Čelí ČR hybridní útokům ze strany RF?

Jedna z nejpoužívanějších definic hybridní války popisuje tento fenomén jako „*komplexní použití konvenčních a nekonvenčních prostředků, včetně vojenských, polovojenských i nevojenských, k dosažení strategických cílů*.“ Abychom tedy mohli odpovědět na otázku položenou v názvu tohoto příspěvku, musíme určit, kterými z výše uvedených prostředků může Ruská federace (RF) proti České republice (ČR) v současnosti působit. Vzhledem k aktuálnímu charakteru vztahů mezi ČR a RF je vysoce nepravděpodobné jakékoliv nasazení těch s vojenským či polovojenským charakterem, tudíž jakékoliv šetření v této věci musí být omezeno pouze na prostředky na první pohled nevojenské – především pak na vlivové operace spojené se šířením propagandy a na kybernetické útoky.

Je přitom zřejmé, že prostředím, v němž se obě výše zmíněné hrozby realizují, je celosvětová komunikační síť internet. Přestože vlivové operace a kybernetické útoky mohou být prováděny i jinými způsoby, právě do značné míry neregulované a anonymní prostředí internetu umožňuje maximální využití jejich potenciálu.

V českém internetovém prostředí tak například vyvíjí svou činnost zhruba čtyřicet[1] tzv. alternativních webů, které zavádějící či propagandistický obsah (vč. propagandy proruské) buď šíří, nebo jej dokonce samy vytvářejí. Patrně nejznámějším příkladem takového webu jsou v současnosti stránky AE News, známější pod svým poloficiálním názvem Aeronet. Tento web, který ve své současné podobě funguje od 30. 6. 2015, byl opakovaně usvědčen ze šíření neobjektivních, nepřesných či záměrně lživých informací, z nichž se resortu obrany například dotýkala Aeronetem vytvořená a šířená dezinformace z února 2017, podle níž došlo k vyjmutí české 4. brn zpod pravomocí vrchního velitele ozbrojených sil ČR a jejímu zařazení pod velitelskou pravomoc německého Budeswehru. Uvedený článek přitom vycházel ze lživé interpretace dohody uzavřené mezi Německem a ČR o úzké spolupráci při výcviku v rámci NATO Framework Nations Concept.

Proruské narativy šíří v českém mediálním prostoru i subjekty s oficiální vazbou na ruskou státní moc. Jedním z nich je ruská státní mediální agentura Sputnik. Ta publikuje zpravodajství převážně pro mimoruské čtenáře v celkem 34 jazykových mutacích včetně češtiny. Již při založení Sputniku v roce 2014 jeho redakce oznamovala, že bude šířit alternativní zpravodajství proti „*monopolární vtíravé propagandě USA*.“ V ČR zahájil Sputnik činnost v březnu 2015, když navázal na postupně rušené rádio Hlas Ruska, oproti kterému představuje (přes značnou podobnost) ideologicky vyhraněnější médium. Česká mutace agentury Sputnik publikuje nejen své vlastní, ale i převzaté články, přičemž byla již mnohokrát obviněna z používání argumentačních klamů (např. nepřesných termínů, prezentování názorů pouze jedné strany, zavádějících úprav rozhovorů, nekorektního označování zdrojů či prezentování neověřitelných údajů). Část české mediální scény rovněž obviňuje Sputnik ze šíření explicitních a cílených dezinformací.

[1] Server Evropské hodnoty uvádí celkem 37 takovýchto webů, podle slovenského učitele, aktivisty a autora seznamu dezinformačních webů Juraje Smetany působí takovýchto webů v českém a slovenském mediálním prostoru celkem 42.

Ani alternativní, ani oficiální ruské weby však v současnosti nedisponují potenciálem oslovit většinovou českou veřejnost. Jejich čtenáři se rekrutují z okrajů politického spektra, přičemž nezřídka zastávají názory blízké marginálním politickým subjektům nacionalistického či slavjanofilského zaměření. S vysokou pravděpodobností tak dezinformace šířené prostřednictvím těchto webových stránek nemají dostatečný dosah na to, aby dokázaly např. změnit postoj české veřejnosti vůči NATO či EU.

Oproti přímému propagandistickému působení však představují výrazně vyšší nebezpečí kybernetické útoky. Prakticky od vzniku počítačové kriminality totiž dochází k jejich kvantitativnímu i kvalitativnímu nárůstu. V současnosti jsou jejich typickým terčem především prvky kritické informační infrastruktury, kdy se útočníci pokoušejí extrahovat informace z významných vládních institucí, bezpečnostních subjektů a soukromých společností. V průběhu posledních let tak byly provedeny útoky proti institucím mnoha evropských zemí (zejména ministerstvům zahraničí či obrany) nebo mezinárodních organizací. Příkladem takové operace byl útok proti Organizaci pro zákaz chemických zbraní, který proběhl krátce poté, co se tato organizace začala intenzivně zabývat incidentem v Salisbury, kde došlo k chemickému útoku na někdejšího ruského agenta Sergeje Skripala. Podobným kybernetickým aktivitám musely v souvislosti s vyšetřováním dopingových skandálů ruských sportovců čelit i Světová antidopingová organizace a Mezinárodní olympijský výbor.

Přes výše uvedená fakta je však značně obtížné blíže popsat skutečné dopady hybridního působení RF v ČR Na druhou stranu je zde ale možno nalézt celou řadu indicií naznačujících, že zmíněná hybridní kampaň dosáhla určitých výsledků. Jednou z nich jsou, na základě facebookových iniciativ, opakované snahy o vytvoření paramilitárních jednotek – většinou v podobě uniformovaných domobraneckých skupin. Takovéto aktivity se začaly objevovat po ruské anexi Krymu a následném zostření vztahů mezi RF a západním společenstvím. V roce 2015 pak do jejich ideologické výbavy přibyl další motiv – obavy z migrační vlny a následné islamizace české a evropské společnosti. Existenci těchto uskupení přitom nelze podceňovat a to minimálně ze dvou důvodů:

Za prvé – vytvářejí potenciálně mobilizovatelnou skupinu odpůrců současného proaliančního a prounijního směřování ČR, která by mohla v případě krize organizovaně narušovat veřejný pořádek nebo by mohla páchat trestnou činnost (od deliktů kriminálního charakteru až po vyzvědačství).

Za druhé – radikalizace jednotlivců, kteří by se jako vlci samotáři mohli dopustit stejné trestné činnosti kdykoliv z vlastních ideologických pohnutek.