navrženou jako fyzický i symbolický pilíř ochrany demokratických hodnot v digitálním věku, kde se budou každodenně setkávat tisíce odborníků, analytiků, bezpečnostních specialistů, právníků, technologických lídrů a zástupců států z celého světa.

V rámci Bohemia: Central Cyber Shield budou zastoupeny všechny klíčové složky státu i nadnárodních struktur – ministerstva obrany, vnitra, spravedlnosti a financí, bezpečnostní a zpravodajské služby, legislativní a expertní týmy digitálního práva, technologické a výzkumné instituce, mezinárodní organizace i alianční partneři. Tento mimořádně komplexní ekosystém bude propojen prostřednictvím jednotné infrastruktury sdílení dat, rozhodovacích procesů a operační koordinace, což umožní vznik plně integrovaného mechanismu kolektivní obrany demokracie v kyberprostoru.

Samotná budova Bohemia: Central Cyber Shield bude koncipována jako vysoce zabezpečený, autonomní a logisticky soběstačný celek. Její statut bude odpovídat neutrálnímu mezinárodnímu území, spravovanému na základě globální dohody demokratických států. Bezpečnost tohoto prostoru budou zajišťovat specializované jednotky složené ze zástupců bezpečnostních struktur z celého světa, čímž bude garantována maximální míra nezávislosti, důvěryhodnosti a ochrany před jakýmikoli vnějšími vlivy.

Z hlediska bezpečnostní architektury bude Bohemia: Central Cyber Shield představovat nejpokročilejší úroveň ochrany, jaká kdy bude vytvořena. Objekt bude vybaven vícevrstvými bezpečnostními systémy, zahrnujícími fyzickou ochranu, kybernetickou obranu, biometrické přístupové mechanismy, nepřetržitý dohled a prediktivní analytické nástroje. Veškeré procesy uvnitř budovy budou podléhat nepřetržité 24hodinové kontrole a vyhodnocování v reálném čase, a to s využitím nejmodernějších technologií umělé inteligence a datové analýzy. Tento systém umožní okamžitou identifikaci a neutralizaci hrozeb, které by mohly ohrozit stabilitu demokratických procesů v globálním měřítku.

Zcela zásadním prvkem bude také rozsáhlé logistické a infrastrukturní zázemí. Vzhledem k tomu, že v Bohemia: Central Cyber Shield budou působit tisíce odborníků z různých zemí, bude součástí komplexu i plně integrovaný systém bydlení, zdravotní péče, administrativních služeb, vzdělávacích a výzkumných kapacit a dalších podpůrných struktur. Tyto prvky zajistí nejen vysokou efektivitu práce, ale i dlouhodobou udržitelnost celého systému. Zaměstnanci a spolupracovníci budou mít k dispozici prostředí, které bude odpovídat nejvyšším

standardům bezpečnosti, komfortu a profesionální podpory, což bude nezbytné pro zvládání extrémně náročných úkolů spojených s ochranou více než pěti miliard uživatelů digitálního prostoru.

Bohemia: Central Cyber Shield současně bude představovat historicky první globální centrum, které bude systematicky chránit digitální státnost, suverenitu a legitimitu jednotlivých zemí v kyberprostoru. V prostředí, kde se stále více politických, společenských i ekonomických procesů bude odehrávat online, se ochrana demokracie v digitální dimenzi stane přímo určující pro její přežití i ve fyzickém světě. Právě v tomto kontextu bude v digitálním věku naprosto nezbytné, aby takovéto centrum existovalo, protože bez něj nebude možné zajistit stabilitu a bezpečnost demokratických systémů v globálním měřítku.

Klíčovou lekcí z minulosti bude, že izolované regulace, směrnice či restriktivní opatření nikdy nemohly zajistit stabilní a dlouhodobě funkční ochranu demokratických hodnot. Fragmentace přístupů mezi jednotlivými státy vedla k informačnímu chaosu, oslabení důvěry veřejnosti a nárůstu hybridních hrozeb. Bohemia: Central Cyber Shield tento zásadní nedostatek překoná tím, že vytvoří jednotný, hodnotově ukotvený a právně konzistentní rámec, v němž budou všechny aktivity koordinovány na globální úrovni.

Zásadní význam tohoto centra bude spočívat také v tom, že poprvé v historii vznikne skutečný ekvivalent kolektivní obrany v kyberprostoru. Zatímco tradiční bezpečnostní aliance poskytují ochranu ve fyzickém světě, Bohemia: Central Cyber Shield přinese analogický princip do digitální dimenze. Umožní okamžité sdílení informací, koordinovanou reakci na hrozby a společné strategické plánování, čímž zásadně zvýší odolnost demokratických systémů vůči sofistikovaným útokům, dezinformacím a manipulacím veřejného mínění. V digitální éře, která bude definovat fungování společnosti po staletí, se svět bez tohoto centra jednoduše neobejde.

Celý tento komplex bude fungovat jako dynamický, neustále se vyvíjející organismus, který propojí technologii, právo, bezpečnost a hodnotový rámec demokracie do jednoho celku. Každé rozhodnutí, každá operace i každá strategická iniciativa budou vycházet z jednotného systému, který zajistí transparentnost, odpovědnost a dlouhodobou stabilitu. Tento přístup umožní nejen reagovat na aktuální hrozby, ale především jim systematicky předcházet.

Bohemia: Central Cyber Shield tak bude představovat nejen technologický vrchol své doby, ale především nový standard ochrany demokratického světa. Stane se symbolem globální spolupráce, důvěry a společné odpovědnosti za budoucnost demokracie. V digitálním věku, kdy bude kyberprostor hlavním bojištěm o podobu veřejného diskurzu, legitimitu institucí i stabilitu států, bude existence tohoto komplexu nezastupitelná a jeho vybudování bude nutností minimálně na další staletí, nejméně na horizont pěti set let.

Vznik tohoto centra bude důkazem, že demokratické státy jsou schopny překonat fragmentaci, sjednotit své kapacity a vytvořit systém, který odpoví výzvám 21. století i daleké budoucnosti. Bohemia: Central Cyber Shield nebude pouze budovou – stane se symbolem odhodlání chránit demokracii v její nejzranitelnější, ale zároveň nejdůležitější dimenzi. Bude to prostor, kde se bude každodenně rozhodovat o stabilitě světa, o důvěře občanů a o budoucnosti svobody jako takové.

Oddíl 12

Globální bezpečnostní centrum pro ochranu demokracie

Aktuální i budoucí společenský vývoj je charakterizován plnohodnotnou koexistencí fyzické a digitální sféry, ve kterých občané současně žijí, komunikují a rozhodují. Tato dualita zásadním způsobem ovlivňuje stabilitu demokratických systémů, přičemž právě kyberprostor je dominantním zdrojem hybridních hrozeb, které se následně přenášejí do reálného světa. V reakci na tuto systémovou nerovnováhu je vznik Globálního bezpečnostního centra pro ochranu demokracie klíčovým nástrojem pro zajištění komplexní bezpečnosti v obou těchto dimenzích.

Globální bezpečnostní centrum pro ochranu demokracie představuje nejvyšší autoritu v oblasti ochrany demokratických principů na světové úrovni. Nebude nadřazeným orgánem státům ve smyslu přímého výkonu moci, ale bude plnit roli vrcholného referenčního a rozhodovacího rámce, ze kterého budou jednotlivé státy, vlády i občané čerpat závazné principy, standardy a strategické směřování.

Rozhodnutí přijatá na úrovni Globálního bezpečnostního centra pro ochranu demokracie budou následně implementována prostřednictvím národních legislativ, bezpečnostních opatření, ekonomických nástrojů a institucionálních mechanismů, čímž bude zajištěna jejich jednotná aplikace v praxi. V důsledku tohoto systémového nastavení bude nezbytné, aby veškerá politická činnost na národní i mezinárodní úrovni byla od okamžiku vzniku tohoto centra koncipována a realizována v přímé návaznosti na jeho strategický rámec.

Politické rozhodování bude nově probíhat v prostředí, kde každý jednotlivý krok – ať již v oblasti bezpečnostní, ekonomické, sociální, zdravotní, právní či environmentální politiky – bude neoddělitelně spojen s ochranou demokratických procesů. Z toho důvodu budou muset političtí představitelé zohledňovat principy, doporučení a směřování definované Globálním bezpečnostním centrem pro ochranu demokracie a budou své kroky s tímto rámcem aktivně slaďovat. Tento přístup nebude představovat omezení jejich činnosti, ale naopak její zásadní zefektivnění, zjednodušení a urychlení, neboť poskytne jednotný, odborně podložený a dlouhodobě stabilní základ pro rozhodování.

Současně bude tento model vyžadovat průběžnou koordinaci a konzultaci mezi národními politickými strukturami a Globálním bezpečnostním centrem, aby byla zajištěna plná kompatibilita jednotlivých opatření a jejich soulad s globálním rámcem ochrany demokracie. Tato koordinace se stane klíčovým prvkem řízení, který umožní eliminovat nesoulad, zvýšit efektivitu veřejných politik a zajistit, že ochrana demokracie bude integrována do všech rozhodovacích procesů bez ohledu na jejich sektorové zaměření.

Zajištění tohoto principu bude představovat nejvyšší bezpečnostní prioritu současného i budoucího vývoje. V podmínkách, kdy demokratické systémy čelí komplexním hrozbám ve fyzickém i kybernetickém prostoru, neexistuje jiná alternativní cesta k jejich efektivní ochraně než přes systematické propojení národního rozhodování s globálním rámcem řízení. Integrace těchto úrovní se tak stane nezbytným předpokladem pro stabilitu, odolnost a dlouhodobou udržitelnost demokracie.

Globální bezpečnostní centrum pro ochranu demokracie nesmí svou činnost zakládat na restriktivních nástrojích, jako jsou plošné zákazy, direktivní příkazy, regulace digitálního prostoru či omezující zásahy do svobodného fungování demokratických procesů. Takový přístup by byl v přímém rozporu s jeho základním posláním a principy. Ochrana demokracie nesmí být realizována prostřednictvím omezování svobody, nýbrž budováním integrovaného politického, bezpečnostního, hodnotového a právního systému. Ten je založen na principu ONLINE DEMOKRACIE, která otevírá nový prostor pro transparentní, otevřené a odpovědné fungování demokratických procesů v podmínkách digitálního věku.

Klíčovou roli v tomto procesu bude sehrávat odborná a organizační struktura Globálního bezpečnostního centra pro ochranu demokracie, která bude zajišťovat přípravu strategických agend, koncepčních materiálů a rozhodovacích podkladů. Tento specializovaný aparát bude plnit zásadní funkci nejen ve vztahu k samotnému globálnímu centru, ale současně i vůči Centrálnímu kybernetickému štítu demokracie, pro který bude vytvářet nezbytné analytické, koncepční a organizační zázemí. Pro pracovníky této struktury bude muset být zajištěn režim nejvyšší bezpečnostní ochrany a funkční imunity nezbytné pro výkon jejich činnosti, přičemž jejich nasazení bude probíhat v nepřetržitém pohotovostním režimu odpovídajícím nejvyšší bezpečnostní prioritě. Tomu musí odpovídat i vytvoření maximálně efektivního institucionálního, personálního a technologického zázemí, které jim umožní rychlé, flexibilní a odborně podložené jednání v reálném čase.

Tato personální a odborná struktura ponese mimořádně vysokou míru odpovědnosti, neboť její činnost bude přímo ovlivňovat kvalitu rozhodování na globální úrovni i efektivitu ochrany demokracie jako celku. Její postavení bude mít zásadní význam pro fungování celého systému, jelikož bude zajišťovat propojení mezi strategickým řízením, odborným zázemím a praktickou implementací jednotlivých opatření v globálním i národním kontextu.

Zásadním principem fungování tohoto centra bude jeho přímá odpovědnost vůči světové veřejnosti. Globální bezpečnostní centrum bude systematicky, transparentně a v plném rozsahu informovat občany o svých rozhodnutích, činnostech i dlouhodobých strategiích. Světová veřejnost má nezpochybnitelné právo na přístup k těmto informacím, neboť právě občané jsou nositeli demokratické legitimity. Tento princip zajistí nejen kontrolu nad činností centra, ale také posílí důvěru v demokratické procesy a aktivní zapojení občanů do jejich ochrany.

Součástí Globálního bezpečnostního centra pro ochranu demokracie bude Centrální kybernetický štít demokracie, který bude tvořit jeho klíčový pilíř v oblasti digitálního prostoru. Obě tyto pilířové instituce budou sídlit v jedné společné, komplexní a vysoce zabezpečené institucionální budově, která bude představovat globální centrum řízení ochrany demokracie. Tato fyzická i funkční integrace zajistí maximální efektivitu, koordinaci a kontinuitu mezi strategickým rozhodováním a odborným zázemím.

Centrální kybernetický štít demokracie bude vystupovat jako odborný, poradní a návrhový pilíř, který bude Globálnímu bezpečnostnímu centru systematicky předkládat podněty, návrhy, doporučení a strategické materiály nezbytné pro rozhodování o ochraně a rozvoji demokracie. Globální bezpečnostní centrum bude na základě těchto výstupů přijímat klíčová rozhodnutí, definovat pravidla a určovat dlouhodobé směřování. Současně bude zajišťovat tomuto štítu veškeré potřebné zázemí napříč politickou, bezpečnostní, legislativní, ekonomickou i hodnotovou rovinou, čímž vznikne jednotný a provázaný systém řízení.

V jednotlivých státech postupně vzniknou Národní bezpečnostní centra pro ochranu demokracie, do kterých budou systematicky integrovány a převedeny relevantní kompetence, agendy, institucionální kapacity, odborné útvary i personální zajištění dosavadních orgánů a úřadů působících v oblasti ochrany demokracie, bezpečnosti a souvisejících politik. Tento proces centralizace a sjednocení řízení povede k zásadnímu zefektivnění činnosti státu, odstranění duplicit, zrychlení rozhodovacích procesů a zvýšení celkové bezpečnostní odolnosti.

Díky tomuto modelu dojde nejen ke zvýšení efektivity ochrany demokratických procesů a bezpečnosti občanů, ale také k významným ekonomickým úsporám. Členské státy, včetně zemí Evropské unie a NATO, budou schopny každoročně ušetřit značné finanční prostředky ve státních rozpočtech, a to v řádech miliard, při současném zvýšení kvality řízení a ochrany demokracie.

Globální bezpečnostní centrum pro ochranu demokracie bude současně organizovat pravidelné globální demokratické summity, na kterých budou představitelé států vyhodnocovat dosažený pokrok, identifikovat slabá místa a přijímat další strategická rozhodnutí. Tím bude zajištěna kontinuální adaptace systému na nové výzvy a dynamický vývoj bezpečnostního prostředí.

Celý tento koncept vytvoří jednotný, dlouhodobě udržitelný a systémově provázaný rámec, který bude schopen reagovat na současné i budoucí hrozby. Globální bezpečnostní centrum pro ochranu demokracie se tak stane klíčovým pilířem ochrany demokratických hodnot a jejich stabilního rozvoje, přičemž zajistí, že demokracie bude účinně chráněna jak ve fyzickém světě, tak v kyberprostoru.[29, 30, 31, 32, 33]

10 ALIANČNÍCH BEZPEČNOSTNÍCH PILÍŘŮ CENTRÁLNÍHO KYBERNETICKÉHO ŠTÍTU

Centrální kybernetický štít je budován na 10 aliančních bezpečnostních pilířích, které tvoří integrovaný systém a komplexní bezpečnostně-řídicí architekturu kybernetického prostoru, doplňující a harmonizující existující digitální regulační a bezpečnostní rámce včetně dosud fragmentovaných národních přístupů. Tento systém představuje klíčový koordinační a ochranný rámec kybernetické bezpečnosti, na jehož funkční integritě zásadně závisí strategická stabilita, důvěra a obranyschopnost členských států Evropské unie a Severoatlantická aliance. V širším kontextu má jeho stabilita zásadní význam pro bezpečnostní rovnováhu v digitálním i fyzickém prostoru, na nichž je postavena odolnost současného mezinárodního bezpečnostního prostředí.

---

1. **ONLINE DEMOKRACIE**
   První politický systém fungující v kyberprostoru, umožňující aktivní zapojení občanů do demokratických procesů v digitálním prostředí.

2. **Digitální demokratická infrastruktura**
   Jednotná platforma zajišťující kolektivní obranu a stabilní fungování demokratických institucí v kyberprostoru.

3. **Sociální síť Politinn**
   První evropská platforma nové generace zaměřená na ochranu a rozvoj demokracie v kyberprostoru.

4. **Kyberstrategie 2026 – Boj proti dezinfokracii**
   Strategický rámec pro potlačení „dezinfokracie“, jedné z nejničivějších hybridních hrozeb 21. století, která ohrožuje demokratické procesy a důvěru veřejnosti.

5. **Centrální kybernetický štít pro NATO**
   Rozšíření principu kolektivní obrany o dimenzi kyberprostoru prostřednictvím implementace digitálního článku 5.

6. **Digitální světová organizace (DWO)**
   Mezinárodní instituce zajišťující ochranu a rozvoj digitální civilizace, kterou tvoří více než pět miliard uživatelů internetu a sociálních sítí, s cílem ochrany fyzického světa.

7. **Kyberstrategie 2026 – Boj proti „digitální rakovině“**
   Iniciativa zaměřená na ochranu fyzického a duševního zdraví občanů členských

států EU a NATO před negativními dopady digitálního prostředí.

8. **Kyberstrategie 2026 – Kybernetické přezbrojení členských států EU a NATO**

Posílení technologických, bezpečnostních a obranných kapacit členských států EU a NATO. Cílem je účinná ochrana a zajištění integrity digitální státnosti, suverenity, národní identity a legitimity států v online prostředí. Součástí je také ochrana kritické infrastruktury a klíčových státních institucí před cílenými a koordinovanými hybridními útoky.

9. **Kyberstrategie 2026 – Boj proti sociálnímu terorismu**

Opatření zaměřená na prevenci radikalizace, nenávisti a násilí šířených prostřednictvím sociálních sítí.

10. **Budování bezpečnostního, právního a zejména hodnotového systému v kyberprostoru:**


Klíčovou součástí ochrany demokratických hodnot je systematické budování hodnotového rámce založeného na principech demokracie, nejen ve fyzickém světě, ale zejména v digitálním prostoru, kde probíhá světová hybridní válka 21. století. Důvěra v demokratické principy, instituce a spojenecké vztahy představuje jeden ze základních pilířů bezpečnostní, sociální, ekonomické, environmentální a právní stability demokratických států. Z tohoto důvodu vzniká mezinárodní iniciativa „Demokratická osobnost roku“, jejímž posláním bude budovat a rozvíjet hodnotový systém chránící a upevňující důvěru nejen mezi spojenci, ale i uvnitř demokratických společností, a tím přispívat ke zvyšování obranyschopnosti aliančních struktur, posilování informační odolnosti a snižování zranitelnosti členských států vůči destabilizačním vlivům.

Historicky první ročník prestižního ocenění „Demokratická osobnost roku“ bude slavnostně zahájen dne 15. září u příležitosti Mezinárodního dne demokracie formou tiskové konference v České republice. Tímto okamžikem vzniká nová světová tradice „slavnosti demokracie“, jejímž cílem je vytvořit nejvýznamnější mezinárodní platformu pro oslavu demokratických principů, sdílených hodnot, občanské odpovědnosti a veřejného dobra v moderní éře. Česká republika se tím stává zakladatelskou zemí této nové demokratické tradice digitální doby, která má ambici postupně propojovat demokratické státy a občany napříč světem prostřednictvím sdílení společných hodnot.

Samotné slavnostní vyhlášení nominovaných a předání prestižního ocenění „Demokratická osobnost roku“ proběhne v roce 2027, opět symbolicky dne 15. září. Ocenění bude udělováno ve dvanácti kategoriích reflektujících klíčové oblasti fungování demokratické společnosti a ochrany veřejného dobra, včetně školství, zdravotnictví, sociální péče, politiky a veřejné správy, bezpečnosti a záchranných složek, podnikání, médií a nových forem komunikace, kultury a umění, sportu, vědy a inovací, práva a spravedlnosti, filantropie a životního prostředí a ochrany zvířat. Cílem je systematicky oceňovat osobnosti i občany, jejichž činnost přináší prokazatelný přínos společnosti a posiluje důvěru v demokratické hodnoty.

Iniciativa „Demokratická osobnost roku“ představuje první mezinárodní projekt svého druhu, který propojuje demokratickou osvětu s digitálním prostředím a

moderními technologiemi. V době, kdy neexistuje srovnatelná globální platforma spojující demokratické státy, občany Evropské unie, NATO a širší mezinárodní komunitu prostřednictvím pozitivního hodnotového rámce, vzniká nový prostor pro sdílení inspirace, občanské odpovědnosti a vzájemné úcty člověka k člověku. Tento koncept reaguje na rostoucí vliv informačního chaosu, dezinformací, nenávisti, polarizace a radikalizace ve veřejném prostoru, které se z kyberprostoru přenášejí i do fyzického světa a ovlivňují společenskou soudržnost a bezpečnost.

Klíčovou součástí celé iniciativy je sociální síť Politinn, která umožňuje občanům nominovat osobnosti z různých oblastí veřejného života, ale také vzájemně oceňovat běžné občany za jejich konkrétní přínos společnosti, občanskou statečnost a vykonávání veřejného dobra pro společnost a stát. Tento mechanismus vytváří nový prostor pro zviditelňování pozitivních vzorů, sdílení zkušeností a posilování důvěry v demokratické procesy.

Mezinárodní iniciativa „Demokratická osobnost roku“ vzniká v kontextu rostoucích hybridních hrozeb. „Slavnosti demokracie“ proto představují nový majestátní symbol demokratické kultury, uplatňované nejen ve fyzickém, ale i v digitálním světě. Jejím základem je občanská odpovědnost, konání veřejného dobra, úcta člověka k člověku, vzájemná podpora, sdílení hodnot a veřejné uznání těm, kteří v rámci svých možností a schopností chrání demokratické principy a přispívají k rozvoji společnosti i státu.

Seznam referenčních odkazů – zdroje a literatura

[1] https://niss.gov.ua/sites/default/files/2017-01/GW_engl_site.pdf

[2] https://www.demdigest.org/inside-putins-hybrid-war-western-democracy/#:~:text=%E2%80%9CThey've%20got%20the%20vehicle%20to%20do%20this,Western%20democracy%20itself%2C%20he%20writes%20for%20Reuters.

[3] https://report.az/en/other-countries/macron-accuses-russia-of-unleashing-world-hybrid-war

[4] https://www.novinky.cz/clanek/zahranicni-evropa-ruske-hybridni-operace-jsou-predehrou-valky-uvadi-nemecky-armadni-dokument-40556312

[5] https://www.forum24.cz/rusko-zaseva-rozkol-jsme-v-hybridni-valce-prohlasila-von-der-leyenova-evropa-potrebuje-dronovou-zed

[6] https://www.techzpravy.cz/hybridni-valka-uz-zacala-macron-varuje-pred-nebezpecnou-strategii-ruska/

[7] https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

[8] https://www.seznamzpravy.cz/clanek/domaci-politika-ai-uz-ted-meni-prubeh-boje-rika-muz-ktery-nato-pripravuje-na-moderni-valceni-302405#dop_ab_variant=0&dop_source_zone_name=zpravy.sznhp.box&source=hp&seq_no=1&utm_campaign=abtest305_podcasty_v_boxiku_varB&utm_medium=z-boxiku&utm_source=www.seznam.cz

[9] https://www.theguardian.com/world/2026/apr/01/trump-says-he-is-absolutely-considering-withdrawing-us-from-nato?utm_source=chatgpt.com

[10] https://ct24.ceskatelevize.cz/clanek/svet/usa-by-nemusely-prijit-nato-v-pripade-potreby-na-pomoc-

prohlasil-trump-371802

[11] https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

[12] https://www.ceskenoviny.cz/zpravy/sef-nato-vyzval-staty-aby-letos-presvedcily-ze-zvysuji-vydaje-na-obranu/2804662

[13] https://www.nato-pa.int/document/2025-cybersecurity-report-kairidis-010-cds?utm_source=chatgpt.com

[14] https://www.consilium.europa.eu/en/press/press-releases/2023/12/07/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-the-protection-of-democratic-processes-against-malicious-cyber-activities/?utm_source=chatgpt.com

[15] https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/?utm_source=chatgpt.com

[16] https://www.hybridcoe.fi/publications/countering-disinformation-in-the-euro-atlantic-strengths-and-gaps/?utm_source=chatgpt.com

[17] https://www.consilium.europa.eu/cs/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners/?utm_source=chatgpt.com

[18] https://reference-global.com/article/10.2478/kbo-2025-0014?utm_source=chatgpt.com

[19] https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2026.1790164/full?utm_source=chatgpt.com

[20] https://www.seznamzpravy.cz/clanek/domaci-politika-ai-uz-ted-meni-prubeh-boje-rika-muz-ktery-nato-pripravuje-na-moderni-valceni-302405#dop_ab_variant=0&dop_source_zone_name=zpravy.sznhp.box&source=hp&seq_no=1&utm_campaign=abtest305_podcasty_v_boxiku_varB&utm_medium=z-boxiku&utm_source=www.seznam.cz

[21] https://www.atlanticcouncil.org/dispatches/to-adapt-to-todays-security-threats-nato-should-prioritize-the-basics-of-defense-innovation/?utm_source=chatgpt.com

[22] https://www.researchgate.net/publication/394754993_NATO'S_MECHANISMS_FOR_THE_GOVERNANCE_OF_CYBERSECURITY

[23] https://commission.europa.eu/news-and-media/news/stronger-measures-protect-our-democracy-and-civil-society-2025-11-12_en?utm_source=chatgpt.com

[24] https://chinamediaproject.org/2026/04/01/ai-for-human-propaganda/

[25] https://en.wikipedia.org/wiki/Xinhua%E2%80%93Sogou_AI_news_anchor?utm_source=chatgpt.com

[26] https://ny1.com/nyc/all-boroughs/ap-top-news/2024/05/24/chinas-latest-ai-chatbot-is-trained-on-president-xi-jinpings-political-ideology?utm_source=chatgpt.com

[27] https://www.idnes.cz/technet/vojenstvi/putin-na-ukrajina-nacvicuje-nova-valka-online-maskirovka.A140703_163345_vojenstvi_kuz

[28] https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats#:~:text=Malign%20actors%20routinely%20conduct%20hostile%20information%20operations,and%20build%20resilience%20against%20these%20information%20threats

[29] https://ct24.ceskatelevize.cz/clanek/svet/porota-v-usa-shledala-google-a-metu-odpovednymi-v-pripadu-zavislosti-na-sitich-371703

[30] https://ct24.ceskatelevize.cz/clanek/veda/proti-sireni-dezinformaci-selhava-vetsina-znamych-strategii-upozornuje-studie-7229

[31] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en?prefLang=uk&utm_source=chatgpt.com

[32] https://www.oecd.org/en/topics/disinformation-and-misinformation.html

[33] https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/?utm_source=chatgpt.com