Otázky a perspektivy kybernetické obrany státu

František Hrubý

Smíchovská střední průmyslová škola a gymnázium

19. září 2025

Abstrakt

Článek se věnuje otázkám kybernetické obrany státu a představuje perspektivy komplexní strategie kybernetické obrany kombinující legislativní, technická a vzdělávacích opatření.

1 Úvod

Kybernetická obrana představuje zásadní oblast národní bezpečnosti. Jde o mezioborovou oblast propojující informatiku, bezpečnostní vědy, mezinárodní vztahy, právo i psychologii. Stát potřebuje ucelenou strategii, která dokáže identifikovat a eliminovat dlouhodobé hrozby nabývající v digitálním prostředí nových podob. Tento článek se zaměří na představení perspektiv které jsou schopné těmto hrozbám čelit.

2 Teoretická východiska

Pro formulaci vize kybernetické obrany je nezbytné vycházet z charakteru současných hrozeb, které zásadně ovlivňují národní bezpečnost. Významnou kategorií je kybernetická kriminalita, zahrnující jak útoky přímo proti ICT (např. šíření škodlivého kódu či neoprávněný přístup), tak i obecnou a hospodářskou kriminalitu realizovanou prostřednictvím internetu. Její typické znaky jsou decentralizace, anonymita a využívání modelu Crime-as-a-Service, což výrazně snižuje vstupní bariéry do kriminálního prostředí. Z pohledu kriminalistiky navíc dochází k oslabení tradičních vyšetřovacích metod, jelikož chybí klasické hierarchické struktury pachatelů, možnost infiltrace či využití korunních svědků. Prokazování trestné činnosti je komplikováno fragmentací stop, častým překračováním jurisdikcí a nutností spoléhat se na digitální důkazní prostředky, jejichž integrita i uchování vyžadují vysoce specializované znalosti a mezinárodní spolupráci.

Na tuto oblast navazují aktivity státních aktérů a APT skupin, jejichž činnost kombinuje technickou sofistikovanost se zpravodajským zázemím. Tyto skupiny představují zásadní hrozbu pro kritickou infrastrukturu a státní správu kvůli využívání zero-day zranitelností, cílených spear-phishingových kampaní. Kybernetická špionáž představuje novou hrozbu, na kterou ve své nejnovější výroční zprávě upozorňuje Bezpečnostní informační služba. Jejich působení má nejen technickou, ale i geopolitickou dimenzi, která vyžaduje specializovaný přístup, tentokrát doplněný o diplomatický rozměr.

Specifickou kategorii tvoří hybridní terorismus a extremismus, kombinující fyzické a digitální prostředky k prosazování ideologických cílů. Internet zde slouží k šíření radikalizačních narativů, náboru i plánování útoků. Zvláštní pozornost si zasluhuje fenomén akceleracionismu a rostoucí radikalizace mládeže prostřednictvím online subkultur.

S tím úzce souvisí dezinformační kampaně, které cizí státy či nestátní aktéři využívají k destabilizaci demokratických institucí prostřednictvím manipulace, polarizace společnosti a narušování důvěry veřejnosti ve stát. Tato hrozba je obzvlášť komplexní, jelikož vyžaduje rovnováhu mezi ochranou bezpečnosti a zachováním svobody projevu.

3 Metodologický rámec

Metodologický rámec tohoto článku vychází z analýzy relevantní odborné literatury, zejména výročních zpráv bezpečnostních sborů, mezinárodních strategických dokumentů a vládních prohlášení. Klíčovým zdrojem byly také poznatky z praxe předních expertů v oblasti kybernetické bezpečnosti a kybernetické obrany. Významně mě ovlivnilo i vedení mého mentora, který zdůrazňoval praktické zásady řízení kybernetické bezpečnosti a důležitost budování vazeb v odborné komunitě.

4 Výsledky

Navrhovaná koncepce kybernetické obrany stojí na čtyřech vzájemně propojených pilířích. Prvním je legislativa a standardizace, které vytvářejí rámec odolné bezpečnostní infrastruktury prostřednictvím definice a vynucování bezpečnostních standardů, sjednocení dodavatelských řetězců, zavedení závazných bezpečnostních politik a cíleného vzdělávání zaměstnanců. Klíčová je rovněž povinnost hlášení incidentů a podpora anonymizovaného sdílení informací, což minimalizuje reputační rizika a zároveň zvyšuje kolektivní odolnost.

Druhým pilířem je přestavba vyšetřování kybernetické kriminality, zahrnující rozlišení mezi čistě technickými delikty a těmi, kde ICT slouží jen jako prostředek spáchání trestného činu. U technických deliktů je výhodný centralizovaný přístup s expoziturami při krajských soudech pro efektivnější sdílení informací a mezinárodní spolupráci, zatímco u kriminality v kyberprostoru zůstává zachována odbornost původního deliktu a technické aspekty řeší specializovaní kriminalisté a soudní znalci.

Třetím pilířem je role zpravodajských služeb, jejichž kompetence jsou jasně diferencovány: vnitřní zpravodajství se soustředí na ochranu kritické infrastruktury a hybridní hrozby, vnější monitoruje APT skupiny a kyberkriminální fóra. Vojenské zpravodajství by mělo rozvíjet své technické kapacity a být technickým partnerem pro ostatní sbory.

Čtvrtým pilířem je vzdělávání a osvěta zahrnující systematické začlenění kybernetické bezpečnosti do vzdělávacího procesu a rozvoj tzv. společenské imunity, která umožňuje občanům lépe odolávat manipulativnímu obsahu a prosazovat zásady kybernetické hygieny.

5 Diskuze

Navržená vize přináší řadu podnětných poznatků, jejichž realizovatelnost je však nutné kriticky zhodnotit. Standardizace může vést k formálnímu plnění povinností bez reálného zvýšení bezpečnosti a svou rigiditou omezovat inovace. Standard proto musí být vymezen minimálně, aby vytvořil odolný základ pro další rozvoj. Problematické je i předávání informací, jelikož obavy z reputačních ztrát často brání spolupráci s veřejnou správou. Centralizace policejní činnosti vede k přetížení regionů, což lze částečně řešit zřízením expozitur při krajských soudech. V oblasti kybernetické expertizy se obtížně zajišťuje nábor a udržení specialistů; vhodnější může být využití externích dodavatelů, kdy se platí pouze za výsledky, nikoliv za provozní zajištění. Zpravodajské služby narážejí na limity dané jejich informační povahou. Rozšíření o represní pravomoci by vyžadovalo ústavní změny a naráželo na historicky podmíněnou nedůvěru. Současně by hrozila fragmentace činnosti, kterou lze překonat pouze pevně zakotvenou institucionální spoluprací. Ve vzdělávací oblasti je realizace dlouhodobého charakteru, a účinky se projevují až na generační úrovni. Dále je nutné zohlednit riziko zastrašování, přičemž vymezení efektivní hranice prevence představuje mimořádně složitý úkol.

6 Závěr

Kybernetická obrana vyžaduje komplexní strategii kombinující legislativní rámec, centralizované kapacity, jasně vymezené role zpravodajských služeb a dlouhodobé vzdělávání. Klíčová je schopnost pružně reagovat na technické změny a systematicky rozvíjet odborné kapacity státu i celé společnosti. Jen propojení těchto prvků vytváří předpoklad pro odolnou infrastrukturu a efektivní reakci na dynamicky se vyvíjející hrozby.