Hybridhotet och kriminaliteten

av Lars Nylén

Résumé

To counter hybrid threats against the EU and NATO, The European Centre of Excellence for Countering Hybrid Threats (CoE) was established in Helsinki in 2016. The center aims to strengthen cooperation between private, public, military and academic sectors. A large number of analyses have been reported. Hybrid activities, from soft power to military means, are nothing new, but have gained a faster and greater impact through digitalisation and social media. Since 2023, there has been a significant increase in threats and attacks against the entire EU. To make attribution more difficult, state actors are increasingly using criminal networks as proxies, Europol reports in 2025. Even young people and the uninitiated are being ensnared as proxies. It is a shadow war that is underway. The attacks disrupt infrastructure, are destabilising and spread unrest. It is often difficult to pinpoint the person behind threats and events, which is why increased vigilance, a holistic approach and multidisciplinary collaboration are required to connect the dots, but also to use various tools to respond to threats and attacks, against both the underlying actors and their proxies.

> Russia is emboldened to sabotage the critical infrastructure of EU and NATO countries, recruit their citizens for clandestine hostile operations, and target their institutions and procedures with hybrid threat operations.

CITATET ÄR EN av slutsatserna i en uppsats från en av forskarna vid European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE, i Helsingfors.[1]

Hybrid CoE

Behovet att stärka det gemensamma arbetet för att stå emot och motverka hybridhot mot EU och Nato ledde i april 2016 till beslutet att etablera ett kompetenscentrum. För det syftet arbetar centrat med att stärka samsynen mellan de privata, offentliga, civila, militära och de akademiska sektorerna – The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Initiativet godkändes av Europeiska unionens råd och Nordatlantiska rådet i december 2016. Hybrid CoE-sekretariatet placerades i Helsingfors. Centrat invigdes officiellt i oktober 2017 av bland andra Natos dåvarande generalsekreterare Jens Stoltenberg och EU:s höga representant för utrikesfrågor och säkerhetspolitik Federica Mogherini. Nio länder undertecknade ett samförståndsavtal.[2] De var Finland, Sverige, Storbritannien, Lettland, Litauen, Polen, Frankrike, Tyskland och USA. Sedan dess har ytterligare 27 länder anslutit sig.

Centrets vision är en värld där våra öppna, demokratiska samhällen fungerar fria från fientlig inblandning utifrån. Det är ett autonomt centrum och den enda aktören där både EU och Nato arbetar och genomför

övningar tillsammans, med aktiviteter som täcker ett brett spektrum av domäner från civila till militära, och från fientlig påverkan till hybridkrigföring.

Genom tvärstatliga och tvärsektoriella nätverk med över 1 800 praktiker och experter uppnår centret hög standard. Förutom att främja akademisk forskning och debatt om relevanta ämnen genomför centret skrivbordsövningar (tabletops) och experimentella övningar med olika hybridhotsscenarier. Under de gånga åren har CoE publicerat över trettio uppsatser med analyser av hybridhotet.

Hybridhot – är det något nytt?

I rubriken ställs frågan om hybridhot, i förlängningen hybridangrepp, är något nytt. Det korta svaret är: Nej.

Ännu en gång kan vi återvända till det klassiska arbetet om krigskonsten som tillskrivs kinesen Sun Zi (född cirka 540 f Kr). Sun Zi beskriver taktiska knep för att påverka utfallet av en konfliktsituation till egen fördel. Han ansåg att den högsta formen av krigskonst är att vinna utan att utkämpa en enda väpnad strid. I normala fall är det bättre att erövra ett land intakt än att krossa det. Den bästa strategin är att sabotera, den näst bästa att motverka allianser.[3] Hybridhot och hybridaktiviteter är med andra ord inget nytt.

Vad innefattas då i begreppet hybridhot? Flera definitioner finns. EU och Nato, Hybrid CoE och svenska myndigheter inom säkerhetsrelaterade verksamhetsområden använder sig av begreppet i bredare eller snävare betydelse.[4]

Begreppet *hot* är det centrala. För juristen kommer då närmast straffstadgandet om olaga hot i 4 kap 5 § brottsbalken i förgrunden. Det handlar om ett brott mot frihet och frid genom att framkalla allvarlig rädsla för egen eller annans säkerhet till person, egendom, frihet eller frid. När hotet realiseras gör man sig skyldig till andra typer av gärningar.

Sedan många år har det på olika sätt redovisats att den grova organiserade brottsligheten är systemhotande. Våren 2024 rapporterade Europol att 821 kriminella nätverk var aktiva i EU och påverkade EU:s inre säkerhet. Bland annat ägnade de sig med stor kraft åt korruption i syfte att påverka rättsapparaten och juridiska processer.

Ungefär samtidigt redovisades motsvarande iakttagelser i en rapport från Brå.[5] Där lyftes det fram i dagsljuset att personer med kopplingar till den organiserade brottsligheten nästlar sig in i samhällsbärande institutioner. Hot och påtryckningar förekommer mot tjänstemän. I tider av ett ökat samarbete mellan vissa länder och grov organiserad brottslighet har det blivit allt viktigare att vara observant på hur hot och aktiviteter från organiserad brottslighet blivit del av en antagonistisk verksamhet från främmande makt i form av hybridaktiviteter.[6]

Genom en proposition i mars 2025 tog regeringen initiativ till ett ökat straffrättsligt skydd för tjänstemän och utövare av vissa samhällsnyttiga funktioner. Utsattheten för våld, hot och trakasserier mot offentliganställda bedömdes vanligare och förekommande i hela förvaltningen. Angreppen mot offentliganställda betraktades i förlängningen även som ett hot mot demokratin och samhället. ”En fortsatt negativ utveckling riskerar även att påverka allmänhetens tillit till myndigheterna och samhället i stort. Situationen är systemhotande och utgör en fara för vårt demokratiska samhälle som i förlängningen även riskerar att underlätta för brottslig verksamhet”,[7] skrev regeringen. Sådana otillbörliga gärningar ingår typiskt sett även i hybridaktörernas verktygslåda.

Också anställda i samhällsviktig verksamhet kan mot denna bakgrund vara måltavlor för hybridaktörer och kriminella proxies, utsättas för otillbörlig påverkan och snärjas för att utföra, passivt och aktivt, hybridhotsaktiviteter. Insiderhotet är en komplex problematik och det kräver uppmärksamhet.

År 2019 redovisade Försvarshögskolan en antologi med ett bredare fokus på hotbegreppet, på antagonistiska hot mot samhällsviktig verksamhet som riskerar att skrämma eller skada institutioner, funktionalitet och system utifrån deras lagstadgade uppgift i samhället.[8]

Man måste fråga sig var gränserna går mellan å ena sidan acceptabel retorik, ett offensivt förhandlingsspråk, och å andra sidan asocialt beteende, d v s brist på respekt för andra människors rättigheter och för sociala normer, som att bryta mot lagen, ljuga och luras. Utvecklingen förskräcker. Vad det långsiktigt får för konsekvenser återstår att se. Blir det rumsrent att hota, förödmjuka, förolämpa och trakassera? Är det då dags för diplomater att gå en kurs hos Gudfadern i gangsterretorik?

Hybrid innebär en blandning eller en korsning av skilda arter. Begreppet finns inom olika ämnesområden. I vår tid möter vi det ofta hos bilförsäljaren i benämningar som laddhybrid, fullhybrid, mildhybrid och plug-in-hybrid. Det handlar då om fordon som kan drivas av mer än en kraft, av fossilt bränsle som bensin och diesel och av el. På 1800-talet förekom hybridfartyg, det vill säga ångfartyg som också, för säkerhets och uthållighets skull, hade segel och kunde drivas av vinden då kolet till ångpannorna tog slut mitt ute i Nordatlanten.

Begreppet hybridhot, hybridangrepp och hybridkrig fick en aktuell och vidare spridning när en mängd ”små gröna maskerade män” översvämmade östra Ukraina och annekterade Krim i februari 2014. Pro-ryska rebeller och ryska specialtrupper utan nationalitetsbeteckningar intog då viktiga platser på halvön och avväpnade ukrainarna.

Då ljög den ryske presidenten Vladimir Putin Tysklands förbundskansler Angela Merkel rakt upp i ansiktet när hon frågade honom om de ryska förband som enligt Natos satellitbilder slogs på separatisternas sida i Luhansk och Donetsk.[9] Inga ryska soldater har skickats dit, om det finns några där, är de där på semester, var Putins besked. Utrustningen kan köpas i vilken militär surplusshop som helst, sa Putin. Man måste dock tillåta sig invändningen att det är sällan som personer åker på semester i stridsfordon. Den dimridån var inte särskilt tät!

> *Hybridhotet och hybridangreppen innefattar även en rad kriminella aktiviteter och taktiker, såsom sabotage av kritisk infrastruktur*

Hybridhotet och hybridangreppen innefattar även en rad kriminella aktiviteter och taktiker, såsom sabotage av kritisk infrastruktur genom digitala eller fysiska medel, informationsstöld, desinformationskampanjer, cyberattacker, migrantsmuggling, vissa typer av narkotikahandel och andra former av brott. Säkerhetspolitiska spänningar och kriser och krig runt om i världen ökar och sprider hybrishotsaktiviteterna, också till EU.

Europeiska unionen konstaterade år 2016 att definitionen av hybridhot varierar och måste vara flexibel eftersom hotet hela tiden förändras. Begreppet syftar, enligt EU, till att fånga upp den blandning av tvångsåtgärder och omstörtande verksamhet samt konventionella och okonventionella metoder (d v s diplomatiska, militära, ekonomiska och tekniska) som statliga eller icke-statliga aktörer kan använda på ett samordnat sätt

för att uppnå särskilda mål, samtidigt som de håller sig under tröskeln för en formell krigsförklaring. Tonvikten ligger vanligen på att utnyttja målets svagheter och skapa tvetydighet för att försvåra beslutsfattande. Massiva desinformationskampanjer, där sociala medier används för att kontrollera den politiska beskrivningen eller radikalisera, rekrytera och leda proxyaktörer, kan fungera som verktyg för hybridhot.[10]

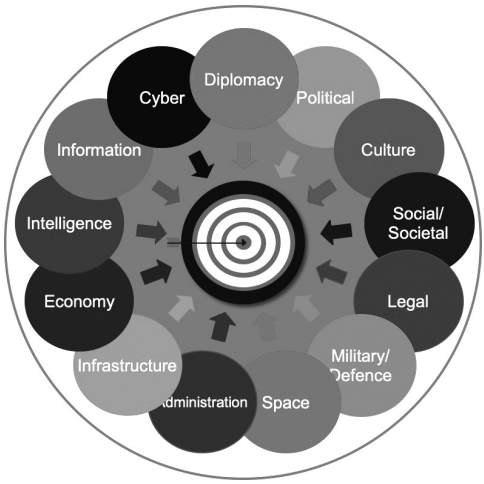
Hybridhotet utvecklas ständigt. EU och dess medlemsstater är just nu föremål för hybridkampanjen som innefattar sabotage, cyberattacker, ekonomiskt tvång, störning och spoofing[11] av satellitsignaler samt genom instrumentaliserad migration. Det framgår av Niinistö-rapporten till EU-kommissionen i oktober 2024.[12]

Hybridhotsaktörerna visar stor uppfinningsrikedom då det gäller att utforma och utföra attacker

Hybridkampanjer av illvilliga statliga aktörer planeras och organiseras ofta av dessa staters utländska underrättelsetjänster och kombineras med spionageverksamhet, medan enskilda handlingar ofta utförs av ombud.[13] Skuggkriget är här för att stanna, skriver ledamoten Patrik Oksanen.[14]

Kampanjerna är således allvarligare än de enskilda uttrycken av dem. Enskilt och styckevis är det brott som begås och som således är en uppgift för rättsväsendet. De bakomliggande syftena gör att brotten, anstiftare och främjare, måste tacklas i ett bredare perspektiv och parallellt med den traditionella brottsbekämpningen. Man måste således agera på flera fronter samtidig och kombinerat, mot anstiftande och främjande statliga aktörer och deras utförare, d v s gärningspersonerna i den konkreta handlingen.

Det krävs ett bättre förberett och motståndskraftigt Europa, konstaterar EU-kommissionen i sitt svar på Niinistö-rapporten i mars 2025.[15] Kommissionen skriver vidare:



Figur 1. Domäner för hybridhotsaktiviteter, Hybrid CoE, Helsingfors.

> In order to prevent, deter and respond more effectively to security incidents and crises, and deter malicious actors, the EU needs to use its full spectrum of tools, including: (i) cyber diplomacy; (ii) FIMI toolbox[16]; (iii) hybrid toolboxes and (iv) space threat response mechanism architecture; as well as (v) defensive capabilities available to the civilian and military communities, including when appropriate, proactive defensive measures, in accordance with the international law.
>
> The High Representative and the Commission will develop strategies to prevent, deter and respond to specific threat actors targeting the EU through hybrid, cyber and FIMI activities. Close coordination with NATO and other like-minded partners is necessary to increase the impact and dissuade threat actors.[17]

Hybrid CoE pekar på tretton olika domäner som kan utgöra mål för hybridhotsaktiviteter (figur 1).[18] Genom att utnyttja sårbarheter och det rätta tillfället kan en aggressor

kraftigt påverka ett annat land utan att öppet behöva utnyttja militära medel. Angreppen kan givetvis överlappa varandra och samtidigt riktas mot flera domäner.

I samma rapport redovisar författarna även en lista med 40 olika verktyg som kan användas av en aggressor för att nå sitt syfte.[19] Samtidigt påpekar de att ”hybrid is always a combination of tools but not all combinations are hybrid”. Domänerna och verktygen utvecklas hela tiden. Genom att angreppen ofta sker dolt och bedrägligt kan det även finnas andra hot. Nya verktyg kommer med all säkerhet att dyka upp i framtiden.

Genom att man, oftast tyst, agerar i gränssnittens gråzoner kan angreppen överraska och ge stor och kostnadseffektiv effekt för angriparen.

Hybridhotet är således ett lågintensivt krig med andra medel i ett svårgripbart stridsfält där kriget nu pågår i stor omfattning. Angreppen sker i skuggan av olika gränssnitt: mellan fred och krig, mellan vän och fiende, öppet eller dolt, mellan inre och yttre

Listade verktyg bl a

Armed forces conventional/sub-conventional operations.	Clandestine operations.
Paramilitary organizations (proxies).	Infiltration.
Military exercises.	Diplomatic sanctions.
Engaging diasporas for influencing.	Boycotts.
Financing cultural groups and think tanks.	Embassies.
Exploiting of sociocultural cleavages (ethnic, religion and culture).	Creating confusion or a contradictory narrative.
Promoting social unrest.	Migration as a bargaining chip in international relations.
Manipulating discourses on migration to polarize societies and	Discrediting leadership and/or candidates.
undermine liberal democracies.	Support of political actors.
Exploiting vulnerabilities in public administration (including emergency management).	Coercion of politicians and/or government.
Promoting and exploiting corruption.	Exploiting immigration for political influencing.
Exploiting thresholds, non-attribution, gaps and uncertainty in the law.	Media control and interference.
Leveraging legal rules, processes, institutions and arguments.	Disinformation campaigns and propaganda.
Intelligence preparation.	Influencing curricula and academia.
	Electronic operations (GNSS jamming and spoofing).

Tabell. Hybrid CoE listar olika verktyg som kan användas av en aggressor.

säkerhet, mellan civilt och militärt och mellan icke-statliga och statliga aktörer.

Det datoriserade, fjärrstyrda, automatiserade och sammankopplade samhället, med system i system, innebär ökat beroende och därmed ökad sårbarhet. Genom att man, oftast tyst, agerar i gränssnittens gråzoner kan angreppen överraska och ge stor och kostnadseffektiv effekt för angriparen. Först då det är för sent upptäcks många av attackerna, om de ens upptäcks. Angreppen sker med ljusets hastighet. Molnbaserade tjänster och artificiell intelligens (AI) innebär dessutom nya utmaningar.[20]

Kriminella som ombud (proxies)

Hybrid CoE ger följande definition på *icke-statliga aktörer*: enheter som spelar en roll i internationella relationer och som utövar tillräcklig makt för att störa, påverka och orsaka förändring utan någon koppling till en stats etablerade institutioner.[21]

Hybrid CoE ger som exempel att ryska gråzonsaktiviteter involverar många okoordinerade aktörer, statligt ägda företag, privata militära företag, patriotiska grupper som bikergäng och hackare, oligarker och den ortodoxa kyrkan.[22] Även populistiska politiska företrädare kan snärjas som proxies.

Liksom under det kalla kriget uppmärksammas återigen utländska investeringar i Sverige som en risk, inte minst i anslutning till en del etableringar av ryska företag och ryskt fastighetsägande. Från det kalla kriget finns erfarenhet av oönskat tekniköverförande och att utländska företag nyttjas som täckmantlar för olovlig underrättelsetjänst. En rapport från FOI diskuterar problematiken.[23]

Ett av de mer påfallande exemplen på proxies utgör de rebeller som Ryssland bland annat utnyttjade som förevändning till anfallskriget på Ukraina i februari 2014.

Betydligt svårare är det, å andra sidan, att omedelbart, eller alls, se hoten och aktiviteterna som iscensätts via enskilda individer och företag, liksom att utröna den egentliga aggressorn i en bakomliggande relation. För att försvåra attribuering och bakåtspårning kan det skapas en eller flera mellanhänder mellan ursprunglig uppdragsgivare och utförare. Avsikten är då givetvis att skapa en suddig, komplex och svårgenomtränglig bild av relationen och skeendet. Att blanda bort korten och blåneka är en självklarhet, om man blir ifrågasatt.

Det kan med andra ord handla om många olika typer av aktörer, ombud och möjliggörare. Deras bevekelsegrunder för att agera som ombud varierar och kan ha ideologiska, etiska, religiösa och ekonomiska skäl. De kan också vara utsatta för utpressning. Egen agenda och ömsesidiga fördelar av att samarbetet varierar med relationen till uppdragsgivaren.

Till ombudens skara hör kriminella personer i den organiserade grova brottsligheten. Den 18 februari 2025 publicerade Europol, EU:s byrå för brottsbekämpning, den årliga rapporten *EU Serious and Organised Crime Threat Assessment* (EU-SOCTA 2025).[24]

EU-SOCTA är en gemensam hotbildsrapport som sammanställs av Europol utifrån uppgifter från medlemsstaterna, egna databaser, andra EU-byråer såsom Frontex och Eurojust, Europols partnerländer utanför EU, privata tredje partner samt öppna källor. SOCTA innehåller en analys av de nuvarande och framtida hot som grov och organiserad brottslighet innebär för EU och ger rekommendationer om vilka brottstyper medlemsländerna bör prioritera.

I EU-SOCTA 2025 konstaterar Europol att det skett en fundamental förändring av blåkopian för grov och organiserad brotts-

lighet. Brottsligheten är mer inkräktande och destabiliserande än någonsin tidigare. Den drabbar även grundvalarna för institutioner och samhälle:[25]

De nyckelområden som utgör den högsta hotnivån mot EU kommer att förvärras ytterligare av den allvarliga och organiserade brottslighetens förändrade DNA. Det som sticker ut idag och kommer att bli ännu mer framträdande i morgon är hur allvarlig och organiserad brottslighet destabiliserar samhället på två sätt: den undergräver EU genom generering av olagliga intäkter och parallella ekonomier, och dessutom destabiliserar den EU eftersom kriminella nätverk i allt högre grad fungerar som ombud i hybridhotaktörers tjänst, ett samarbete som är ömsesidigt förstärkande.

Dessutom frodas den grova och organiserade brottsligheten i allt högre grad online, med fler och mycket påverkande kriminella aktiviteter som till stor del sker i det digitala rummet. Och den accelereras av AI och annan ny teknik, vilket gör grov och organiserad brottslighet mer tillgänglig och automatiserad, ökar dess omfattning och räckvidd och förbättrar dess kapacitet, menar Europol.

Samarbetet mellan kriminella nätverk och hybridhotsaktörer destabiliserar samhället. Det finns anledning att tro att även vissa av de kriminella aktörerna har intresse av att destabilisera EU och dess medlemsstater. Dessa kan då ha fokus på demokratiska processer, social koherens inom samhället, trygghetskänslan och rättsstatens principer. Även den finansiella stabiliteten i ekonomin kan påverkas, påpekar Europol.[26]

Samarbetet med kriminella nätverk och hybridhotsaktörer är ofta till ömsesidig nytta, de utnyttjar varandras resurser, expertis, och skydd för att uppnå målen. Om man ska utföra något måste man också få något, även om balansen i perspektivet *quid pro quo* kan vara ojämn. Samtidigt varierar styrkan och formen för kopplingen mellan de båda aktörerna. Stater utnyttjar även personer som inte är medvetna om att de är indragna i och utnyttjas i hybridaktiviteter, begreppet ”nyttig idiot” är känt sen länge. Omvänt kan proxies vara skapade av en statlig aktör.[27] De kriminella nätverken är i första hand ute efter att tjäna pengar, men de kan samtidigt skaffa sig en ”safe haven”, om än osäkert och så länge det varar, att verka från. Nätverken kan också ha andra egna syften, men det kan även vara en ohelig allians.

En särskild problematik, att allt mer hålla ögonen på, är rekrytering via nätet av unga personer för hybridaktiviteter. Med tydlig erfarenhet från den grova brottslighetens rekrytering av unga, inklusive den snabba radikaliseringsprocessen till terrorism via nätet, onlineverktyg och slutna plattformar, måste uppmärksamhet riktas mot risken att hybridhotsaktörer för sina hostila syften även kan aktivera unga personer. I det fallet avskräcker knappast det sedan år 2023 införda straffstadgandet, 16 kap 5a § brottsbalken, om *involverande av en underårig i brottslighet*:

Den som för brott eller brottslig verksamhet anlitar, betalar, instruerar eller överlämnar egendom till någon som inte har fyllt arton år och därigenom, eller på annat liknande sätt, involverar honom eller henne i brottet eller den brottsliga verksamheten, döms för involverande av en underårig i brottslighet till fängelse i högst fyra år. Detta gäller även om den som begår en sådan gärning inte haft uppsåt till men varit oaktsam beträffande omständigheten att den andra personen inte fyllt arton år.

Ledamoten Johan Olsson konstaterar i sitt inträdesanförande år 2024 att aktörerna inom den grova organiserade brottsligheten är multikriminella och utvecklingsorienterade. De sätter ihop nätverk för att

genomföra olika typer av brottsupplägg och effektiviteten i dessa nätverk är hög och många funktioner går att köpa genom det som kallas crime-as-a-service. Det går idag att köpa malware, bedrägeriupplägg, logistikupplägg, bolag, identiteter etcetera på en global marknad.

Europol konstaterar i sin SOCTA-rapport 2025 att de kriminella aktörerna tidigt erbjöd tjänster på cyberområdet och att de nu på ett signifikant sätt bidrar med ransomware-attacker mot kritisk infrastruktur, företag och myndigheter.[28] De kan även, på uppdrag, genom att infiltrera säkra system stjäla information av strategisk betydelse för myndighetsutövning eller företagsverksamhet. De förser sina uppdragsgivare med ovärderlig information som de i sin tur kan använda för spioneri, till sin ekonomiska fördel eller till och med våldsaktiviteter.[29]

Ytterligare områden där kriminella nätverk verkar som proxies är det som kallas instrumentaliserad migration. Krig och kriser i EU:s närområde är ”push factors” i detta sammanhang och tydliga exempel finns på flera sådana hybridattacker, även mot det nordiska området, enligt den Europeiska gräns- och kustbevakningsbyrån (Frontex).[30]

I en EU-förordning på migrations- och asylområdet från maj 2024 konstateras att det kan uppkomma en instrumentaliseringssituation när ett tredje land eller en fientlig icke-statlig aktör uppmuntrar eller underlättar tredjelandsmedborgares och statslösa personers förflyttning till unionens yttre gränser eller till en medlemsstat, och detta agerande tyder på ett tredjelands eller en fientlig icke-statlig aktörs avsikt att destabilisera unionen eller en medlemsstat och därigenom agerande riskerar att äventyra en medlemsstats väsentliga funktioner, inbegripet upprätthållandet av lag och ordning eller skyddet av den nationella säkerheten.[31] I sådana situationer står således kriminella nätverk som sysslar med migrantsmuggling till förfogande.

Ursprungligen skedde hybridangreppen som enskilda och omfattande attacker utförda av ett annat land. Nu förekommer de också som delar i ett större strategiskt syfte, även utförda av kriminella nätverk: fortlöpande till synes mindre attacker som sammantaget urholkar stabilitet, säkerhet och förtroende för olika institutioner, som ett hackspettsangrepp.[32]

När det gäller påverkanskampanjer hamnar lagstiftaren i en demokratisk stat i ett dilemma. Frågan är hur reaktionerna ska utformas när utländska krafter skapar oro och eldar på konfrontationer, exempelvis som under påskuppploppen påskhelgen 2022, flickmorden i Storbritannien i augusti 2024 och i anslutning till koranbränningar i Sverige och Danmark.

Att yttrandefrihet används som argument för att tillåta bränningar ansågs otillräckligt och irrelevant av många. Svensk polis kritiserades för att skydda koranbrännare, dels genom att inte ingripa mot dem, dels genom att hindra åskådare från att avbryta eller släcka bränningar.

Bränningarna kallades islamofobiska, rasistiska och hatiska. De beskrevs som medvetet provokativa, som en aggression, och som en kriminell handling. I juni 2023 greps två syriska bröder i Tyskland och dömdes senare i Hamburg för att ha planerat ett islamiskt motiverat terrorbrott i Sverige. Enligt de tyska åklagarna planerade de ett bombdåd mot en kyrka i Sverige, som hämnd för koranbränningar.[33] Denna och ytterligare bränningar sommaren 2023 uppgavs, likt tidigare bränningar, vara exempel på västerländsk arrogans och en överlägsen hållning gentemot den muslimska världen. Att bränna koranen blev ett exempel på västerländska länders ”moraliska förfall”.

Objekt som representerar Sverige och Danmark i utlandet blev måltavlor.[34] I sociala medier uppmanades till bojkott av kända svenska varumärken, varor och tjänster. Därmed hamnade svenska internationella företag i en utsatt position.

Efter ett grovt dataintrång i juli 2023 genomförde iranska statliga organ en påverkansoperation mot Sverige genom ett massutskick av sms. Därvid uppmanades till hämnd mot koranbrännare och påstods att Sverige förberedde krig mot den muslimska världen.

Krav på förbud av olika slag restes i debatten. Samtidigt menade många att händelser av detta slag inte får leda till oreflekterade författningsändringar som inskränker de demokratiska friheterna. Vad skulle kraven kunna betyda för centrala frågor som skyddas av yttrandefrihetsgrundlagen? Det anses å ena sidan att ett fritt och rättvist samhälle måste kunna tolerera även det intoleranta. Å andra sidan måste samhället ha en rimlig rätt till självbevarelse. Kan en sådan diskussion även vara kopplad till och få bränsle genom hybridaktiviteter?

Det dilemma som detta innebär kallas toleransparadoxen eller Popper-paradoxen, vilken beskrevs av filosofen Karl Popper år 1945. Han menade att om vi inte är beredda att försvara ett tolerant samhälle mot de intolerantas angrepp, då kommer de toleranta att gå under, och toleransen med dem. Ett demokratiskt och öppet samhälle är således alltid utsatt för förfall inifrån, från människor som drar nytta av de friheter ett tolerant samhälle erbjuder i akt och mening att bekämpa dess friheter.

Bland rysslandkännare finns en tydlig uppfattning att Ryssland för ett politiskt krig mot västvärlden. För den skull sår man via det lågintensiva kriget tvivel, oro och aggression samt skapar avsiktligt missförstånd. Man stöttar europeiska populistpartier.

Hybridhotsaktörer

Cyberkriminalitet emanerar främst från Ryssland, Kina, Iran och Nordkorea. Kina anses ha världens mest omfattande hackerprogram.

Niinistö-rapporten redovisar en markant ökning av antalet (försök till) fysiska sabotagehandlingar över hela unionen sedan 2023. Till exempel kunde tyska myndigheter stoppa en misstänkt rysk komplott som involverade sprängämnen och mordbrand på militära och industriella anläggningar i april 2024. År 2023 frihetsberövade polska myndigheter medlemmar av en påstådd rysk spionring som planerade att spåra ur ett tåg som transporterade hjälp till Ukraina.[35]

I en rapport i februari 2025 från Hybrid CoE uppger man att det inte enbart är stormakter som använder sig av proxy wars. Stater runt om i världen strävar efter att skörda frukterna av proxies samtidigt som de minimerar kostnaderna för striderna, och det är naturligt att det också sker i gråzonen. De vanligaste statliga sponsorerna av väpnade ombud inkluderar Libyen, Saudiarabien, Kuba, Pakistan och Iran.[36]

Liksom narkotikahandeln i världen via omvägar, där uppmärksamheten vanligen är lägre, söker sig till destinationslandet för att minska risken för upptäckt, kan man tänka sig att även hybridhotsaktörer engagerar proxies från länder som typiskt sett ådrar sig mindre uppmärksamhet vid gränspassager. Ungefär som i fallet med den uppgivne brasilianske forskaren som tog sig till Norges arktiska universitet i Tromsö, men i oktober 2022 avslöjades som rysk illegalist och anklagades för spionerі.

Sammanfattning

Flera rapportörer redovisar en markant ökning av hybridaktiviteter. Vi har alltså ”sett

det komma". Detta hot kräver ett ändrat tankesätt, särskilt som verktygslådan för att hantera problematiken är spridd över flera organ. Det krävs att flera pusselbitar läggs samman för att bilden ska framstå, dessutom en vaksamhet, en helhetssyn och ett multidisciplinärt ansvarstagande. Det gäller att se skogen bland träden och förstå komplexiteten.

Niinistö-rapporten har fått EU att röra sig i rätt riktning och vi behöver ta ansvar för vår säkerhet. Regeringens kommittédirektiv i oktober 2023 om översyn av underrättelseverksamheten omfattar delvis problematiken.[37] Direktiven kan tyckas alltför kliniskt sektoriserade mot bakgrund av den senare tidens utveckling där kriminella nätverk i ökad grad engageras av hybridhotsaktörer för att ludda till bilden och lägga ut dimridåer. Ser man problematiken från andra hållet än ur underrättelseperspektivet, det vill säga att något hänt och kräver respons, kan det vara svårt att omedelbart veta vad som ligger bakom händelsen och hur insatsansvaret fördelas.

Problematiken är överlappande. Det som från början uppfattas som en olycka kan senare visa sig vara iscensatt av främmande makt. Hybridhot och annan brottslighet har en tendens att äga rum utan respekt för våra förvaltningsgränser och organisatoriska rutor, snarare finns en förmåga att utnyttja dessa till egen fördel. Hinder för samverkan måste minska.

Författaren är tidigare chef för Rikskriminalpolisen och generaldirektör. Han är ledamot av KKrVA.

Noter

1. Kubica, Lucjan: ”Ukraine’s Position in Russia’s strategic thinking: Domestic, regional and International order”, *Hybrid CoE Paper 20*, september 2024, s 21.
2. *https://www.hybridcoe.fi/wp-content/uploads/2017/08/Hybrid-CoE-final-Mou-110417-1.pdf*, (2025-02-02).
3. Ooi, Kee Beng och Pettersson, Bengt: *Sun Zi:s Krigskonst*, 2. uppl, Försvarshögskolan, Stockholm 1999, s 25.
4. Appelgren, Jessica; Bay, Sebastian, Malminen, Johannes och Zouave, Erik: *Strategisk verktygslåda mot hybridhot. Ett ramverk för gemensam problemförståelse*, FOI-R-4816-SE, 2020, s 16.
5. *Möjliggörare för kriminella nätverk*, Rapport 2024:2, Brottsförebyggande rådet.
6. Nylén, Lars: ”Förändrad sårbarhet i en tid av oro” i Andersson, Björn (red): *I närtid*, Projekt SV-A-R, mellanrapport årsskiftet 2024/25, del II, Kungl Krigsvetenskapsakademien, Stockholm 2025, s 239.
7. Prop. 2024/25:141, s 19.
8. Häggström, Henrik och Brun, Hans (red): *Antagonistiska hot och dess påverkan på lokalsamhället. En antologi*, Försvarshögskolan 2019.
9. Merkel, Angela: *Frihet: Minnen 1954–2021*, Albert Bonniers Förlag 2024, s 431.
10. Europeiska kommissionen och Europeiska utrikestjänsten: ”Gemensamt Meddelande till Europaparlamentet och Rådet: Gemensam Ram För Att Motverka Hybridhot”, Bryssel 2016, *https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018*, (2025-02-03).
11. Spoofing (av engelskans *spoof*, parodi som intill förväxling liknar förebild) innebär att förfalskad eller lånad identitet på internet eller via telefoni används i bedrägligt syfte. Spoofing av satellitsignaler innebär att ”falsk” information skickas till en mottagare. Falsk data skickas till satelliter som i sin tur skickar felaktiga positioneringssignaler till exempelvis flygplan. Ryska väpnade styrkor har ett brett spektrum av militär utrustning avsedd för GNSS-störning (Global Navigation Satellite Systems).
12. Niinistö, Sauli: *Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness*, report to European Commission, okt 2024, *https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf*, (2025-03-29), s 102.
13. Ibid.
14. Oksanen, Patrik: *Rysslands hemliga krig mot Sverige*, Volante, Falun 2025, s 28.
15. *European Preparedness Union Strategy*, European Commission, 2025-02-26, *https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin*, (2025-03-28).
16. FIMI – Foreign Information Manipulation and Interference.
17. *European Preparedness Union Strategy*, s 12.
18. Giannopoulos, Georgios; Smith, Hanna och Theocharidou, Marianthi (red): *The landscape of Hybrid Threats: A Conceptual Model (Public Version)*, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, s 17.
19. Ibid, s 33.
20. Thiele, Ralph D och Schmid, Johann: ”Hybrid Warfare – Orchestrating the Technology Revolution”, *ISPSW Strategy Series: Focus on Defense and International Security*, nr 663, Berlin 2020, *https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf*, (2025-03-27).
21. Giannopoulos, Smith, och Theocharidou, *The landscape of Hybrid Threats: A Conceptual Model (Public Version)*, s 22.
22. Rauta, Vladimir: ”Countering state-sponsored proxies: Designing a robust policy”, *Hybrid CoE Paper 23*, feb 2025, s 12.
23. Almén, Oskar; Malmlöf Tomas och Lusua, Jens: *Ryska investeringar och ekonomiska intressen i Sverige*, Försvarets forskningsinstitut (FOI), FOI-5377-SE, 2022.
24. *The changing DNA of serious and organised crime*, Europol, *https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf*, (2025-03-20)
25. Ibid, s 88.
26. Ibid, s 14.
27. Rauta, ”Countering state-sponsored proxies: Designing a robust policy”, s 7.

28. *The changing DNA of serious and organised crime*, s 15.
29. Ibid, s 15.
30. Nylén, ”Förändrad sårbarhet i en tid av oro”, s 11 resp 220.
31. Europaparlamentets och rådets förordning (EU) 2024/1359 av den 14 maj 2024 om hantering av kris- och force majeure-situationer på migrations- och asylområdet och om ändring av förordning (EU) 2021/1147, *https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202401359*, (2025-03-30)
32. *The changing DNA of serious and organised crime*, s 15.
33. Hedberg, Sofia: ”Bröder dömda för terrorplaner mot svenska kyrkan”, *SVT Nyheter*, 2023-12-19, *https://www.svt.se/nyheter/utrikes/broder-domda-for-terrorplaner-mot-svensk-kyrka*, (2024-08-16).
34. ”Omvärldens reaktioner på koranbränningar i Sverige sommaren 2023”, *Svenska institutet*, *https://si.se/omvarldens-reaktioner-pa-koranbranningar-i-sverige-sommaren-2023/*, (2024-08-13).
35. Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, s 105.
36. Rauta, ”Countering state-sponsored proxies: Designing a robust policy”, s 7.
37. ”Översyn av underrättelseverksamheten”, Regeringen, Kommittédirektiv 2023:150.