

# BROTTETS IMPERIUM

STATEN OCH SKUGGAN I DEN RYSKA HISTORIEN



RYSK ORGANISERAD BROTTSLIGHET  
SOM STATLIGT VERKTYG

**1500–2025**

*”DET ÄR STRUKTUREN SOM UTGÖR HOTET –  
INTE INDIVIDEN”*



TEXT OCH ANALYS:

JÖRGEN HOLMLUND & THOMAS AHLERUP

## Förord

Den organiserade brottslighet som uppstod i Ryssland efter Sovjetunionens fall, hade sina rötter i en specifik sovjetisk kriminell struktur, som fick ett ekonomiskt grepp om hela det ryska samhället under 1990-talet. Statsmakten hade små resurser att bekämpa detta maffiasamhälle, som i stället gradvis trängde in i både i politiken och rättsmaskineriet. Sedan början av 2000-talet, den tid då Ryssland styrts av Vladimir Putin och hans närmaste krets, med starka rötter i säkerhetstjänstens olika grenar, har gränsen mellan statsmakten och den organiserade brottsligheten alltmer suddats ut.

Följden är att den organiserade brottsligheten, utöver att tjäna pengar med osunda metoder, allt oftare används för den ryska statens intressen. Den medverkar aktivt till kringgående av sanktioner, genom smuggling och penningtvätt, den agerar som ett instrument för utpressning, påverkan, infiltration och destabilisering - även utanför Rysslands gränser. Den kan idag knytas direkt till den ryska statens geopolitiska intressen. Att underskatta kopplingen mellan organiserad brottslighet och makten i Kreml vore ett strategiskt misstag.

För Sverige och andra europeiska demokratier innebär detta en ny typ av säkerhetsutmaning. Den måste förstås både som ett polisiärt problem och en fråga om nationell säkerhet. Denna rapport bidrar i det sammanhanget med viktig kunskap. Genom att synliggöra strukturer, nätverk och metoder stärker den möjligheten att möta de olika hoten med större precision och bättre samordning.

I en tid av öppet pågående hybridkrig, där kriminalitet och ekonomisk infiltration är en del av hotbilden, är ökad förståelse i sig ett försvarsvapen. Den stärker det svenska rättssamhället, förbättrar motståndskraften mot otillbörlig påverkan och bidrar till Sveriges säkerhet som nation.

*Malcolm Dixelius,*

författare till böckerna "Rysslands undre värld" och "Maffians Ryssland"

## INNEHÅLLSFÖRTECKNING

| <u>Kapitel</u> |   | <u>Sida</u> |
|----------------|---|-------------|
|                | EXECUTIVE SUMMARY   | 4           |
| 1              | INLEDNING: STAT OCH BROTT I SYMBIOS   | 6           |
| 2              | METOD, KÄLLOR OCH ANALYTISK RAM   | 14          |
| 3              | FRÅN VÅLDSSTAT TILL TVÅNGSSYSTEM  | 21          |
| 4              | DEN SVARTA EKONOMIN, BLAT OCH SÄKERHETSAPPARATEN (1953–1991)                              | 24          |
| 5              | SYSTEMKOLLAPS OCH HYBRIDISERING (1991–2000)   | 29          |
| 6              | PUTINSYSTEMET: DEN INSTITUTIONALISERADE SKUGGAN (2000–2014)                               | 34          |
| 7              | HYBRIDKRIGFÖRING SOM PERMANENT TILLSTÅND (2014–2025)                                      | 38          |
| 8              | EXEMPEL: ROSNEFT, GAZPROM OCH ROSTEC  | 43          |
| 9              | KOPPLING TILL TOTALFÖRSVARET OCH KRITISK INFRASTRUKTUR (SVERIGE/EU)                       | 52          |
| 10             | SVERIGESPECIFIK HOTPRIORITERING – TOPP 10 (PMESII/HYBRID)                                 | 61          |
| 11             | SVERIGE I FOKUS: TRE MARKNADER FÖR PÅVERKAN   | 68          |
| 12             | STRATEGISKA IMPLIKATIONER FÖR SVERIGE OCH EUROPA  | 72          |
|                | AVSLUTANDE ANALYS, SAMMANFATTNING OCH REKOMMENDATION                                      | 75          |
|                | BEDÖMNING AVSEENDE FÖREKOMST AV RYSK BROTTSLIGHET MED KOPPLING TILL TRE SVENSKA RÄTTSFALL | 77          |
|                | REFERENSER OCH LITTERATUR   | 81          |

## EXECUTIVE SUMMARY

*Rysk statstjänande kriminalitet, hybridpåverkan och systemhot mot Sverige*

### Inledning

Denna rapport analyserar hur rysk organiserad brottslighet historiskt har utvecklats från informell överlevnadsstruktur till statligt användbar metod. Utgångspunkten är att kriminalitet i rysk kontext inte enbart ska förstås som ett avvikande fenomen vid sidan av staten, utan som en återkommande funktion i statens sätt att utöva makt.

I västerländsk analys betraktas organiserad brottslighet ofta som ett tecken på statligt misslyckande. I rysk historisk kontext är relationen mer komplex. Under olika epoker har informella och kriminella strukturer fungerat som ersättning för svaga institutioner, som smörjmedel i dysfunktionella system och som verktyg för en starkare stat när makten återcentraliserats.

*Rapportens centrala slutsats är därför att kriminalitet i rysk kontext inte bara är ett ordningsproblem. Den kan också vara en metod.*

Denna historiska logik får särskild betydelse efter 2014. Annekteringen av Krim och kriget mot Ukraina markerar en strategisk brytpunkt där den ryska symbiosmodellen i allt högre grad projiceras utåt mot Europa. Cyberoperationer, informationspåverkan, ekonomisk infiltration, sanktionsundandragande, energiberoenden, penningtvätt, kriminella intermediärer och gråzonsoperationer fungerar inte som separata fenomen, utan som delar av ett bredare system.

För Sverige innebär detta att hotet inte enbart finns i militära scenarier. Det uppträder i vardagliga strukturer: bolag, avtal, kapitalflöden, leverantörskedjor, upphandlingar, informationsmiljöer, IT-system, hamnar, energi och kommunal infrastruktur.

*”Det är strukturen som utgör hotet – inte individen”*

Hotet ligger inte i varje enskild affär, transaktion, kabelincident, cyberintrång eller påverkanstext. Det ligger i den ackumulerade effekten när många små, ofta förnekbara handlingar samverkar över tid och skapar strategisk påverkan.

Sveriges sårbarhet ligger samtidigt i något som i grunden är en styrka: öppenhet, tillit, regelstyrning och decentraliserat ansvar. Dessa egenskaper gör det svenska samhället effektivt i fredstid, men kan utnyttjas av aktörer som verkar genom juridiska gråzoner, formellt legitima strukturer och indirekta mellanhänder.

För att möta denna typ av hot krävs ett perspektivskifte. Sverige behöver gå från reaktiv incidenthantering till proaktiv systemförståelse. Det innebär att näringsliv, finanssektor, offentlig sektor, kommuner, säkerhetsmyndigheter och totalförsvaret måste se dessa risker som sammanhängande – inte som isolerade problem.

Motståndskraft byggs inte enbart genom fler regler. Den byggs genom bättre förmåga att se mönster, förstå beroenden, identifiera svaga signaler och agera innan strukturerna blivit strategiska sårbarheter.

Stockholm maj 2026

*Författarna*

*Jörgen Holmlund & Thomas Ahlerup*

*Redaktör: Mikael R. Hylin*

## KAPITEL 1 – INLEDNING: STAT OCH BROTT I SYMBIOS

*Det är strukturen som utgör hotet – inte individen*

Ryssland utmanar i dag Europas och Sveriges säkerhet genom en kombination av militära, ekonomiska och informella metoder som går långt utöver traditionell säkerhetspolitik. För att förstå detta agerande räcker det inte att analysera den formella staten. Det krävs ett längre historiskt perspektiv där staten och den organiserade brottsligheten betraktas som sammanflätade snarare än som varandras motsatser.

I fem sekler har den ryska staten utvecklats i nära symbios med informella nätverk, våldsstrukturer och parallella ekonomier. Organiserad brottslighet har inte varit ett avvikande fenomen vid sidan av staten, utan har återkommande fungerat som reservkapacitet, komplement eller ersättning för formella institutioner. Detta mönster är äldre än Sovjetunionen, äldre än tsardömet i dess sena form, och fortsätter att prägla dagens ryska politiska och ekonomiska system.

I samhällen där staten ofta varit stark i centrum men svag i periferin, och där rättsstatliga institutioner saknat förtroende och kontinuitet, har befolkningen utvecklat parallella system för trygghet, ordning och resursfördelning. Dessa informella strukturer – från lokala skyddsnät och kriminella hierarkier till skuggekonomier – har inte bara samexisterat med staten, utan i många perioder varit nödvändiga för dess funktion.

Rapportens grundläggande utgångspunkt är därför att brottslighet i rysk kontext inte bör förstås som ett sammanbrott av ordning, utan som en återkommande funktion i statens sätt att utöva makt.

Den centrala insikten kan sammanfattas i tre historiskt återkommande funktioner:

1. när staten är svag fyller brottsligheten tomrummet,
2. när staten är ineffektiv fungerar informella ekonomier som smörjmedel,
3. när staten är stark absorberas brottets strukturer och används som politiskt verktyg.

Organiserad brottslighet i Ryssland utgör därmed inte en parallell värld vid sidan av staten, utan är integrerad i statens styrningslogik. Det är denna logik som, i modern tappning, formar den ryska maktmodell som i dag används både inrikes och utrikes.

I dagens geopolitiska landskap blir detta särskilt tydligt. Rysslands användning av energiresurser, ägarstrukturer, cyberoperationer, kriminella mellanled, paramilitära aktörer och informationspåverkan kan inte analyseras var för sig. De är komponenter i en hybridiserad maktmodell där statens formella institutioner samverkar med informella nätverk – ofta med kriminell karaktär – för att uppnå politiska, ekonomiska och strategiska mål.

Syftet med denna rapport är att visa hur detta system vuxit fram, hur det fungerar och vilka konsekvenser det får för Europa och Sverige.

### **Varför denna rapport – problemet med västerländska tolkningsramar**

Ryssland utgör i dag en av de mest komplexa säkerhetspolitiska utmaningarna för Europa. Landets agerande präglas av en kombination av militära hot, ekonomisk påtryckning, informationspåverkan och användning av informella aktörer – ofta under tröskeln för öppen konflikt. Trots detta analyseras Ryssland fortfarande ofta genom västerländska tolkningsramar som förutsätter en tydlig åtskillnad mellan stat och brott, mellan lagligt och olagligt, mellan offentligt och privat.

Denna rapport utgår från att dessa antaganden i grunden är missvisande i rysk kontext.

Inom västerländsk politisk teori ses organiserad brottslighet normalt som ett tecken på statligt misslyckande: något som uppstår där staten är svag, korrupt eller dysfunktionell. Staten och brottet betraktas som motpoler. I Ryssland har relationen historiskt sett varit en annan. Här har organiserad

brottslighet återkommande fungerat som ersättning, komplement eller verktyg för staten – inte som dess fiende.

Statsvetare och historiker som **Richard Pipes** [Penguin Random House 1974: ”*Russia Under the Old Regime*”], **Hugh Seton-Watson** [”*The Russian Empire*”] samt **Moshe Lewin** [Verso Books: ”*The Soviet Century*”] visar samstämmigt att den ryska staten utvecklats utan den institutionella kontinuitet som kännetecknar Västeuropa. I stället har makt utövats genom personliga lojaliteter, våld och informella arrangemang.

Problemet är därför inte att Ryssland ”avviker” från en norm, utan att normen i sig är fel vald. Denna rapport tar sin utgångspunkt i att rysk statsmakt måste förstås på sina egna historiska och strukturella villkor.

Rapportens analys vilar på fem grundläggande observationer:

1. den ryska statens svaga institutionella traditioner,
2. våldets roll som organiserande kraft,
3. den informella ekonomins kontinuitet,
4. säkerhetstjänsternas funktion som maktens ryggrad,
5. symbiosen mellan stat och brott över tid.

Dessa faktorer är inte moderna avvikelser, utan resultatet av flera sekler av statlig organisering. De utgör det analytiska raster genom vilket hela rapporten ska läsas.

## Den historiska huvudlinjen – stat och brott i symbios

Rapportens centrala utgångspunkt är att relationen mellan stat och organiserad brottslighet i Ryssland inte är episodisk, utan strukturell. I minst femhundra år har informella våldsaktörer, skuggekonomier och kriminella nätverk återkommande fyllt funktioner som staten själv inte kunnat eller velat upprätthålla.

Detta mönster kan spåras från tsartidens ”*razboyniki*”<sup>1</sup> via Gulags ”*vory v zakone*”<sup>2</sup>. Sovjetunionens informella ekonomi och 1990-talets maffia-oligark-KGB-triangel, fram till dagens paramilitära grupper, cybernätverk och gråzonsfinans. Det som förändras är formerna – inte funktionen.

Denna kontinuitet är central. Den innebär att organiserad brottslighet i Ryssland inte kan förstås som ett modernt fenomen kopplat till Sovjetunionens kollaps eller 1990-talets kaos. I stället är den en återkommande lösning på ett strukturellt problem: statens oförmåga eller ovilja att utöva makt genom stabila, rättsstatliga institutioner.

Historikern **James H. Billington** [Vintage Books 1966: ”*The Icon and the Axe: An interpretive History of Russian Culture*”] beskriver hur rysk politisk kultur präglats av en grundläggande misstro mot formella institutioner och en parallell tilltro till personliga nätverk. Denna kultur har gjort informella strukturer både legitima och funktionella över tid.

Rapportens grundtes är därför enkel men långtgående:

- *I Ryssland är brottslighet inte ett sammanbrott av ordning – det är en metod för ordning.*

### Huvudtes

Rapportens centrala tes, utvecklad av författarna, är att – den ryska staten inte i första hand bekämpar organiserad brottslighet – den använder den.

I västerländsk analys betraktas kriminalitet och statsmakt som motpoler. I den ryska kontexten är gränsen mellan dem porös. Staten tolererar, absorberar eller aktiverar kriminella strukturer när det är funktionellt för maktutövningen.

Huvudtesen sammanfattas i tre grundprinciper:

- a. när staten är svag fyller brottsligheten vakuumet,
- b. när staten stärks integreras brottets strukturer,
- c. brottslighet i Ryssland är ett styrningsverktyg, inte ett sammanbrott.

Från tsartidens ” *razboyniki*” via Gulags *vory v zakone*” till dagens paramilitära och ekonomiska nätverk återkommer samma struktur. Aktörerna förändras, men logiken består.

---

1 ”Rövare” - Begreppet har en lång historisk laddning i rysk historia och kultur. Det användes redan under tsartiden om väpnade grupper som opererade utanför statens kontroll

2 ”Tjuvar i lagen” - Det är inte bara ett vanligt kriminellt nätverk utan en historisk, hierarkisk och nästan kastliknande elit inom den postsovietiska organiserade brottsligheten

## Rapportens syfte och målgrupper

Rapportens syfte är att ge beslutsfattare inom näringsliv – stat och kommun, analytiker och säkerhetsfunktioner en sammanhängande ram för att förstå hur den ryska staten använder informella aktörer och nätverk som en del av sin maktutövning.

Fokus ligger inte på brottslighet i traditionell kriminologisk mening, utan på hur kriminalitet, gråzonsekonomi och informella strukturer används som verktyg i statens styrning – både inrikes och utrikes.

Rapporten ska särskilt bidra till svensk riskanalys inom områden som:

- a. ägarstrukturer och företagskontroll,
- b. kapitalflöden och finansiella nätverk,
- c. logistiska beroenden,
- d. cyber- och informationsmiljöer,
- e. strukturell påverkan i gråzon mellan lagligt och olagligt.

Den avgörande poängen är att dessa fenomen inte är fristående. De är delar av ett sammanhängande system. Först när de analyseras i sin helhet blir riskbilden begriplig.

## Tre funktioner av brott i rysk statsutövning

För att göra denna tes analytiskt användbar identifierar rapporten tre återkommande funktioner som organiserad brottslighet fyller i rysk historia. Dessa funktioner är inte tidsbundna till specifika regimer, utan återkommer när strukturella förutsättningar sammanfaller.

### För det första:

- När staten är svag eller frånvarande fyller brottsliga och informella aktörer ett ordningsvakuum. De erbjuder skydd, konfliktlösning, resursfördelning och ibland rättskipning. Detta är tydligt i tsartidens periferi, i inbördeskrigets kaos och under 1990-talets kollaps.

### För det andra:

- När staten är ineffektiv fungerar informella ekonomier och kriminella nätverk som smörjmedel. De möjliggör distribution, produktion och logistik där den formella ekonomin misslyckas. Detta mönster är centralt under Sovjetunionens bristsamhälle, där ”Blat” – ett centralt begrepp i sovjetisk och rysk samhällsstruktur och betyder ungefär informella kontakter, nätverkstjänster, gentjänster, tillgång genom relationer snarare än formella regler. Det kan beskrivas som: ett parallellt informellt system för tillgång, inflytande och resurser. Under Sovjettiden var ekonomin kroniskt ineffektiv därför blev personliga nätverk ofta viktigare än formella institutioner.

### För det tredje:

- När staten är stark och centraliserad absorberas brottets strukturer och används som verktyg. Våld outsourcas, kapital döljs, sanktioner kringgås och påverkan sker genom aktörer som formellt står utanför staten men funktionellt tjänar den.

Dessa tre funktioner utgör rapportens analytiska ryggrad och återkommer genom samtliga historiska kapitel.

### Mål och syfte med rapporten

Det är avgörande att tydligt definiera vad denna rapport är – och lika viktigt, vad den inte är. Denna avgränsning är inte en redaktionell formalitet utan en nödvändig metodologisk förutsättning för att analysen ska vara begriplig, användbar och hållbar i ett säkerhetspolitiskt och akademiskt sammanhang.

Rapporten är inte en studie av organiserad brottslighet i kriminologisk mening. Den har inte som syfte att kartlägga brottsnätverk, identifiera gärningsmän, klassificera brottstyper eller föreslå brottsbekämpande åtgärder. En sådan ansats förutsätter ett rättsstatligt ramverk där kriminalitet utgör ett avvikande fenomen vid sidan av staten, och där staten i grunden står i ett antagonistiskt förhållande till brottsliga aktörer. Denna grundförutsättning är inte tillämplig i rysk kontext.

I Ryssland har organiserad brottslighet historiskt inte primärt varit ett uttryck för statens misslyckande, utan ett alternativt – och ofta funktionellt – sätt att organisera makt, resurser och våld. I vissa perioder har informella och brottsliga strukturer vuxit fram i statens frånvaro; i andra perioder har de integrerats i statens funktionssätt och använts som verktyg för styrning. Detta innebär att kriminalitet inte kan analyseras isolerat från staten, utan måste förstås som en del av statens styrningsrepertoar och maktutövning.

Forskning inom statsteori och säkerhetsstudier ger ett tydligt stöd för denna ansats. **Joel S. Migdal** [Princeton University Press 1988: ”*Strong Societies and Weak States: State – Society Relations and State Capabilities in The Third World*”] visar hur stater med svaga eller fragmenterade institutioner ofta styr genom informella arrangemang snarare än genom lag, byråkrati och transparent förvaltning. I sådana system blir våldsaktörer, kriminella nätverk och ekonomiska gråzoner inte undantag, utan funktionella komponenter i statens maktutövning.

På liknande sätt beskriver **James C. Scott** [Yale University Press 1998: ”*Seeing Like a State: How Certain Schemes to Improve the Human Condition have Failed*”] hur staten tenderar att förenkla komplexa samhällen i sina formella modeller, men i praktiken ofta blir beroende av just de informella strukturer den officiellt söker eliminera. I rysk kontext har detta beroende blivit strukturellt, långvarigt och systembärande.

## **Avgränsningar, syfte och metodologisk disciplin – från kriminalitet till statlig metod vad rapporten gör och inte gör**

Mot denna bakgrund är rapportens syfte inte att analysera vad kriminalitet är, utan att beskriva hur kriminalitet används. Fokus ligger på funktion snarare än normativ klassificering. Det centrala analytiska objektet är inte det enskilda brottnätverket, utan det system som gör brottnätverk, gråzonsaktörer och informella ekonomier användbara för statlig maktutövning – både inrikes och utrikes.

Detta placerar rapporten tydligt utanför traditionell brottsforskning och inom ett annat analytiskt fält. Den utgör i första hand ett bidrag till strategiska studier, säkerhetspolitisk analys samt statlig och institutionell teori, med särskild relevans för studier av hybridkrigföring och gråzonsmakt. I detta perspektiv blir organiserad brottslighet ett av flera verktyg – vid sidan av ekonomiska flöden, informationspåverkan, juridisk manipulation och militär kapacitet – som används för att skapa politisk, ekonomisk och geopolitisk effekt.

För Sverige och Europa är detta perspektiv avgörande. Rysk påverkan manifesteras sällan som öppna brott eller direkta hot. Den uppträder i stället som strukturell närvaro: genom ägande, kapitalflöden, logistiska beroenden, rättsliga gråzoner och informella mellanhänder. Utan en analys som betraktar kriminalitet som metod snarare än avvikelser riskerar dessa mönster att förbli osynliga, eller att feltolkas som isolerade och icke-strategiska fenomen.

För att analysen ska vara både analytiskt och rättsligt hållbar är den inspirerad av etablerade arbetssätt inom strategiska studier, försvarsanalys, underrättelsenära öppna källor och säkerhetspolitisk systemanalys. Den är konsekvent systemisk och strukturell, inte personbaserad. Den gör inga spekulationer om enskilda och innehåller inga operativa utpekanden. Analysen rör inte skuld, ansvar eller brottslighet hos namngivna aktörer, utan fokuserar på institutionella mönster, historisk kontinuitet och dokumenterade nätverkslogiker.

### **Analysens räckvidd**

Denna avgränsning är inte en begränsning av analysens räckvidd, utan en förutsättning för dess precision. I den ryska modellen används informella ekonomier för strategiska syften; brottsliga och gråzonsaktörer fungerar som statens operativa mellanled; kapitalflöden, ägarstrukturer och logistik blir geopolitisk hävstång; och staten utnyttjar nätverkens flexibilitet för att uppnå effekter som formella institutioner inte kan leverera. Det är denna mekanism som utgör kärnan i den symbios mellan stat och brott som rapporten analyserar.

Rapportens konsekventa fokus på strukturer snarare än individer är därför inte bara etiskt eller juridiskt motiverat, utan analytiskt nödvändigt. I västerländsk analys finns en stark tendens att personifiera hot genom att identifiera ”nyckelpersoner”, ”ledargestalter” eller ”huvudansvariga”. Denna logik är rationell i rättsliga sammanhang men djupt problematisk i analys av system där makt är nätverksbaserad, distribuerad och funktionell. I den ryska modellen är individer i regel utbytbara; det är rollerna och funktionerna som består. Ett

individfokus riskerar därför att skapa en illusion av förändring där det i själva verket råder kontinuitet.

Forskning om organiserad brottslighet i statliga gråzoner, exempelvis publicerad av **Mats Berdal och Monica Serrano** [Lynne Rienner Publishers 2002: ”*Global Organized Crime and International Security*”] visar att när kriminella strukturer är integrerade i statliga system blir det analytiskt missvisande att betrakta dem som autonoma organisationer. De fungerar snarare som operativa moduler inom ett större maktsystem.

Mot denna bakgrund gör rapporten medvetet följande avgränsningar: den analyserar inte enskilda svenska individer eller företag; den drar inga referenser om juridisk skuld baserat på strukturella samband; den blandar inte underrättelseindikationer med beviskrav; och den pekar inte ut aktörer utan rättslig prövning. Dessa avgränsningar skyddar inte bara individer – de skyddar analysens integritet och säkerställer att fokus förblir på hur system fungerar, snarare än på moraliska eller politiska bedömningar av enskilda aktörer.

### **Den grundläggande principen är därför enkel och genomgående för hela rapporten:**

Detta innebär också att rapporten är placerad inom ett annat analytiskt fält än traditionell brottsforskning. Den är i första hand ett bidrag till:

- strategiska studier
- säkerhetspolitisk analys
- statsteori och institutionsanalys
- studier av hybridkrigföring och gråzonsmakt

För att vara analytiskt och rättsligt hållbar ansluter rapporten till etablerade arbetssätt inom strategiska studier, försvarsanalys, underrättelsenära öppna källor och säkerhetspolitisk systemanalys, och avgränsar sig tydligt från spekulationer om enskilda individer eller företag. Analysen är systemisk och strukturell, inte personbaserad.

### **Rapporten innehåller därför:**

- **inga** uttalanden om svenska individer,
- **inga** spekulativa kopplingar,
- **inga** antydningar om kriminalitet hos icke namngivna aktörer,
- **inget** operativt utpekande.

### **Mot denna bakgrund gör rapporten följande avgränsningar:**

- den analyserar **inte** enskilda svenska individer eller företag
- den gör **inga** inferenser om juridisk skuld baserat på strukturella samband

- den blandar **inte** underrättelseindikationer med beviskrav
- den pekar **inte** ut aktörer utan rättslig prövning

Detta ligger i linje med etablerade arbetssätt inom strategiska studier, försvarsanalys, underrättelsenära öppna källor och säkerhetspolitisk systemanalys. Syftet är inte att peka ut skyldiga, utan att identifiera risker, mönster och mekanismer som är relevanta för nationell och europeisk säkerhet.

Den grundläggande principen är därför enkel – *det är strukturen som utgör hotet – inte individen.*

### **Rapportens struktur, läsanvisning och analytiska progression**

Rapportens struktur är medvetet utformad för att leda läsaren från teoretisk förståelse till strategisk tillämpning. Den ska inte läsas som en kronologisk historiebeteckning i traditionell mening, utan som en successiv uppbyggnad av en analysmodell.

Rapporten i sin helhet bör läsas från början till slut. Varje kapitel bygger vidare på det föregående. Kapitel 1 etablerar den begreppsliga och analytiska ramen. De efterföljande kapitlen visar hur modellen konkretiseras historiskt och hur den, i modern form, påverkar Europa och Sverige.

Detta innebär att de historiska kapitlen inte ska betraktas som bakgrundsmaterial i perifer mening. De fungerar som empiriska belegg för modellens giltighet. När samma logik återkommer över fem sekler – trots radikalt skilda politiska system – utgör det ett starkt argument för att det handlar om struktur snarare än tillfällighet.

Läsaren bör därför betrakta denna inledning som en instruktionsmanual för hur rapporten ska förstås. Utan denna analytiska ram riskerar rysk organiserad brottslighet, korrupktion, hybridkrigsföring och ekonomisk påverkan att framstå som separata fenomen. Med ramen framträder de i stället som delar av ett sammanhängande system.

Det är först då som rapportens slutsats blir tydlig – och obekvämt:

I Ryssland är brottsligheten inte statens skugga; den är en del av statens infrastruktur.

## KAPITEL 2 – METOD, KÄLLOR OCH ANALYTISK RAM

### *Hur informell makt analyseras i en hybridstat*

#### **Metodologisk utgångspunkt – systemanalys av hybridstat**

Att analysera rysk organiserad brottslighet som ett kriminalpolitiskt problem är metodologiskt otillräckligt. Det förutsätter en västerländsk separation mellan stat och brott som inte existerar i den ryska kontexten. I Ryssland är organiserad brottslighet inte ett externt hot mot staten, utan en del av dess historiska funktionssätt. Detta kräver en analys som betraktar brottslighet, informella nätverk och statlig makt som samverkande systemkomponenter.

Denna rapport utgår därför från ett systemperspektiv, snarare än ett aktörs- eller händelseperspektiv. Metodologiskt innebär detta att fokus ligger på funktion, struktur och kontinuitet, snarare än på enskilda personer eller isolerade brott. En sådan ansats ligger i linje med den institutionella statsvetenskapen och modern säkerhetsanalys, snarare än klassisk kriminologi.

**Joel S. Migdal** [Princeton University Press 1988:”*Strong Societies and Weak States: State – Society Relations and State Capabilities in The Third World*”] och **James C. Scott** [Yale University Press 1998:”*Seeing Like a State: How Certain Schemes to Improve the Human Condition have Failed*”] visar hur stater med svaga institutioner ofta förlitar sig på informella maktstrukturer för att uppnå kontroll. I dessa system är gränsen mellan lagligt och olagligt mindre relevant än frågan om funktionalitet. Det avgörande är inte om en aktör är formellt statlig, utan om den bidrar till regimens stabilitet och handlingsfrihet.

Den ryska staten har historiskt utvecklats genom just denna logik. När formella institutioner varit otillräckliga har staten tolererat, utnyttjat eller absorberat informella strukturer. Detta gäller både ekonomiska nätverk, våldsaktörer och säkerhetstjänstrelaterade skuggsystem. Att analysera dessa fenomen isolerat leder därför till fragmenterade och ofta missvisande slutsatser.

#### **Rapportens metod bygger därför på tre övergripande principer:**

1. **Systemisk analys** – staten betraktas som ett ekosystem av formella och informella komponenter.
2. **Historisk kontinuitet** – nutida fenomen förstås som uttryck för långsiktiga mönster.
3. **Funktion före juridik** – analysen fokuserar på vad strukturer gör, inte hur de klassificeras rättsligt.

Denna metodologiska hållning är avgörande för att förstå varför rysk organiserad brottslighet inte kan reduceras till ett ordningsproblem, utan måste analyseras som ett styrningsverktyg i en hybridstat.

## Källmaterial, triangulering och begränsningar

Rapporten bygger uteslutande på öppna källor, men använder dem på ett sätt som speglar underrättelse- och säkerhetspolitisk analys snarare än traditionell akademisk monografi. Ingen enskild typ av källa är tillräcklig för att förstå ett system där stat, brott och ekonomi är sammanflätade. Därför krävs källbredd och triangulering. Läsreferenser för de källor som används och förslag på litteratur för fördjupade studier återfinns i slutet av rapporten.

### Källmaterialet omfattar fem huvudsakliga kategorier:

1. **Akademisk forskning och historiska verk**, särskilt inom rysk historia, statsteori och informell ekonomi. Centrala referenser inkluderar **Richard Pipes** [Penguin Random House 1974: ”*Russia Under the Old Regime*”], **Hugh Seton-Watson** [”*The Russian Empire*”] samt **Moshe Lewin** [Verso Books: ”*The Soviet Century*”]
2. **Säkerhetspolitiska analyser** från FOI, MCF – Myndigheten för civilt försvar (tidigare MSB), NATO och EU-institutioner, där rysk hybridpåverkan, gråzonsoperationer och ekonomisk krigföring behandlas.
3. **Underrättelsenära öppna källor**, inklusive rapporter från europeiska säkerhetstjänster och ”Think tanks” som analyserar ryska nätverk och påverkan.
4. **Ekonomiska data och rättsfall**, särskilt rörande penningtvätt, ägarstrukturer och kapitalflöden. Svenska domar, däribland Södertörns Tingsrätt B 13688–25, används som empiriska exempel på hur internationella nätverk kan operera genom legala bolagsstrukturer.
5. **Kvalificerad journalistik**, exempelvis granskningar av internationella finansflöden, oligarkstrukturer och säkerhetstjänstkopplingar som till exempel Acta Publicas rapport [2025:01 – ”Ryska Intressen – en fördjupad studie av svenska bolag med rysk koppling”]

Metodologiskt är det avgörande att dessa källor inte används isolerat. Rysk officiell statistik hanteras med hög skepsis. Journalistik används inte som bevis i sig, utan som indikator. Underrättelserapporter betraktas som hypotesgenererande snarare än slutgiltiga.

Det är först när flera oberoende källor – med olika incitament och ursprung – pekar i samma riktning som slutsatser dras. Detta följer klassisk trianguleringsprincip inom säkerhetsstudier och underrättelseanalys.

### Källkritik och rysk ”maskirovka”

Analys av ryska förhållanden innebär särskilda källkritiska risker. Den ryska staten använder aktivt desinformation, selektiv transparens och vad som i rysk militärdoktrin

benämns ”*maskirovka*” – vilseledning som strategiskt verktyg. Detta påverkar inte bara rysk intern information, utan även västerländska analyser.

**Ofer Fridman** [Oxford University Press 2018: ”*Russian 'Hybrid Warfare': Resurgence and Politicization*”] och **Agnia Grigas** [Yale University Press 2016: ”*The New Russian Empire*”] och visar hur informationspåverkan inte är ett tillägg till rysk strategi, utan en integrerad del av den. Detta innebär att även öppna källor kan vara kontaminerade av avsiktlig vilseledning.

#### De huvudsakliga riskerna är:

- politiserad statistik,
- underrättelserapporter med begränsad verifierbarhet,
- återcirkulering av obekräftade uppgifter,
- västerländsk projektion av egna institutionella antaganden på rysk verklighet.

För att hantera detta arbetar rapporten konsekvent med negativ kapabilitet: frånvaro av bevis tolkas inte som bevis på frånvaro. Analysen är därför medvetet försiktig i kausala påståenden, men tydlig i strukturella mönster.

#### Juridiska och etiska avgränsningar – varför strukturer, inte individer, är analysens kärna

En av rapportens mest avgörande metodologiska utgångspunkter är dess konsekventa avgränsning bort från individbaserad analys. Detta är inte en fråga om juridisk försiktighet eller redaktionell neutralitet, utan en grundläggande vetenskaplig nödvändighet. I analyser av system där statlig makt, informella nätverk och kriminella strukturer samverkar riskerar individfokus att både förvanska analysen och dölja de mekanismer som faktiskt skapar strategisk effekt.

Inom västerländsk rättsstatlig tradition är det naturligt att söka ansvar, kausalitet och skuld hos individer. Denna logik är central i juridiska sammanhang men blir metodologiskt problematisk i strukturell säkerhetsanalys. Som **James C. Scott** [Yale University Press 1998: ”*Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*”] påpekar tenderar staten – och analytikern – att förenkla komplexa sociala system genom att reducera dem till hanterbara enheter. I rysk kontext leder detta ofta till felaktiga slutsatser, eftersom maktutövningen inte primärt är individualiserad utan nätverksbaserad.

I den ryska modellen är individer i regel utbytbara. Det är funktionerna – våldskapacitet, tillgång till kapital, kontroll över logistik, informationsdominans och lojalitetsförmedling – som är konstanta. När en individ faller bort ersätts denne snabbt av en annan som fyller samma roll i nätverket. Ett individfokus riskerar därför att skapa en illusion av förändring där det i själva verket råder kontinuitet.

Forskning om organiserad brottslighet i hybridstater, exempelvis visar **Monica Serrano** [Lynne Rienner Publishers 2002: ”*Global Organized Crime and International Security*”], att kriminella strukturer som är integrerade i statliga system inte fungerar enligt personcentrerade hierarkier, utan som adaptiva nätverk. Att analysera dem genom att identifiera ”ledare” eller ”nyckelpersoner” är därför ofta analytiskt missvisande.

Detta gäller i ännu högre grad när kriminella strukturer fungerar som statliga verktyg snarare än autonoma aktörer. I sådana fall är individen sällan den primära beslutsfattaren; denne är snarare en bärare av statens behov. Rapportens fokus på strukturer, mönster och logiker syftar därför till att synliggöra hur systemet producerar effekt, inte vem som råkar befinna sig i dess centrum vid en given tidpunkt.

Den juridiska avgränsningen fyller här en dubbel funktion. För det första säkerställer den att rapporten inte gör ogrundade eller spekulativa påståenden om enskilda personer eller företag, särskilt i svensk kontext. För det andra skyddar den analysens vetenskapliga integritet. Att peka ut individer utan rättslig prövning riskerar att förskjuta fokus från strukturell förståelse till moralisk eller politisk polemik.

Avgränsningen innebär därför att rapporten:

- **inte** uttalar sig om enskilda svenska individer eller företag,
- **inte** gör inferenser om skuld baserat på strukturella samband,
- **inte** blandar juridisk skuld med säkerhetspolitisk risk,
- **inte** använder underrättelseindikationer som bevis.

I stället analyseras institutionella mönster, historisk kontinuitet och funktionella relationer mellan stat, ekonomi och informella nätverk. Detta ligger i linje med etablerad praxis inom strategiska studier och underrättelseanalys, där syftet inte är att fälla domar utan att förstå hotmiljöer.

**Joel S. Migdal** [Princeton University Press 1988: ”*Strong Societies and Weak States: State – Society Relations and State Capabilities in The Third World*”] beskriver hur stater med svaga institutioner ofta styr genom informella arrangemang snarare än genom lag. I sådana system blir det analytiskt meningslöst att skilja strikt mellan lagligt och olagligt, eftersom båda sfärerna tjänar samma överordnade mål: regimens överlevnad och handlingsfrihet.

Rapportens etiska hållning följer därför en enkel princip: det är strukturen som utgör risken, inte individen. Först när denna princip accepteras blir det möjligt att analysera rysk påverkan utan att fastna i personfixering, juridiska gråzoner eller politiserade narrativ. Detta gör analysen både mer robust och mer användbar för strategisk planering.

## PMESII som analytisk ram – från sektoranalys till systemförståelse

Den ryska statens maktutövning kan inte förstås genom sektorsvisa analyser isolerade från varandra. Militär styrka, ekonomiska flöden, informationspåverkan och kriminella nätverk fungerar inte som separata verktyg, utan som integrerade komponenter i ett sammanhängande system. PMESII-ramverket (**Political, Military, Economic, Social, Information, Infrastructure**) används i denna rapport för att synliggöra just denna systemintegration.

PMESII har sitt ursprung i militär och strategisk analys, men dess verkliga styrka ligger i dess förmåga att bryta ned komplexa samhällen i analytiskt hanterbara domäner utan att förlora helheten. I rysk kontext är detta avgörande, eftersom maktutövningen konsekvent sker domänöverskridande.

**I den politiska domänen (P)** ser vi en extrem centralisering där formella institutioner existerar, men där verklig makt utövas genom personliga lojaliteter och informella nätverk. Detta skapar ett politiskt system där beslut sällan följer formella processer, utan fattas i slutna kretsar. Denna struktur förutsätter parallella maktmedel som inte är bundna av lag eller transparens.

**I den militära domänen (M)** kompletteras reguljära styrkor av privata militära företag, paramilitära grupper och kriminella våldsaktörer. Som **Ofer Fridman** [Oxford University Press 2018: ”*Russian ‘Hybrid Warfare’: Resurgence and Politicization*”] konstaterar används dessa aktörer för att skapa militär effekt utan formellt ansvar. Våld outsourcas, men förblir statligt i funktion.

**Den ekonomiska domänen (E)** präglas av råvaruberoende, statligt kontrollerade bolag och omfattande informella kapitalflöden. Här blir organiserad brottslighet och gråzonsfinans inte avvikelser, utan nödvändiga mekanismer för att kringgå sanktioner, dölja ägande och upprätthålla internationell handlingsfrihet. Ekonomi fungerar därmed både som finansieringskälla och som vapen.

**Den sociala domänen (S)** kännetecknas av låg tillit till institutioner, demografisk stress och beroende av informella nätverk. Detta skapar en befolkning som är anpassad till parallella system och där lojalitet ofta riktas horisontellt snarare än mot staten som institution. Detta är den sociala grogrund som gör informella strukturer uthålliga.

**Informationsdomänen (I)** är i rysk strategi inte en stödjande funktion, utan ett primärt stridsfält. Desinformation, psykologiska operationer och narrativ kontroll används för att forma både inhemsk och internationell perceptionsmiljö. Informationspåverkan samverkar ofta med ekonomiska och kriminella verktyg, exempelvis genom utpressning, läckor eller komprometterande material.

**Slutligen utgör infrastrukturen (I)** både sårbarhet och hävstång. Transportnoder, energidistribution, digital infrastruktur och finansiella system kan utnyttjas för påverkan långt

under tröskeln för militär konflikt. När ägande, drift eller finansiering sker genom informella eller kriminella strukturer suddas gränsen mellan civil och säkerhetspolitisk infrastruktur ut.

PMESII gör det möjligt att se hur dessa domäner inte bara samverkar, utan förstärker varandra. Kriminella nätverk blir ekonomiska verktyg, ekonomiska beroenden blir politiska påtryckningsmedel och informationsoperationer skyddar eller möjliggör ekonomiska flöden.

För Sverige är detta perspektiv avgörande. Utan PMESII riskerar analysen att fragmenteras: ekonomi analyseras för sig, cyber för sig, organiserad brottslighet för sig. PMESII visar i stället hur dessa fenomen är delar av samma struktur och måste förstås som sådana.

I denna rapport används PMESII därför inte som checklista, utan som integrerande analysram. Den gör det möjligt att identifiera strukturella risker som är lagliga till formen men strategiska till funktionen – och därmed centrala för svensk och europeisk säkerhet.

### PMESII-analysen visar hur:

- a. **politiskt**: extrem centralisering och repression formar maktvertikalen,
- b. **militärt**: hybridkapacitet och outsourcing av våld kompletterar reguljära styrkor,
- c. **ekonomiskt**: svart ekonomi, råvarulogik och oligarkstruktur dominerar,
- d. **socialt**: demografisk kris, misstro och informella nätverk präglar samhället,
- e. **information**: propaganda, desinformation och psykologiska operationer används systematiskt,
- f. **infrastruktur**: förfall och beroenden skapar strategiska sårbarheter.

PMESII används i rapporten som förklaringsmodell, inte som teoretisk dekor. Den löper genom hela analysen.

### Varför PMESII är centralt för Sverige 2026

För Sverige är det otillräckligt att analysera hot som enbart militära eller politiska. Ryska informella nätverk verkar horisontellt över sektorsgränser och utnyttjar lagliga strukturer för strategiska syften.

PMESII-analysen synliggör svenska sårbarheter inom:

- a. **energi** – beroenden och prispåverkan,
- b. **logistik** – hamnar, transportkedjor och flaskhalsar,
- c. **fastigheter** – ägarstrukturer och finansiell sårbarhet,
- d. **cyber** – utpressning, datastöld och systemstörningar,
- e. **information** – narrativ påverkan och desinformation,
- f. **ekonomi** – kapitalflöden och råvaruberoenden.

Hoten manifesteras sällan som öppna angrepp. De uppträder som långsamma, strukturella beroenden – ofta lagliga till formen, men strategiskt farliga till funktionen.

## KAPITEL 3 – FRÅN VÅLDSSTAT TILL TVÅNGSSYSTEM

*Den historiska grundlogiken bakom rysk statstjänande kriminalitet (1500–1953)*

### **En stat stark i våld men svag i institutioner**

Den ryska statens relation till organiserad brottslighet är inte ett modernt fenomen och inte heller ett resultat av tillfälligt institutionellt sammanbrott. Den är i stället förankrad i en lång historisk utveckling där statlig makt byggts genom våld, personliga lojaliteter och informella arrangemang snarare än genom rättsstatliga institutioner. Redan från 1500-talet utvecklas Ryssland som en paradoxal våldsstat: extremt centraliserad i centrum, men administrativt svag, fragmenterad och ofta frånvarande i periferin.

Till skillnad från Västeuropa, där lokalt självstyre, domstolar och gradvis institutionaliserad rättskipning växte fram, förblev den ryska staten personifierad och godtycklig. Lagen var ett instrument för maktutövning, inte ett neutralt ramverk. För undersåten innebar detta att staten inte fungerade som garant för skydd, egendom eller förutsägbarhet. I praktiken skapade detta ett strukturellt vakuum där människor tvingades söka trygghet, ordning och konfliktlösning utanför staten.

### **”Razboyniki” och den informella ordningens legitimitet**

I detta vakuum uppstår tidiga former av organiserad brottslighet med samhällsbärande funktioner. *Razboyniki* – ofta reducerade till “rövare” i förenklad historieskrivning – var i praktiken informella våldsaktörer som i många regioner fungerade som beskyddare, rättskipare och resursfördelare. De var inte legitima i juridisk mening, men ofta legitima i funktionell och social mening.

*Razboyniki* betydelse ligger inte i deras kriminalitet som sådan, utan i den roll de spelade i ett samhälle där staten inte kunde leverera stabil ordning. De skapade förutsägbarhet genom selektivt våld och personliga lojaliteter, ofta riktat mot lokala ämbetsmän eller exploaterande eliter. I flera fall uppfattades deras våld som mer begripligt och mindre godtyckligt än statens.

Avgörande för rapportens analys är att staten periodvis tolererade dessa strukturer och senare absorberade dem när centralmakten stärktes. Brottslighet uppstod därmed inte i opposition till staten, utan som ersättning för statliga funktioner – och kunde därefter integreras i statens maktutövning. Här etableras den första versionen av den symbioslogik som kommer att präglade hela den ryska historien.

### **Revolutionen 1917 – institutionell implosion snarare än nyordning**

Revolutionen 1917 markerar inte ett brott med denna grundlogik, utan dess radikaliserings. I stället för att bygga nya stabila institutioner sker en institutionell implosion. Den provisoriska staten kollapsar, och bolsjevikernas maktövertagande sker i ett samhälle där rättsordning, förvaltning och ekonomi redan är i fritt fall.

I denna miljö blir våld, tvång och informell kontroll inte undantag utan grundläggande styrmedel. Den bolsjevikiska staten prioriterar överlevnad och kontroll framför rättsstatlig konsolidering. Juridik reduceras till ett politiskt instrument, och handlingar som i andra sammanhang skulle klassificeras som brott – konfiskationer, summariska arresteringar, extrajudiciella avrättningar – görs till legitima statliga metoder.

Det centrala analytiska skiftet sker här: staten börjar inte bara tolerera brottets metoder, utan producerar dem själv. Brottslighetens logik blir en del av statens funktionssätt.

### **Säkerhetsapparaten och den permanenta undantagsstaten**

Med inrättandet av Tjekan 1917 institutionaliseras våld utanför rättsprocesser som permanent styrningsprincip. Säkerhetsapparaten konstrueras inte för rättssäkerhet, utan för operativ effekt. Under 1920- och 1930-talen vidareutvecklas denna modell genom GPU, OGPU och slutligen NKVD, som blir navet i ett system där repression, resursfördelning och ekonomisk styrning sammanflätas.

Detta skapar vad som kan beskrivas som en permanent undantagsstat. Undantaget – möjligheten att åsidosätta lag och rätt – är inte längre ett svar på kris, utan ett normaltillstånd. Gränsen mellan lagligt och olagligt förlorar sin analytiska betydelse; det avgörande blir om en handling är funktionell för regimen mål.

Säkerhetsapparaten får därmed en dubbel roll: den skyddar regimen mot verkliga och inbillade hot, men fungerar också som administrativ motor för disciplin, mobilisering och kontroll. Våld blir inte bara repressivt utan produktivt.

### **Gulag – när repression och ekonomi smälter samman**

Kulmen på denna utveckling är Gulag-systemet. Gulag är inte enbart ett terrorinstrument utan en central ekonomisk institution. Tvångsarbete används systematiskt för att bygga infrastruktur, exploatera naturresurser och genomföra projekt i geografiskt och klimatmässigt extrema områden där frivillig arbetskraft hade varit dyr eller otillgänglig.

Tvångsekonomin bygger på en enkel men brutal logik: staten kan alltid skapa arbetskraft genom kriminalisering. Genom att vidga brottsbegreppet till att omfatta politisk avvikelse, arbetsdisciplin, spekulation och sociala kategorier produceras ett konstant inflöde av fångar. Brott blir därmed en administrativ resurs.

Ur ett strikt produktivitetperspektiv var Gulag ofta ineffektivt och slösaktigt. Men ur ett politisk-ekonomiskt perspektiv var systemet rationellt: det möjliggjorde snabb mobilisering, externisering av mänskliga kostnader och total kontroll över arbetskraften. Tvångsekonomin blev en reservmotor som staten kunde aktivera när frivilliga system inte räckte till.

### **”Vory v zakone” – kriminell ordning som funktionell modul**

I Gulags extrema miljö uppstår ”vory v zakone” som ett kodifierat kriminellt normsystem. Dessa kriminella hierarkier fungerade som parallella ordningsstrukturer som kunde upprätthålla disciplin, lösa konflikter och organisera informella flöden av varor och tjänster bland internerade.

Det paradoxala är att staten ofta tolererade eller instrumentellt använde dessa strukturer. I ett system för brutalt och omfattande för att mikro-styras fullt ut av formella institutioner blev kriminella ordningar funktionella. De bekämpades selektivt, men integrerades när de levererade stabilitet.

Här institutionaliseras den symbios som är central för rapportens övergripande tes: brottslighet är inte en extern fiende till staten, utan en modul som kan aktiveras, tolereras eller absorberas beroende på behov.

### **Tvångsekonomins sociala och institutionella arv**

Även efter Stalins död lever tvångsekonomins och Gulags logik kvar. Miljontals människor har passerat genom lägren eller levt i deras skugga. Detta formar normer om tillit, lojalitet och överlevnad. Informella nätverk, tyst kunskap och ”genvägar” normaliseras som rationella strategier i mötet med en opålitlig stat.

Samtidigt lämnar Gulag ett djupt institutionellt arv: hemlighetskultur, dubbel bokföring, parallella distributionskanaler och säkerhetsapparatens dominans. Staten vänjer sig vid att använda informella, rättslösa metoder för att uppnå mål – en vana som senare epoker anpassar snarare än överger.

### **Sammanfattning – när brottets logik blir statens infrastruktur**

Perioden 1500–1953 visar inte en serie historiska avvikelser, utan en sammanhängande utveckling där informella vålds- och brottsstrukturer först ersätter staten, därefter kompletterar den och slutligen absorberas i dess kärna. Från *razboyniki* till Gulag etableras en stabil styrningslogik: staten bekämpar brott selektivt men behåller brottets metoder som verktyg.

Detta är inte bakgrund till den moderna ryska hybridstaten – det är dess operativa manual. Den symbios mellan stat och kriminalitet som i dag projiceras utåt mot Europa har sin djupaste förklaring i denna historiska period, där brottslighet upphörde att vara ett sammanbrott av ordning och i stället blev en metod för ordning

## KAPITEL 4 – DEN SVARTA EKONOMIN, BLAT OCH SÄKERHETSAPPARATEN (1953–1991)

*Hur ett helt samhälle lär sig att fungera i gråzon – och varför det blev grunden för dagens system*

### Från massrepression till “förvaltad rädsla” – kontinuitet under ytan efter 1953

Stalins död 1953 innebar inte en återgång till legalitet och institutionell normalitet, utan en förändring i styrningens intensitet och form. Terrorn som massverktyg minskar; samtidigt består den grundläggande maktlogiken: politisk kontroll prioriteras framför rättsstat och förutsägbara spelregler. ”Av-Staliniseringen” och den gradvisa reduceringen av lägersystemet innebär att staten söker stabilitet genom mindre synlig repression, men inte genom att stärka de institutioner som i en rättsstat skulle bära upp ordning, ansvar och tillit.

Detta skapar en särskild typ av efterkrigssovjjetisk stabilitet: staten blir mer förutsägbar, men förblir i grunden opålitlig som normbärare. Medborgare och organisationer kan inte förlita sig på lagen som skydd; snarare lär man sig att lagen kan aktiveras selektivt. Resultatet blir vad man skulle kunna kalla en “förvaltad rädsla”: ett samhälle där de flesta kan leva relativt normalt så länge de håller sig inom informella toleransgränser, men där staten alltid kan ingripa om lojaliteten eller kontrollen hotas.

Denna mekanism är central för rapportens huvudlinje. I stället för att minska informell ordning driver den fram en mer sofistikerad informalisering: människor och organisationer internaliserar att systemet fungerar genom kontakter, mutor, byteshandel, “regler som kan böjas”, och att säkerhetsapparaten utgör den yttersta domaren över vad som tolereras. **Moshe Lewin** [Verso Books: 2005 ”*The Soviet Century*”] beskriver just denna kombination av stabilitet och strukturell dysfunktion som kännetecknande för den senare sovjetperioden: staten består men kan inte leverera effektivitet och innovation i den omfattning som krävs.

### Bristsamhället och den informella ekonomins normalisering

Efterkrigstidens sovjetiska ekonomi är inte bara ineffektiv; den är strukturellt oförmögen att producera korrekt information. Planekonomin kräver att center (Gosplan<sup>3</sup> och ministerier) vet vad som ska produceras, var flaskhalsar uppstår och hur konsumtionsbehov förändras. I praktiken kan center inte veta detta i realtid, särskilt i ett system där lokala chefer har incitament att manipulera rapportering för att uppfylla planer, säkra resurser eller undvika

---

<sup>3</sup> Sovjetunionens centrala statliga planeringsmyndighet och står för: ”**Gosudarstvenny Planovy Komitet**” (Statliga planeringskommittén). Myndigheten skapades 1921 och blev hjärtat i den sovjetiska planekonomin. I praktiken försökte Gosplan planera nästan hela Sovjetunionens ekonomi från centrum i Moskva.

bestraffning. Informationsbrist och felaktiga signaler leder till kroniska bristsituationer och kvalitetsproblem.

Här uppstår den “andra ekonomin” – den informella och svarta ekonomin – som en sorts korrigerande mekanism. Den fungerar inte som ett alternativ till planekonomin, utan som ett parallellt system som möjliggör att planekonomin överhuvudtaget kan upprätthålla vardagsfunktioner. Den svarta ekonomin fyller luckor i distribution, service, reservdelar, livsmedelsförsörjning och produktionskedjor. Den gör det möjligt att få tag på det som systemet enligt plan skulle leverera men inte förmår.

I en säkerhetspolitisk analys är den avgörande poängen att denna ekonomi inte är marginell. Den tränger in i fabriker, byggprojekt, sjukhus, universitet, transportsektorn och partiförvaltning. Den blir “infrastrukturell”: en uppsättning informella flöden som bär upp formella verksamheter. Detta gör att gränsen mellan stat och informell ekonomi suddas ut. Delar av staten börjar “leva av” gråzonen och delar av gråzonen börjar “arbeta för” staten.

Ekonomihistoriska och institutionsanalytiska studier visar att detta är en typisk dynamik i system där formella regler inte kan leverera funktionalitet: informella mekanismer ersätter formella, men blir sedan själva beroenden som blockerar reform. Här är **Paul Gregorys** [Cambridge University Press 2004: ”*The Political Economy of Stalinism*”] arbeten om sovjetisk ekonomistyrning relevanta som bakgrund till varför planekonomin skapar just dessa incitament.

### **Blat som institution och systemsmörjmedel**

Om den svarta ekonomin är systemets materiella parallellstruktur, är Blat dess sociala operativsystem. Blat består av personliga relationer, gentjänster, lojaliteter och förtroende i nätverk. Det avgörande är att Blat inte bara handlar om att “få tag på varor”; det är en styrningsmekanism som ersätter opålitliga institutioner med relationer. **Alena Ledeneva** [Cambridge University Press 1998: ”*Russia's Economy of Favours: Blat, Networking and Informal Exchange*”] har visat hur Blat fungerar som ett informellt distributions- och beslutssystem: vem som får tillgång till bostad, utbildning, läkemedel, resor, material, anställning eller administrativt skydd avgörs ofta mindre av formella kriterier och mer av nätverk. Detta skapar två långsiktiga effekter som är direkt relevanta för “var vi är i dag”:

1. **Institutionell devalvering:** Om systemet fungerar via relationer försvagas incitamenten att bygga och respektera formella institutioner. Lagen blir inte en neutral spelregel utan ett verktyg som kan kringgås.
2. **Moralisk glidning:** När “genvägar” blir nödvändiga för överlevnad upphör de att uppfattas som avvikelser. Detta normaliserar korruption och gråzonsbeteende på ett sätt som senare kan skalas upp under marknadsliberalisering.

Här uppstår ett samhälleligt habitus: medborgare och chefer lär sig att framgång kräver informell kompetens – förmågan att navigera nätverk, byta tjänster och skapa skydd. Denna

kompetens är i praktiken densamma som senare, i 1990-talets privatiseringar, möjliggör snabb kapitalackumulation och kontroll över nyckelresurser.

### Säkerhetstjänsternas roll i ekonomin

Efter Stalins död blir säkerhetsapparatens relation till den informella ekonomin mer pragmatisk och sofistikerad. Den centrala uppgiften är inte längre att terrorisera hela befolkningen, utan att upprätthålla regimens stabilitet, kontrollera elitens lojalitet och hantera hot. KGB utvecklar en strategi där småskalig illegalitet ofta tolereras så länge den inte hotar politisk kontroll eller skapar oberoende maktcentra. Men denna tolerans har ett pris: aktörer i gråzonen blir per definition utpressningsbara.

Detta är en nyckelmekanism. Den informella ekonomin blir ett rekryterings- och kontrollfält. Personer som driver illegal produktion, smuggling, mutnätverk eller byteshandel kan användas som källor, mellanhänder eller "tekniska lösningar" på problem som staten inte vill lösa formellt. Samtidigt kan säkerhetsapparaten när som helst aktivera lagens fulla kraft mot dem. Denna asymmetri skapar en lojalitetsdisciplin: gråzonens aktörer blir beroende av beskydd och anpassning. **Christopher Andrew och Vasili Mitrokhin** [Basic Books 1999: *"The Sword and The Shield: The Mitrokhin Archive and the Secret History of the KGB"*] belyser hur säkerhetsapparaten i praktiken fungerar som ett parallellt styrsystem som övervakar och påverkar både ekonomiska och sociala miljöer. För rapportens syfte är poängen att KGB inte bara är "repression"; KGB blir en institutionell bro mellan formell stat och informell ekonomi.

### Den svarta ekonomin som systembärande funktion

Under 1970- och 1980-talen sker en gradvis professionalisering av kriminella nätverk. De kriminella miljöer som formats av Gulag (*vory*-kultur, hierarkier, disciplin) möter den sena sovjetiska brist- och bytesekonomin och utvecklar alltmer stabila distributions- och beskyddsmodeller. Denna professionalisering sker i samspel med delar av den statliga apparaten, där lokala tjänstemän, företagsledare och ibland polis/partifunktionärer blir del av en gråzon där resurser, tjänster och skydd byts.

**Federico Varese** [Oxford University Press 2001: *"The Russian Mafia: Private Protection in a New Market Economy"*] har visat hur ryska kriminella strukturer ofta uppstår och blir starka just i institutionella vakuum eller där formella institutioner inte kan garantera kontrakt, egendom och tvistelösning. Den sena sovjetperioden erbjuder en särskild version av detta: ett samhälle med stark stat i formell mening men svag stat i kontrakts- och servicekapacitet. Detta gör att "skydd" och "garanti" blir en efterfrågad tjänst, vilket senare blir kärnan i 1990-talets kriminella beskyddsekonomi.

**Mark Galeottis** [Ebury Publishing 2018: *"The Vory: Russia's Super Mafia"*] arbete om *Vory*-traditionen är också relevanta här som kulturellt arv: den kriminella subkulturen skapar

normer om lojalitet, disciplin och kapitalförvaltning som kan omsättas när ekonomiska möjligheter öppnar sig.

### **Perestrojka: liberalisering utan rättsstat – den accelererande informaliseringen**

Gorbatjovs reformer syftade till att modernisera systemet genom *glasnost* och *perestrojka* (ombyggnad och öppenhet). Men reformerna liberaliserade delar av ekonomin utan att samtidigt skapa robusta institutioner för äganderätt, kontraktsverkställighet, konkurrensneutralitet och rättssäkerhet. Denna obalans är central: när formella barriärer tas bort men institutionell kapacitet saknas, får informella nätverk en historisk möjlighet att omvandla socialt och politiskt kapital till ekonomisk makt.

Kooperativ och halvprivata strukturer blir arenor där aktörer med nätverkskapital – ofta kopplat till partiapparat, företagsledning eller säkerhetsmiljöer – kan skaffa sig tillgång till varor, valuta, import/exportkanaler och ibland rena tillgångsövertaganden. Perestrojka blir därmed inte bara en reformperiod; den blir en **förberedelsefas** för den senare privatiseringsvågen: de som redan behärskar informell logik får ett försteg när marknadselement införs.

**Vladislav Zubok** [Yale University Press 2021: ”*Collapse: The Fall of the Soviet Union*”] visar hur den sovjetiska elitens, ekonomins försämring och det politiska kontrollsystemets erosion skapade en situation där gamla regler inte längre fungerade men nya regler ännu inte fanns. Detta är exakt den typ av “interregnum” där informella strukturer historiskt blomstrar: nätverk ersätter institutioner, och säkerhets- och beskyddskapacitet blir central.

Den avgörande bryggan till “i dag” – tre arv som 1990-talet och Putin bygger på

Om kapital 3 visar hur tvång och rättslöshet institutionaliseras i industriell skala, visar kapital 4 hur denna logik socialiseras och blir vardag. Det är här grunden läggs för 1990-talets systemkollaps och Putins senare rekonfiguration.

Tre arv är särskilt viktiga:

#### **Informell kompetens blir elitkompetens:**

- Efterkrigstidens och sen-sovjetiska samhälle lär ut att framgång kräver nätverkskapital, lojalitetsband, och förmåga att navigera toleransgränser. När Sovjet faller är det denna kompetens som kan omsättas i egendom, kapital och kontroll.

#### **Selektiv legalitet blir en styrningsmekanism:**

- Staten (via säkerhetsapparaten) lär sig att tolerera illegalitet men använda den selektivt. Detta är direkt kompatibelt med dagens modell där juridik och regler ofta används instrumentellt: lagar kan aktiveras mot motståndare och neutraliseras för lojala.

**Gråzonsekonomi blir strukturellt normaliserad:**

- Den svarta ekonomin och Blat gör att gråzonen inte uppfattas som avvikelser utan som nödvändighet. När marknadsreformer kommer blir gråzonen inte mindre; den byter skepnad och skalar upp.

Dessa tre arv innebär att 1990-talets “explosion” av organiserad brottslighet och oligarkmakt inte bör förstås som en plötslig mutation, utan som en frisläppning och omkalibrering av redan existerande strukturer.

**Sammanfattning – ett samhälle i permanent gråzon**

Perioden 1953–1991 skapar därför en paradoxal förutsättning: den levererar stabilitet nog för att institutioner ska överleva, men dysfunktion nog för att informella system ska bli nödvändiga. Resultatet blir en stat som ser formellt stark ut men som i praktiken drivs av nätverk, gråzon och selektiv kontroll. Detta är den exakta strukturella miljö där post-sovjetiska aktörer – oligarker, kriminella nätverk och säkerhetsmiljöer – kan omvandla tidigare sociala och politiska resurser till ekonomisk och senare geopolitisk makt.

I den meningen är kapital 4 inte en mellanperiod, utan den operativa kod som gör 1990-talet och därefter begripligt. Det är här samhälle och stat tillsammans lär sig att fungera i ett system där:

- formella regler är flexibla,
- informella nätverk bär upp vardag och ekonomi,
- illegalitet är tolererad men kontrollerad,
- och säkerhetsapparaten är den yttersta garantin för regimens stabilitet.

Det är därför rimligt att se 1953–1991 som perioden då den ryska symbiosmodellen går från att vara episodisk och brutal till att bli normaliserad, vardaglig och därmed uthållig — vilket i sin tur skapar den kulturella och institutionella grund som dagens hybridstat kan bygga vidare på.

## KAPITEL 5 – SYSTEMKOLLAPS OCH HYBRIDISERING (1991–2000)

*Hur informella strukturer tar över när formella institutioner faller – och varför 1990-talet blev regimens råmaterial*

### 1991 sovjetunionens upplösning och statens reträtt

Sovjetunionens upplösning 1991 är inte bara ett politiskt skifte utan en institutionell kollaps. Den formella staten förlorar snabbt sin förmåga att upprätthålla tre grundfunktioner:

- a. monopol på legitimt våld,
- b. kontroll över skattebas och resurser, samt
- c. förutsägbar rättsordning. När dessa funktioner simultant försvagas uppstår inte en “fri marknad” i västerländsk mening, utan en konkurrens mellan informella aktörer om kontroll över egendom, kontrakt och beskydd.

Här blir arvet från kapital 4 direkt operativt. Samhället och eliterna är redan socialiserade in i att institutioner inte går att lita på och att nätverk ersätter regler. När Sovjetstatens formella ram faller är det därför inte ett tomrum som uppstår, utan en “avformaliserad kontinuitet”: de informella ordningar som tidigare bar upp systemet expanderar och blir dominerande.

**Stephen Kotkin** [Princeton University Press 2001: ”*Armageddon Averted: The Soviet Collapse. 1970 – 2000*”] har beskrivit kollapsen som en process där staten inte övergår till något stabilt, utan fragmenteras och lämnar efter sig en struktur av svaga institutioner, starka intressen och regionala maktcentra. För rapportens syfte är poängen att statens frånvaro blir en marknad för våld och beskydd, där organiserad brottslighet och säkerhetsaktörer kan monetarisera kontroll.

### Oligarker, maffia och säkerhetstjänst – marknadsreformer utan rättsstat

De tidiga reformerna i Ryssland syftade till att snabbt stabilisera ekonomin och övergå till marknad. I praktiken skapade de en institutionell obalans: prislösningar, privatiseringar och avregleringar genomfördes innan robusta institutioner för äganderätt, konkurrens, domstolar och reglerad finans fanns på plats. Resultatet blev en ekonomi där “marknad” innebar frihet för starka aktörer att erövra resurser, snarare än lika spelregler.

**Abraham Katz** [Praeger, New York 1972: ”*The Politics of Economic Reform in the Soviet Union*”] har belyst logiken bakom chockterapi och dess mål, men det centrala här är inte reformideologi utan den institutionella konsekvensen: när rättsstat och kontraktsverkställighet saknas ersätts de av informella garantier. Den som kan erbjuda skydd – genom våldskapacitet, nätverk, korrupcion eller politiska kontakter – får ett strukturellt försteg i tillgångsovertaganden.

Det är här 1990-talets fundament byggs: egendom blir inte en juridisk kategori, utan en praktisk kontrollrelation. Vem som “äger” avgörs av vem som kan hålla, försvara och monetarisera tillgången.

### **Triangelmodellen: Stat – Kapital – Kriminalitet**

Voucher-privatiseringen – där medborgare tilldelades privatiseringskuponger som formellt gav dem del i tidigare statliga tillgångar – och de efterföljande privatiseringsvågorna var formellt utformade för att skapa brett ägande. I praktiken skapade de möjligheter för välpositionerade aktörer att ackumulera tillgångar via informationsövertag, nätverk och manipulation. Många medborgare sålde sina vouchers under ekonomisk press; mellanhänder och insiders kunde därmed konsolidera kontroll över företag.

Den avgörande mekanismen var att privatiseringen inte följdes av ett robust system för Corporate Governance, transparent redovisning och oberoende domstolar. Detta gjorde att de nya ägarrelationerna blev instabila och öppna för konflikt. I denna miljö blev organiserad brottslighet och privata säkerhetsstrukturer naturliga aktörer: de kunde erbjuda “kontraktsverkställighet” och beskydd i avsaknad av staten.

Här knyter kapitlet direkt till den teori **Federico Varese** [Oxford University Press 2001: ”*The Russian Mafia: Private Protection in a New Market Economy*”] har utvecklat om hur maffialiknande strukturer växer fram där staten inte kan garantera kontrakt och egendom. Den ryska varianten 1991–1994 är emellertid särskilt explosiv eftersom den kombinerar massiv tillgångsöverföring med svag stat och hög vapentillgång.

### **Våld, privatisering och tillgångskontroll**

En av 1990-talets mest centrala sociala och ekonomiska innovationer är fenomenet *krysha* (“tak”) – ett beskyddssystem där företag, marknader och individer betalar för skydd mot våld, utpressning och konkurrens – eller mot samma aktör som erbjuder skyddet. *Krysha* fungerar som en privat “institution” som ersätter domstol, polis och reglerade marknader.

Det är viktigt att förstå *krysha* som mer än kriminalitet. Det är ett samhällsligt kontrakt under tvång. Företag betalar inte bara för att undvika våld; de betalar för att få tillgång till marknader, leveranser, licenser, tullpassager och ibland politiskt inflytande. Det är ett system som knyter samman kriminella nätverk, privata säkerhetsbolag (ofta med ex-militär/ex-KGB-personal) och lokala myndigheter.

**Mark Galeotti** [Ebury Publishing 2018 ”*The Vory: Russia’s Super Mafia*”] har skrivit om rysk organiserad brottslighet. Här beskriver Galeotti hur 1990-talets kriminella landskap professionaliseras och hur gränsen mellan brott, affärsverksamhet och statlig kontroll blir flytande. För rapportens övergripande argument är poängen att *krysha* blir en praktisk modell för hur rysk makt senare kan organiseras: informell kontroll, selektiv legalitet och beskydd som styrningsmekanism.

## Oligarkerna – kapitalackumulation, politisk makt och mediasystem

Begreppet “oligark<sup>4</sup>” syftar inte enbart på rika individer, utan på en struktur där enorm ekonomisk makt omvandlas till politiskt inflytande, ofta via media, finans och relationer till staten. Under 1990-talet växer en grupp affärsmän fram som inte bara äger företag, utan formar politiska beslut, ministerutnämningar och valkampanjer.

I denna period blir media ett strategiskt instrument. Oligarker kontrollerar tv-kanaler och tidningar som formar opinion och skyddar deras intressen. Detta är en nyckel till att förstå varför 1990-talet inte är “fri marknad” utan en maktkamp mellan konkurrerande nätverk med ekonomiska, politiska och ibland våldsbaserade resurser.

Denna oligarkiska struktur är samtidigt instabil eftersom den bygger på personliga lojaliteter och tillfälliga allianser, inte på institutioner. Det skapar en miljö där staten kan återta kontroll genom att spela ut aktörer mot varandra – vilket blir centralt efter 1999.

“Loans-for-shares” – när staten pantsätter framtiden och skapar en ny lojalitetsregim

Programmet “loans-for-shares” (1995–1996) är en av de mest avgörande mekanismerna i 1990-talets kapitalformation. Under förevändning att staten behövde finansiering, pantsattes andelar i strategiska bolag (särskilt råvaru- och industriföretag) som säkerhet för lån från banker. När staten inte kunde återbetala övergick ägandet till långivarna, ofta via auktioner som kritiserats för bristande transparens.

Det centrala är inte bara att tillgångar bytte ägare, utan att ägande kopplades till politisk lojalitet. Staten skapade ett system där utvalda finansaktörer fick strategiska tillgångar i utbyte mot politiskt stöd, särskilt inför presidentvalet 1996. Detta är ett tydligt exempel på hur ekonomisk struktur blir politisk struktur: ägande blir ett instrument för regimens överlevnad, och ekonomiska eliter blir politiska aktörer.

I rapportens logik är detta ett avgörande steg mot dagens modell: staten lär sig att skapa lojalitetsregimer genom att distribuera eller återta tillgångar, och att använda legalitet selektivt som disciplinärt verktyg.

## Säkerhetsapparaten återkom – ”siloviki<sup>5</sup>” och statens rekonstruktion från insidan

Ett återkommande tema i analyser av det sena 1990-talet är hur personer med bakgrund i säkerhetsapparat och militära strukturer gradvis återtar centrala positioner i staten och i strategiska företag. Dessa aktörer – ofta kallade *Siloviki* – har ett särskilt habitus: de prioriterar kontroll, lojalitet och operativ kapacitet snarare än marknadslogik.

---

<sup>4</sup> Ordet kommer från grekiskans: oligarki - “fämannavälde” – ett system där ett litet antal personer kontrollerar stora delar av ekonomi och makt.

<sup>5</sup> Ordet kommer från: *silovye struktury* (“maktstrukturer” eller “styrkestrukturer”). I modern rysk kontext används *siloviki* främst om: den nätverksbaserade elit av tidigare och nuvarande säkerhets- och underrättelsepersoner som har stort inflytande över staten, ekonomin och strategiska sektorer.

Här är det viktigt att se denna återkomst som en funktion av 1990-talets kaos. När staten uppfattas som svag och hotad av oligarkisk fragmentering och kriminell kontroll blir säkerhetsapparaten logik attraktiv som stabiliserande kraft. Den erbjuder ordning, men också ett system där informell kontroll, hemlighet och selektivt ingripande är normala metoder.

Detta är en direkt bro till 2000-talet. Putins konsolidering blir begriplig som en rekonstruktion av staten där informella metoder från sovjetisk och post-sovjetisk erfarenhet integreras i en centraliserad modell. 1990-talet producerar både problemet (fragmentering) och lösningen (*Siloviki*-modellens legitimitet).

### **Regionalisering och statens fragmentering – lokala furstendömen och våldskapital**

Under 1990-talet fragmenteras inte bara den federala staten utan även territoriell kontroll. Guvernörer och regionala eliter skapar egna maktbaser, ofta med lokala säkerhetsstrukturer och ekonomiska nätverk. Detta innebär att den ryska staten i praktiken blir ett lapptäcke av lokala ordningar med varierande grad av rättssäkerhet, korruption och kriminell integration.

Denna regionala fragmentering förstärker behovet av informell governance. Företag behöver lokala beskyddssystem, och konflikter mellan regioner och center löses ofta via förhandlingar, byteshandel och selektiv repression. Detta är en viktig del av varför centraliseringsprojektet efter 1999 får ett så starkt institutionellt och politiskt stöd.

### **Den andra Tjetjenienkonfliktens föregångare och våldets politiska funktion**

Tjetjenienkrigen under 1990-talet är både symptom och drivkraft i statens kollaps. De visar statens militära svaghet, men skapar också ett narrativ om nationell kris och behov av stark ledning. Konflikten blir en arena där våldsaktörer, kriminella ekonomier och statliga strukturer interagerar – smuggling, vapenflöden, kidnappningar och informella finansieringskedjor.

Även om en fullständig analys av Tjetjenien kräver ett eget kapitel är det viktigt att notera dess roll som katalysator för legitimeringen av säkerhetsapparaten återkomst och den politiska viljan att “återställa ordningen”.

### **Sammanfattning – grunden för den moderna hybridstaten**

1991–1999 bör förstås som den period då Ryssland genomgår en massiv fördelningskamp under institutionell svaghet. Den formella staten tappar kontroll, och informella strukturer – kriminella nätverk, privata säkerhetsaktörer, oligarkiska finansgrupper och regionala maktcentra – tar över funktioner som normalt tillhör en stat: kontraktsverkställighet, egendomsskydd, konfliktlösning, resursallokering och ibland även politisk styrning.

Ur rapportens perspektiv producerar 1990-talet tre avgörande arv som leder in i – var vi är idag:

- a. **Egendom som kontrollrelation:** Äganderätt blir i praktiken något som måste försvaras med nätverk, våld eller politisk lojalitet. Detta gör att staten senare kan återta tillgångar genom selektiv legalitet.
- b. **Beskydd som governance:** *Krysha* etablerar en modell där skydd, tillgång och lojalitet binds samman. Denna logik är kompatibel med en centraliserad hybridstat som erbjuder “stabilitet” i utbyte mot lydnad.
- c. **Säkerhetsapparaten som stabiliseringsmyt och verklighet:** *Siloviki*-modellen framstår som lösningen på kaos. Men den bygger på samma informella logiker som 1990-talet visar: nätverk, hemlighet, selektivt våld och instrumentell legalitet.

Därmed blir 1990-talet inte ett undantag eller en “övergång” till demokrati och marknad. Det blir en strukturell förberedelseperiod där informell makt koncentreras, våld ”privatifieras” och staten lär sig att rekonstruera kontroll genom att absorbera – och disciplinera – de nätverk som först växte fram i dess frånvaro.

## KAPITEL 6 – PUTINSYSTEMET: DEN INSTITUTIONALISERADE SKUGGAN (2000–2014)

*När staten återtar kontrollen genom att absorbera den ekonomiska och informella ordningen*

### **Putin 1.0 – disciplinering och maktkonsolidering**

När Vladimir Putin tillträder som president år 2000 gör han det i ett Ryssland som präglas av institutionell erosion, våldsmonopol i spillror och en ekonomi dominerad av oligarkiska och kriminella nätverk. Den centrala politiska uppgiften är därför inte demokratisering eller marknadsutveckling, utan *rekonstruktion av statlig kontroll*. Avgörande är att denna rekonstruktion inte sker genom att ersätta informella strukturer med rättsstatliga institutioner, utan genom att *underordna dem staten*.

Putins projekt kan därmed förstås som ett svar på 1990-talets fragmentering, men också som en fortsättning på en längre historisk logik: staten återtar makt genom att absorbera, disciplinera och omforma informella nätverk. I detta avseende representerar Putin inte ett brott med det förflutna, utan en syntes av sovjetisk säkerhetslogik och post-sovjetisk nätverkskapitalism.

**Stephen Kotkin** [Princeton University Press 2001: ”*Armageddon Averted: The Soviet Collapse. 1970 – 2000*”] Putins tidiga år som en period där staten ”reasserts itself” snarare än reformeras i västerländsk mening. Denna återassertion bygger på selektiv legalitet, kontroll över nyckelresurser och lojalitetsbaserad maktfördelning.

### **Siloviki och statlig absorption av informella strukturer**

En av de mest avgörande förändringarna under Putins första mandatperiod är *Silovikis* framväxt som dominerande elit. Personer med bakgrund i KGB/FSB, militär, inrikestrupper och säkerhetsrelaterade strukturer tar successivt över nyckelpositioner inom stat, statsägda företag och strategiska myndigheter.

Denna utveckling är inte bara personalpolitisk; den är institutionell. *Siloviki* delar en gemensam världsbild där staten ses som ett hotat system som måste skyddas, där lojalitet prioriteras framför lagbundenhet, och där makt utövas genom kontroll snarare än transparens. De bär med sig en professionell kultur präglad av hemlighet, informella kommandokedjor och operativ pragmatism.

**Catherine Belton** [HarperCollins 2020 – ”*Putin's People: How the KGB Took Back Russia and Then Took on the West*”] diskuterar begreppet ”The New Nobility” och visar hur man successivt institutionaliserar sin roll och skapar ett system där säkerhetsapparaten inte längre är ett instrument under staten – den är staten.

### Selektiv rättstillämpning och lojalitetsstyrning

Putins uppgörelse med oligarkerna i början av 2000-talet – symboliserad av Michail Chodorkovskijs fall – är central för att förstå regimens styrningslogik. Detta var inte en kamp mot korruption eller olaglig rikedom i sig, utan en omförhandling av maktrelationer. Oligarker som accepterade politisk underordning och avstod från självständig maktutövning fick behålla sina tillgångar; de som utmanade staten neutraliserades genom rättsliga och administrativa medel.

Här etableras selektiv legalitet som styrningsprincip. Lagen används inte universellt, utan instrumentellt. Detta skapar en disciplinerande effekt långt bortom de individer som faktiskt drabbas. Ekonomiska aktörer internaliserar att äganderätt är villkorad av politisk lojalitet.

Denna mekanism har analyserats av **Federico Varese** [Oxford University Press 2001: ”*The Russian Mafia: Private Protection in a New Market Economy*”] som pekar på hur staten i Putins Ryssland inte avskaffar beskyddssystemet från 1990-talet, utan ersätter privata *krysha* med en statlig *krysha*.

### Ekonomisk centralisering och strategiska företag – från statskapitalism till hybridkrigföring

Under 2000-talet utvecklas i Ryssland en särskild form av statskapitalism där staten, genom direkt ägande eller informell kontroll, dominerar strategiska sektorer såsom energi, råvaror, försvar, transport och finans. Företag som ROSNEFT, GAZPROM, och ROSTEC fungerar i detta system inte enbart som kommersiella aktörer, utan som integrerade geopolitiska verktyg i statens kontroll av internationell påverkan och maktutövning.

Denna modell kombinerar marknadselement med tydlig politisk styrning: vinster kan i praktiken privatiseras till lojala aktörer, medan den strategiska kontrollen förblir statlig.

Ledande positioner tillsätts systematiskt med personer ur den så kallade *Siloviki-kretsen* – individer med bakgrund i säkerhetstjänst, militär eller statlig maktapparat – vilket suddar ut gränsen mellan ekonomiskt och säkerhetspolitiskt beslutsfattande.

Denna struktur etableras successivt under Vladimir Putins första mandatperioder, men får en kvalitativt ny betydelse efter 2014. Annekteringen av Krim markerar inte bara en militär och politisk brytpunkt, utan också en operativ fasförskjutning där de statligt kontrollerade företagen i allt högre grad används som aktiva komponenter i rysk hybridkrigföring.

Ekonomiska relationer, investeringar och leveranser börjar systematiskt användas för extern påverkan, samtidigt som de formellt hålls inom ramen för avtal, bolagsrätt och internationell handel. På så sätt kan strategisk effekt uppnås utan att tydligt bryta mot internationell rätt eller utlösa direkta motåtgärder.

### **Organiserad brottslighet i den nya ordningen – absorption snarare än utrotning**

En avgörande aspekt av Putins konsolidering är hur organiserad brottslighet hanteras. Till skillnad från 1990-talet, då kriminella nätverk ofta var autonoma eller konkurrerade med staten, sker nu en absorption. Kriminella strukturer som kan kontrolleras och användas tolereras eller integreras; de som hotar statens monopol neutraliseras.

**Mark Galeotti** [Ebury Publishing 2018 ”*The Vory: Russia’s Super Mafia*”] har beskrivit detta som en övergång från “criminal chaos” till “criminal governance”. Brottslighet blir inte längre ett parallellt maktcentrum, utan en resurs som kan utnyttjas för kapitalflöden, påverkansoperationer, smuggling och informella uppdrag – ofta med ”plausible deniability”.

Detta är en direkt fortsättning på den symbiosmodell som etablerats i tidigare kapitel: staten bekämpar brottslighet selektivt, men behåller dess metoder och nätverk som verktyg.

Mediekontroll och informationsdomänen – från *pluralism* till *narrativ dominans*.

Under 2000-talet omformas den ryska mediemiljön från ett relativt pluralistiskt men oligarkstyrtd landskap till ett system där staten – direkt eller indirekt – kontrollerar de viktigaste tv-kanalerna och informationsflödena. Detta sker inte enbart genom censur, utan genom ägarstruktur, ekonomisk press och rättsliga mekanismer.

Informationskontroll blir en central del av statens maktutövning. Narrativ om stabilitet, suveränitet och yttre hot används för att legitimera centralisering och säkerhetsåtgärder. Detta är en förutsättning för senare hybridstrategier där informationspåverkan riktas även externt.

**Alexei Yurchaks** [Princeton University Press ”*Everything Was Forever, Until It Was No More: The Last Soviet Generation*”]. analyser av sen-sovjetisk “som-om”-kultur är här relevanta som förhistoria: staten producerar narrativ som alla vet är förenklingar, men som fungerar socialt och politiskt.

### **Regional centralisering och “maktens vertikal”**

Putins konsolidering innebär också en omstrukturering av relationen mellan centrum och regioner. Guvernörernas autonomi begränsas, federala distrikt skapas och utnämningssystem förändras. Detta reducerar regional fragmentering men ersätter den med lojalitetsbaserad centralism.

Den så kallade “maktens vertikal” är inte en byråkratisk hierarki i klassisk mening, utan ett nätverk av lojalitetsrelationer där centrum har sista ordet men tillåter lokal flexibilitet så länge kontrollen inte hotas. Detta speglar återigen den ryska traditionen av informell styrning under formell centralism.

### **Utrikespolitisk hybridisering – inrikes metoder projiceras utåt**

Mot slutet av perioden, särskilt efter Georgienkriget 2008, blir det tydligt att de metoder som utvecklats för intern kontroll också kan användas externt. Ekonomiska påtryckningar,

energiberoenden, informationspåverkan och användning av informella aktörer blir verktyg i utrikespolitiken.

Detta markerar övergången från intern konsolidering till *extern hybridisering*. Staten har nu tillgång till ett integrerat system av formella och informella medel som kan användas flexibelt och med förnekbarhet.

### **Ekonomisk centralisering och strategiska företag**

Perioden 2000–2014 representerar kulmen på den historiska utveckling som rapporten beskriver. Staten återtar kontroll, men inte genom att eliminera brottets och informella nätverks logik. I stället institutionaliseras dessa logiker inom staten själv.

Resultatet är en hybridstat där:

- legalitet är selektiv och instrumentell,
- ekonomi och säkerhet är sammanflätade,
- organiserad brottslighet är absorberad snarare än utplånad,
- och informella nätverk är en del av statens infrastruktur.

Detta system är stabilt på kort och medellång sikt, men bygger på kontinuerlig kontroll och konfliktproduktion – både internt och externt. Det är denna modell som ligger till grund för Rysslands agerande efter 2014 och framåt.

## KAPITEL 7 – HYBRIDKRIGFÖRING SOM PERMANENT TILLSTÅND (2014–2025)

*När den ryska symbiosmodellen blir operativ verklighet i Europa och Sverige*

### **Krim, Ukraina och strategisk brytpunkt**

År 2014 utgör den avgörande brytpunkten i den europeiska säkerhetsordningen. Annekteringen av Krim och den efterföljande destabiliseringskampanjen i östra Ukraina markerade inte enbart början på ett regionalt krig, utan starten på en ny fas i rysk maktutövning gentemot Europa. Det som därefter följer är inte ett tillfälligt undantagstillstånd, utan etableringen av ett permanent konflikttillstånd under krigströskeln.

I denna fas börjar den ryska staten systematiskt projicera den styrningslogik som utvecklats under 1900-talet – och analyserats i de föregående kapitlen – utanför sina egna gränser. Informella nätverk, organiserad brottslighet, ekonomiska gråzoner, cyberkapacitet och informationspåverkan kombineras till ett sammanhängande kampanjsätt. Den centrala poängen är att dessa medel inte ersätter militär makt, utan kompletterar och förstärker den, samtidigt som de skapar förnekbarhet och politisk friktion för motståndaren.

Detta är inte hybridkrigföring som doktrinärt begrepp, utan som praktiserad statsmodell.

### **Informationspåverkan och FIMI\* [ref - Foreign Information Manipulation and Interference]**

För att förstå perioden 2014-idag räcker det inte att analysera enskilda cyberangrepp, kabelbrott eller desinformationskampanjer. Dessa är manifestationer av ett underliggande system. Den ryska modellen bygger på att skapa sammanlagd strategisk effekt genom ackumulering av små, ofta juridiskt tvetydiga handlingar, snarare än genom öppna, eskalerande angrepp.

I detta system fyller statstjänande kriminalitet en avgörande funktion. Kriminella nätverk och ekonomiska gråzonsaktörer erbjuder den ryska staten tre strategiska fördelar: operativ flexibilitet, låg kostnad och maximal förnekbarhet. De kan användas för logistik, penningtvätt, sabotageförberedelser, proxy-uppdrag och sanktionsundandragande – utan att staten formellt exponeras.

Här blir den historiska kontinuiteten tydlig. Precis som i tsartidens periferi, i Gulags parallellförvaltning och i den sena sovjetiska svarta ekonomin används kriminalitet inte trots staten, utan **för staten**. Skillnaden är att arenan nu är europeisk.

### **Cyberoperationer och gråzonssabotage**

Efter 2014 intensifieras ryska påverkansoperationer i Europa och får en tydligare kampanjkaraktär. Informationspåverkan används inte primärt för att övertyga befolkningar om en specifik rysk världsbild, utan för att undergräva tillit: till medier, till myndigheter, till

valprocesser och till internationella samarbeten. Polarisering blir ett mål i sig, eftersom ett splittrat samhälle är mindre handlingskraftigt.

Cyberoperationer integreras tätt i denna logik. Intrång används för underrättelseinhämtning och förpositionering, men också för att skapa störningar med breda civila bieffekter. Denna typ av "spillover" är inte nödvändigtvis ett misslyckande, utan kan fungera som strategisk signalering: stöd till Ukraina och konfrontation med Ryssland kan få kostnader även långt från frontlinjen.

Parallellt ser vi en ökning av fysisk subversion och sabotage i Europa, ofta genom proxy-aktörer. Dessa handlingar är i regel småskaliga men systematiska: kabelskador, bränder, störningar i logistiska noder och tester av beredskap. Deras värde ligger inte i den direkta skadan, utan i den osäkerhet de skapar och den resursdränering de tvingar fram hos mottagaren.

Undervattensinfrastruktur i Östersjön – elkablar, datakablar och pipelines – blir här särskilt central. Den är kritisk för samhällsfunktioner, svårt att skydda och ännu svårare att attribuera när skador uppstår. Denna domän illustrerar hybridkrigets kärna: låg angreppskostnad, högpolitisk effekt.

### **Ekonomisk infiltration och sanktionsundandragande**

Sverige framträder i denna miljö inte som ett primärt militärt mål, utan som ett strategiskt gynnsamt operationsområde. Landets öppenhet, godtrohet, höga institutionella tillit och komplexa ekonomi gör det särskilt mottagligt för lågröskelinfiltration snarare än konfrontation.

Här blir den svenska kartläggningen av rysk organiserad brottslighet, genomförd av Acta Publica [RAPPORT 2025:1 "Ryska Intressen: En fördjupad studie av svenska bolag med rysk koppling"] ett avgörande empiriskt bidrag. Rapporten visar hur ryska kriminella nätverk och associerade aktörer etablerat sig i svenska bolagsstrukturer, fastighetsaffärer och kapitalflöden. Det centrala är att denna närvaro i många fall är formellt laglig, men strategiskt problematisk.

Detta bekräftar rapportens övergripande tes: hybridhot verkar ofta under tröskeln för juridiskt ingripande men över tröskeln för nationell säkerhet. När aktörer följer bolagsrätt, skatteregler och upphandlingsformalia, men samtidigt ingår i nätverk som tjänar en främmande makts intressen, uppstår ett säkerhetspolitiskt vakuum.

### **Kriminella Proxys och fysisk subversion**

Acta Publicas analys identifierar tre marknader där den ryska närvaron är särskilt betydelsefull ur säkerhetssynpunkt. Dessa arenor måste förstås i relation till hybridkrigets logik, inte som separata problemområden.

I näringslivet används företag sällan för öppna övertaganden, utan som plattformar. Genom ägande, partnerskap och investeringar skapas tillgång till leverantörskedjor, teknik,

affärsinformation och personliga nätverk. I hybridlogik är detta förberedande terrängtagning. Ett bolag som i dag framstår som legitimt kan i morgon fungera som kanal för underrättelseinhämtning, sanktionsundandragande eller politisk påverkan. Hotet ligger inte i den enskilda affären, utan i ackumulerad exponering.

I finanssektorn är hotet ännu mer systemiskt. Acta Publica visar hur samma individer och strukturer återkommer i flera bolagsupplägg, ofta via mellanhänder och jurisdiktioner som försvårar insyn. Varje enskild transaktion kan vara korrekt, men helheten möjliggör penningtvätt, kapitalflytt och finansiering av andra hybridoperationer. I detta perspektiv blir finansiell brottslighet inte ett isolerat kriminalproblem, utan en geopolitisk möjliggörare.

Den tredje arenan är offentlig sektor. Kommuner, regioner och statliga myndigheter verkar i ett system där rättssäkerhet och likabehandling är grundläggande principer. Just därför blir de sårbara. När aktörer uppfyller formella krav men samtidigt agerar i linje med främmande makts intressen saknas ofta verktyg för tidigt ingripande. Upphandling i högriskbranscher, beroende av externa leverantörer och begränsad säkerhetsanalytisk kapacitet skapar strukturella angreppspunkter. Här kolliderar juridisk formalism med säkerhetspolitisk verklighet.

### **Statstjänande kriminalitet som modulärt verktyg**

I den samtida ryska hybridmodellen fungerar kriminalitet modulärt. Kriminella nätverk kan användas för avgränsade uppdrag – sabotage, spaning, transport, penningtvätt – utan att integreras formellt i staten. Detta skapar en operationsmiljö där ansvar kan förnekas, aktörer bytas ut och risk spridas.

Det avgörande är att dessa nätverk inte behöver styras i detalj. Det räcker att de verkar i ett ekosystem där deras aktiviteter sammanfaller med statens strategiska intressen och där tolerans, beskydd eller selektiv rättstillämpning fungerar som styrmedel. Detta är samma logik som under sovjettiden gjorde den svarta ekonomin systembärande – nu applicerad i internationell miljö.

### **Den svenska åtgärdsutmaningen – från reaktiv rättsstat till strategisk resiliens**

Den hotbild som detta kapitel beskriver kan inte mötas enbart med traditionella brottsbekämpande eller underrättelsemässiga verktyg. Den ryska hybridmodellen, sådan den manifesteras i Sverige, verkar systemiskt och långsiktigt genom formellt legala strukturer, ekonomiska relationer och sociala nätverk. Detta innebär att Sveriges främsta sårbarhet inte är brist på lagar, utan brist på sammanhållen strategisk tillämpning.

I grunden står Sverige inför en strukturell paradox. Den svenska rättsstaten är uppbyggd för att skydda individen mot staten och säkerställa förutsebarhet, likabehandling och transparens. Den är däremot mindre anpassad för att hantera hot som utnyttjar just dessa principer för strategisk påverkan. När främmande makt agerar genom proxies, bolagsstrukturer och

kriminella nätverk som håller sig inom lagens formella ramar uppstår ett glapp mellan legalitet och säkerhet.

Den svenska åtgärdsutmaningen handlar därför inte om att överge rättsstatliga principer, utan om att komplettera dem med säkerhetspolitisk analys, riskbaserad styrning och strategisk tillsyn.

### **Policy och lagstiftning – behovet av ett säkerhetspolitiskt raster**

På policy- och lagstiftningsnivå krävs ett tydligare erkännande av att organiserad brottslighet och ekonomisk infiltration i dag utgör nationella säkerhetshot, inte enbart kriminalpolitiska problem. Detta innebär att lagstiftning som rör bolagsbildning, ägande, upphandling, investeringar och finansiella flöden måste analyseras genom ett säkerhetspolitiskt raster.

Sverige har på senare år tagit viktiga steg genom lagstiftning om säkerhetsskydd, utökade möjligheter till informationsdelning och förstärkt tillsyn inom finanssektorn. Samtidigt kvarstår ett grundproblem: många av de strukturer som identifieras i Acta Publicas material faller mellan regelverken. De är varken tillräckligt brottsliga för straffrättsliga åtgärder, eller tillräckligt säkerhetsklassade för att omfattas av säkerhetsskyddslagstiftning.

Ett centralt utvecklingsområde är därför förmågan att väga samman flera svaga signaler – ekonomiska, organisatoriska och personella – till en samlad riskbedömning. Detta kräver i sin tur:

- tydligare mandat för myndighetssamverkan,
- gemensamma hotbilder snarare än sektorsvisa lägesbilder,
- och en ökad acceptans för att säkerhetsrisk kan föreligga även när lagöverträdelse inte kan styrkas.

### **Tillsyn och myndighetsansvar – från regelkontroll till riskstyrning**

Den svenska tillsynsmodellen är i hög grad regelbaserad. Myndigheter kontrollerar efterlevnad av specifika regelverk inom sina respektive ansvarsområden. Denna modell är effektiv mot traditionella regelöverträdelse, men mindre lämpad för att identifiera strategiska mönster över flera sektorer.

Acta Publicas kartläggning visar hur samma aktörer kan förekomma i flera bolag, branscher och transaktioner utan att någon enskild tillsynsmyndighet ser mer än en begränsad del av helheten. Resultatet blir fragmenterad riskuppfattning och fördröjd respons.

### **En strategisk tillsynsmodell skulle i stället utgå från:**

- nätverksanalys snarare än enskilda ärenden,
- historik och mönster snarare än punktinsatser,
- och säkerhetseffekt snarare än enbart regeluppfyllelse.

**Detta kräver inte nödvändigtvis nya myndigheter, men nya arbetssätt:**

- gemensamma analysfunktioner, systematisk informationsdelning och ett uttalat mandat att beakta nationell säkerhet även i ärenden som formellt ligger inom exempelvis bolagsrätt, arbetsrätt eller upphandling.

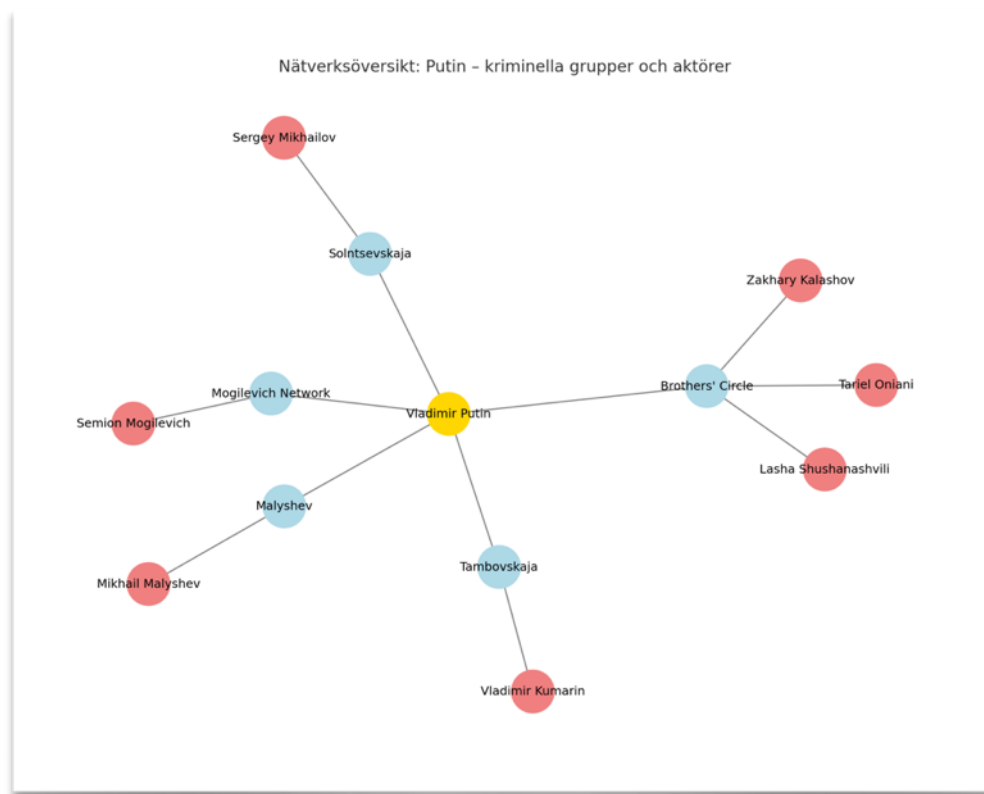
**Sammanfattning – hybridkrig under krigströskeln**

Kapitel 10 visar att det ryska hotet mot Sverige och Europa inte främst tar formen av militär invasion, utan av vardaglig systempåverkan. Genom ekonomi, kriminalitet, information och juridiska gråzoner skapas ett kontinuerligt tryck som undergräver tillit, ökar osäkerhet och begränsar politiskt handlingsutrymme.

Det farliga ligger inte i någon enskild incident, utan i helheten. Varje kabelbrott, cyberintrång, desinformationskampanj eller misstänkt affär kan framstå som hanterbar i sig. Tillsammans utgör de ett sammanhängande mönster av strategisk påverkan.

Detta är inte ett framtidsscenario. Det är den säkerhetspolitiska samtid Sverige redan befinner sig i.

## KAPITEL 8 – EXEMPEL: ROSNEFT, GAZPROM OCH ROSTEC

**ROSNEFT – statskapitalism, sanktionsevasion och geopolitisk byteshandel**

ROSNEFT är det kanske tydligaste exemplet på hur rysk statskapitalism efter 2014 övergår från intern maktkonsolidering till extern hybridpåverkan. Formellt är ROSNEFT ett kommersiellt energibolag, men i praktiken fungerar det som ett instrument för Kremls utrikes- och säkerhetspolitik. Bolagets utveckling efter Krimannekteringen illustrerar hur ekonomiska investeringar, ägande och handelsstrukturer används för att skapa politiskt inflytande, resiliens mot sanktioner och strategisk förnekbarhet.

I exemplet ROSNEFT illustreras hur staten disciplinerar kapital och centraliserar kontroll.

- Nyckelperson: *Igor Sechin*, tidigare vice premiärminister och en av Putins närmaste medarbetare (FSB-bakgrund).
- Genombrott: 2003–2004 – rättsprocessen mot oligarken Mikhail Khodorkovsky.

Händelseförlopp:

- Yukos (Rysslands då största privata oljebolag) anklagas för skattebrott.
- Tillgångar beslagtogs, bolaget försätts i konkurs.
- 2004–2007: Rosneft övertar Yukos kärntillgångar till kraftigt reducerade priser.

Poängen: Lagen används selektivt – inte för att eliminera korrupktion, utan för att omförhandla makt.

Budskapet till näringslivet:

— *ägande är villkorat av politisk lojalitet.*

ROSNEFTS operativa centrum är dess verkställande direktör Igor Sechin, en av Vladimir Putins närmaste förtrogna och en central figur i *siloviki*-kretsen. Sechin kombinerar rollen som företagsledare med direkt tillgång till statens högsta beslutsnivå, vilket gör gränsen mellan affärsstrategi och geopolitisk strategi i praktiken obefintlig.

Efter 2014 intensifierar ROSNEFT användningen av delägarskap och joint ventures i politiskt strategiska regioner. År 2016 förvärvar bolaget 30 procent av gasfältet ZOHR i Egypten från ENI<sup>6</sup>. Affären sammanfaller med att Egypten fördjupar sitt militära samarbete med Ryssland och intar en mer återhållsam linje gentemot väst i internationella forum.

Investeringen stärker inte bara ROSNEFTS energiposition i östra Medelhavet, utan bidrar också till ett politiskt beroende där energisamarbete och diplomatiskt stöd går hand i hand.

Året därpå investerar ROSNEFT miljardbelopp i oljefält och pipelines i irakiska Kurdistan<sup>7</sup> – en region med oklar rättslig status och pågående territoriella konflikter. Genom att bli en nyckelaktör i exportinfrastrukturen skaffar sig Ryssland inflytande över energiflöden som berör både Irak, Turkiet och EU, samtidigt som Moskva positionerar sig som politisk beskyddare i en instabil region.

Samma år leder ROSNEFT ett konsortium som förvärvar 49 procent av indiska Nayara Energy<sup>8</sup>, vilket skapar ett långsiktigt energiberoende i en av världens viktigaste tillväxtmarknader. Indien kommer därefter att inta en konsekvent balanserande hållning gentemot Ryssland både efter 2014 och efter invasionen av Ukraina 2022.

Efter 2022 anpassas ROSNEFTS modell till ett hårdare sanktionslandskap. Bolaget, tillsammans med närstående strukturer, använder traderbolag i Förenade Arabemiraten,

<sup>6</sup> ENI:s egen pressrelease från december 2016: “ENI has agreed to sell to Rosneft a 30 percent participating interest in the Shorouk Concession, offshore Egypt, where the supergiant gas field Zohr is located.”

<sup>7</sup> Reuters, oktober 2017, där det framgår att Rosneft tog kontroll över huvudledningen för oljeexport från irakiska Kurdistan och att investeringen uppgick till omkring 1,8 miljarder USD

<sup>8</sup> 2017 ledde Rosneft ett internationellt konsortium som förvärvade 49,13 procent av det indiska energibolaget Essar Oil (senare Nayara Energy) i en transaktion värd omkring 12,9 miljarder USD. Källa: Rosneft med flera.

Turkiet och Asien för att sälja rysk råolja till kraftigt rabatterade priser. Oljan omlastas till havs, blandas med andra kvaliteter och säljs vidare som “blended crude”, ofta utan tydlig ursprungsmärkning. Dessa arrangemang bryter sällan explicit mot enskilda regelverk, men urholkar sanktionernas effekt och säkrar intäktsflöden till den ryska staten.

ROSNEFT illustrerar därmed kärnan i rysk hybridkrigföring: marknadsformer används för att uppnå strategisk effekt, ekonomiska relationer omvandlas till politiska beroenden och juridisk gråzon blir ett medvetet verktyg. Delägarskap och joint ventures som geopolitisk mekanism. Efter 2014 intensifierar ROSNEFT användningen av delägarskap och joint ventures i strategiskt viktiga regioner, där kommersiella investeringar kopplas till politiska lojaliteter snarare än strikt marknadslogik.

### **Egypten – ZOHR-fältet (2016)**

ROSNEFT förvärvar 30 procent av gasfältet ZOHR från italienska ENI.

Affären genomförs parallellt med ett fördjupat politiskt och militärt samarbete mellan Ryssland och Egypten efter 2014, inklusive vapenleveranser och diplomatiskt stöd i FN.

Investeringen stärker ROSNEFTS närvaro i östra Medelhavet samtidigt som Egypten blir en återkommande rysk partner i internationella forum.

### **Irak (Kurdistanregionen) – pipeline- och investeringar upstream (2017)**

ROSNEFT investerar miljardbelopp i oljefält och pipelines i irakiska Kurdistan, trots regionens omstridda rättsliga status. Affären ger Ryssland inflytande över en kritisk exportkorridor och positionerar Moskva som politisk beskyddare i en konfliktfylld region.

- Ekonomisk investering fungerar samtidigt som geopolitisk positionering gentemot Bagdad, Ankara och väst.

### **Indien – Nayara Energy (2017)**

Ett konsortium lett av ROSNEFT förvärvar 49 procent av Nayara Energy (tidigare Essar Oil). Indien fördjupar därefter energisamarbetet med Ryssland samtidigt som landet intar en försiktig och delvis neutral hållning gentemot Ryssland efter 2014 och 2022.

- Delägarskap används för att skapa långsiktigt politiskt handlingsutrymme i en nyckelstat i Asien.

## **PMESII-mappning av ROSNEFT som hybridverktyg**

### **Ekonomisk och politisk påverkan (E/P)**

ROSNEFTS roll i PMESII-ramverket är mer direkt kopplad till ekonomisk (E) och politisk (P) påverkan, med särskilt fokus på långsiktigt beroendebyggande och sanktionsresiliens. Till skillnad från GAZPROM, vars styrka ligger i flödeskontroll, verkar ROSNEFT främst genom ägande, kapital och handel.

I den ekonomiska domänen används ROSNEFT för att skapa alternativa energiflöden, kringgå sanktioner och upprätthålla statliga intäkter. Genom delägarskap, joint ventures och

traderstrukturer kan rysk olja fortsätta nå världsmarknaden även under hårda restriktioner. Den ekonomiska effekten är inte bara finansiell, utan strategisk: staten säkrar handlingsutrymme trots internationellt tryck.

I den politiska domänen fungerar ROSNEFT som ett instrument för relationsbyggande med nyckelstater i Mellanöstern, Afrika och Asien. Investeringar och energisamarbeten knyts till diplomatiskt stöd, neutralitet eller passivitet i internationella forum. Detta skapar ett nätverk av stater som, av egenintresse, undviker att fullt ut stödja västliga initiativ mot Ryssland.

ROSNEFTS verksamhet berör även Information (I)-domänen indirekt, genom narrativ om “legitim handel”, “energisäkerhet” och “global syd-solidaritet”, men detta är understödande snarare än bärande.

*Sammanfattning ROSNEFT: ROSNEFT är ett E/P-verktyg som omvandlar ekonomiska relationer till politiska lojaliteter och strategiskt handlingsutrymme.*

### **GAZPROM – energiflöden som beteendestyrning och geopolitisk hävstång**

GAZPROM utgör gasmarknadens motsvarighet till ROSNEFT och är ett centralt instrument i Rysslands hybridkrigföring mot Europa. Även här är den formella bilden ett kommersiellt bolag, medan den faktiska funktionen är att fungera som geopolitisk hävstång.

Sedan 2001 leds GAZPROM av *Alexey Miller*, en nära allierad till Vladimir Putin från tiden i Sankt Petersburgs stadshus. Under 2000-talet återtar staten kontrollen över bolaget, vilket gör GAZPROM till ett direkt styrbart verktyg för Kreml.

Efter 2014 förändras GAZPROM operativa roll. Gasleveranser används inte längre enbart för intäktsmaximering, utan för beteendestyrning av mottagarländer. Leveransvolym, kontraktsvillkor, prissättning och lagringsstrategier används selektivt för att skapa osäkerhet och politisk press, utan att formellt bryta mot avtal. Inom EU är Tyskland ett tydligt bevis på hur effektiv denna strategi är och vilka resultat som kan uppnås.

Åren efter Krim präglas av återkommande leveranskonflikter med Ukraina, vilket indirekt påverkar flera EU-länder. Under 2021 fyller GAZPROM inte sina europeiska lager trots höga marknadspriser, vilket bidrar till energikris, inflation och politisk splittring i Europa strax före invasionen av Ukraina 2022. Efter invasionen reduceras leveranser till flera EU-länder genom tekniska och kontraktsnära argument, snarare än öppna politiska beslut.

GAZPROMS styrka i hybridkrigföringen ligger i dess förnekbarhet. Varje enskilt beslut kan motiveras kommersiellt, men den samlade effekten blir strategisk: ökad sårbarhet, politisk oenighet och ekonomisk stress i målstaters samhällen.

GAZPROM är det mest tydliga exemplet på hur ett formellt kommersiellt bolag fungerar som statligt verktyg.

- Ägande och kontroll: Ryska staten tog åter kontroll över GAZPROM 2005 när staten ökade sitt ägande till +50 procent.
- Nyckelperson: *Alexey Miller*, VD sedan 2001, är en nära allierad till Vladimir Putin från tiden i Sankt Petersburgs stadshus på 1990-talet.
- *Siloviki*-koppling: Styrelse och ledning har genomgående bestått av personer med bakgrund i statlig förvaltning, säkerhetstjänst eller presidentadministrationen.

Operativ användning:

- 2006 och 2009: Gasleveranser till Ukraina reduceras/stoppas i samband med politiska konflikter vilket också har en betydande indirekt påverkan på EU-länder.
- 2014–2021: Differentierade gaspriser till EU-länder beroende på politisk relation till Moskva.
- 2022: Leveransminskningar till Europa efter invasionen av Ukraina – utan formellt sanktionsbrott, men med massiv strategisk effekt.

## PMESII-mappning av GAZPROM som hybridverktyg

### GAZPROM – Ekonomisk och infrastrukturell påverkan (E / I)

GAZPROMS primära funktion i rysk hybridkrigföring ligger i skärningspunkten mellan den ekonomiska (E) och den infrastrukturella (I) domänen. Bolaget kontrollerar inte bara produktion och export av gas, utan även kritisk infrastruktur i form av pipelines, lagringskapacitet och transitberoenden. Detta gör GAZPROM till ett verktyg för att påverka hela samhällssystem snarare än enskilda marknadsaktörer.

I den ekonomiska domänen används GAZPROM för att påverka priser, inflation och statsfinanser i mottagarländer. Genom selektiv prissättning, kontraktsvillkor och volymjusteringar kan bolaget skapa ekonomisk stress som får politiska följd effekter, exempelvis ökade energikostnader för hushåll och industri eller tryck på statsbudgetar. Denna påverkan sker ofta utan att formella avtal bryts, vilket gör motåtgärder politiskt och juridiskt svåra.

I den infrastrukturella domänen fungerar GAZPROM som kontrollpunkt för flöden snarare än som enbart leverantör. Beroendet av rysk gas – i synnerhet före 2022 – gav Ryssland indirekt inflytande över europeisk energisäkerhet, industriproduktion och samhällsresiliens. Under 2021–2022 blev detta tydligt när reducerade leveranser och utebliven lagring bidrog till systemisk osäkerhet i Europa.

Sekundärt berör GAZPROM även Political (P)-domänen genom att ekonomisk och infrastrukturell stress översätts till politisk splittring mellan och inom stater, men detta är en följd effekt snarare än huvudsyftet.

*Sammanfattning GAZPROM: GAZPROM är ett E/I-verktyg som angriper motståndarens samhällsekonomi och kritiska system snarare än dess militära kapacitet.*

— *GAZPROM agerar inom kontraktsramar, men timing, volymer och prissättning används politiskt.*

### **ROSTEC – den militär-industriella dimensionen av rysk hybridkrigföring**

ROSTEC kompletterar bilden av rysk statskapitalism genom att förena industri, försvar och utrikespolitik i en och samma struktur. Koncernen, som grundades 2007 och i dag samordnar över 700 företag inom försvar, flyg, elektronik och avancerad teknologi, leds av *Sergey Chemezov*, tidigare KGB-officer med långvariga personliga och professionella band till Vladimir Putin. Under Chemezovs ledning har ROSTEC utvecklats till ett nav där kommersiell verksamhet, militär kapacitet och säkerhetspolitisk påverkan smälter samman.

Efter 2014 får ROSTEC en tydligt förstärkt roll i Rysslands hybridstrategi. Vapensystem, militär teknologi och försvarsrelaterade tjänster exporteras i ökande omfattning till Mellanöstern, Afrika och Asien. Dessa leveranser sker sällan isolerat. De kombineras ofta med utbildning, tekniskt underhåll, säkerhetsrådgivning och i vissa fall även informationspåverkan. Resultatet blir långsiktiga beroenden där mottagarländer binds tekniskt, logistiskt och doktrinärt till rysk försvarsteknologi. Detta skapar inte bara intäkter, utan även politiskt inflytande och säkerhetspolitiskt handlingsutrymme för Moskva.

I flera fall sammanfaller ROSTECs vapenexport med diplomatiskt stöd till Ryssland i internationella forum eller med tillträde till naturresurser, baseringsmöjligheter och politiskt inflytande i strategiskt viktiga regioner. Leveranser till Syrien har fungerat både som militär testmiljö och som strategisk signalering gentemot NATO, medan affärer i afrikanska stater ofta kombineras med säkerhetsrådgivning, informationspåverkan och resurskontrakt. ROSTEC fungerar därmed inte enbart som industrikoncern, utan som en civil fasad för rysk säkerhetspolitisk expansion, ofta i samspel med privata militära aktörer – särskilt tydligt före Wagner-krisen 2023.

ROSTEC låga transparens och täta koppling till staten gör bolaget särskilt lämpat för verksamhet i gråzonen mellan krig och fred. Kommersiella kontrakt blir bärare av militär och politisk effekt, samtidigt som den formella marknadsformen ger hög grad av förnekbarhet. Militär påverkan levereras via till synes normala affärsrelationer, vilket försvårar både juridisk och politisk respons från omvärlden.

Denna militär-industriella dimension kompletteras av andra statliga strukturer som förstärker hybridlogiken. Russian Railways får efter 2014 en ökad säkerhetspolitisk betydelse genom sin roll i militär logistik till Krim och Ukraina, genom styrning av exportflöden mot politiskt “vänliga” hamnar och korridorer samt genom infrastrukturprojekt som skapar beroenden i

angränsande länder. Logistik blir därmed ett maktmedel: kontroll över tempo, riktning och sårbarhet i både civila och militära flöden.

Parallellt skärps den statliga modellen för ”krysha” – beskydd i utbyte mot lojalitet – som nu får en tydlig extern dimension. Bolag och aktörer som deltar i sanktionsundandragande eller strategiskt viktiga upplägg skyddas av staten, medan aktörer som samarbetar med väst kan straffas retroaktivt genom rättsliga eller administrativa medel. I detta sammanhang används även kriminella nätverk som möjliggörare för penningtvätt, transporter och sabotage. Kriminalitet blir därmed inte ett avsteg från statlig kontroll, utan en outsourcad statskapacitet inom ramen för hybridkrigföringen.

Sammantaget visar ROSTEC och de kringliggande strukturerna hur den ryska modellen för ekonomisk centralisering efter 2014 utvecklas till ett fullskaligt hybridverktyg. Strategiska företag används inte bara för intern disciplinering av eliter och kapital, utan för extern påverkan genom försvar, energi, investeringar, handel, transport och logistik. Dessa flöden är inte biprodukter av geopolitiken, utan centrala instrument i den. Den avgörande poängen är att påverkan i stor utsträckning sker under tröskeln för formell konflikt och juridisk eskalation. Det är just denna kombination av marknadsform, statlig styrning och förnekbarhet som gör den ryska statskapitalismen – och i synnerhet ROSTECs militär-industriella roll – till en bärande komponent i Rysslands hybridkrigföring mot Europa efter 2014.

## **PMESII-mappning av ROSTEC som hybridverktyg**

### **ROSTEC – Militär och ekonomisk påverkan (M / E)**

ROSTEC verkar främst i den militära (M) domänen, men med stark koppling till den ekonomiska (E). Bolaget utgör länken mellan rysk försvarsindustri, militär kapacitet och internationella beroendestrukturer.

I den militära domänen levererar ROSTEC vapensystem, teknologi, underhåll och utbildning till stater och aktörer utanför NATO-sfären. Detta skapar långsiktiga beroenden eftersom mottagarna blir tekniskt, logistiskt och doktrinärt knutna till rysk materiel. Effekten är inte nödvändigtvis omedelbar stridsförmåga, utan ett uthålligt militärt inflytande.

I den ekonomiska domänen används vapenexport och industriella samarbeten för att säkra intäkter, tillgång till råvaror och politiskt inflytande. Försvarsaffärer kombineras ofta med kreditlösningar, motköp eller infrastruktursamarbeten, vilket ytterligare binder mottagarstaterna till Ryssland.

ROSTEC har även kopplingar till Information (I) genom att rysk militär teknik demonstreras i skarpa konflikter (exempelvis Syrien), vilket fungerar både som marknadsföring och strategisk signalering.

*Sammanfattning ROSTEC: ROSTEC är ett M/E-verktyg som använder försvarsindustri och militär export för att skapa säkerhetspolitiska beroenden och geopolitisk räckvidd.*

**PMESII-Heatmap EU/Sverige per bolag:**

- GAZPROM
- ROSNEFT
- ROSTEC

Skala: Låg /Medel /Hög (påverkansgrad mot EU/Sverige). Bedömningen avser hybridpåverkan under tröskeln för öppen konflikt, inklusive sanktions- och gråzonslogik.

**GAZPROM – (Gas)**

- P (Political): Medel–Hög. Energiosäkerhet driver splittring inom EU, pressar nationella regeringar och skapar utrymme för “undantag”, bilaterala deals och populistisk mobilisering.
- M (Military): Låg. Indirekt, via samhällsstress och resiliens.
- E (Economic): Hög. Pris- och volymchocker påverkar inflation, industri, statsfinanser och konkurrenskraft.
- S (Social): Medel. Högre energipriser ger protester, polarisation, misstro och social stress.
- I (Information): Medel. Narrativ om “tekniska problem”, “marknadslogik” och “EU:s eget fel” används för förnekbarhet och splittring.
- I (Infrastructure): Hög. Kontroll över flöden (pipeline/logistik/lager) och beroenden i energisystemet.

Domänprofil: E/I (starkast), sedan P/S som följd effekter.

**ROSNEFT – (Olja/kapital/handel)**

- P (Political): Medel–Hög. Ägande, Joint Ventures och investeringar i tredjeländer skapar diplomatiskt stöd/neutralitet och motstånd mot skärpta åtgärder.
- M (Military): Låg–Medel. Indirekt genom intäktsflöden som finansierar statens militära uthållighet.
- E (Economic): Hög. Sanktionsresiliens via traders, blandning, omlastning och omdirigering av exportflöden.
- S (Social): Låg–Medel. Effekter via energipriser och finansiering av konflikter som driver sekundära migrations- och stabilitetsrisker.
- I (Information): Medel. Narrativ om “legitim handel”, “energisäkerhet” och “global syd” för att legitimera alternativa flöden.

- I (Infrastructure): Medel. Påverkan via shipping, hamnar, terminaler, raffinaderiflöden och logistik i tredjeländer.

Domänprofil: E/P (starkast), därefter I/I som möjliggörare.

### **ROSTEC – (Försvar/industri/teknologi)**

- P (Political): Medel. Skapar politiska beroenden via vapenexport, serviceavtal och industripaket; påverkar röstningsmönster och EU-linjer indirekt.
- M (Military): Hög. Militär kapacitet, export, service/utbildning, teknologispridning och “combat-proven” signalering.
- E (Economic): Medel–Hög. Teknologiförsörjning, kringgående av exportkontroll, komponentanskaffning via tredjeland.
- S (Social): Låg–Medel. Indirekt via konfliktförlängning som driver instabilitet och sekundära effekter.
- I (Information): Medel. Marknadsföring av krigserfaren teknik, psykologisk signalering, narrativ om västlig svaghet.
- I (Infrastructure): Medel. Militär infrastruktur i tredjeländer (baser, depåer, radar/sensorer), underhållsnoder, beroenden.

Domänprofil: M/E (starkast), därefter I/I som möjliggörare.

## KAPITEL 9 – KOPPLING TILL TOTALFÖRSVARET OCH KRITISK INFRASTRUKTUR (SVERIGE/EU)

### 1. Totalförsvarets logik: från “skydd” till “systemresiliens”

Totalförsvaret behöver behandla dessa bolag som systempåverkare snarare än enbart “utländska företag”. Hotet ligger i samverkande effekter: energi (GAZPROM) → ekonomi och social stabilitet → politiskt beslutsutrymme; oljeintäkter och handelsstrukturer (ROSNEFT) → uthållig rysk handlingsfrihet; försvarsteknologi och export/anskaffning (ROSTEC) → militär kapacitet och teknologiskt läckage.

### 2. Kritiska infrastrukturektorer som berörs direkt/indirekt

- a. Energi: gasmarknad, elpris, industriförsörjning, reservkraft, energilagrar.
- b. Transport/logistik: hamnar, terminaler, shipping, järnvägskorridorer, depåer (särskilt vid omlastning/ursprung).
- c. Telekom/IT/OT: industriell styrning (OT), komponentförsörjning, cyberrisker i leverantörsled.
- d. Finans: betalflöden, handelshus, försäkring, rederifinansiering, sanktionsefterlevnad.
- e. Försvars- och dual-use industri: exportkontroll, återexport, “frontbolag”, teknologimigrering.

### 3. Praktisk implikation för Sverige

För Sverige innebär detta att resiliensåtgärder inte bara är fysiska skydd (skyddsobjekt) utan också:

- a. leverantörsleds-säkerhet (ägende, nyttjanderätt, kontroll, mellanhänder),
- b. sanktions- och exportkontrollkapacitet (myndighet + näringsliv),
- c. informationsresiliens (förnekbarhet och narrativförskjutning),
- d. samordning civilt–militärt (Totalförsvarets kärna).

### Early Warning-indikatorlista baserad på PMESII per sektor (EU/Sverige)

Nedan indikatorer är formulerade så att de kan användas i en “watchlist” (myndighet, bolag, branschorgan). Tanken är mönsterigenkänning, inte beviskrav i domstol.

#### Political (P) – indikatorer

- Plötslig ökning av politiska krav på “undantag” från sanktioner/exportkontroll med hänvisning till energisäkerhet eller industrijobb.

- Ökad bilateralism (enskilda länder gör egna energi-/handelslösningar) i strid med EU-samordning.
- Återkommande röstningsmönster i internationella forum där energipartners konsekvent dämpar kritik mot Ryssland.
- Lobbying via indirekta kanaler (branschföreningar, konsultled, “oberoende” expertgrupper) med identiska argumentationslinjer.

### **Military (M) – indikatorer**

- Ökad “combat-proven”-marknadsföring av rysk teknik kopplat till stora exportaffärer.
- Nya service-/underhållshubbar i tredjeländer som ökar rysk räckvidd (depåer, utbildningscenter, radar/sensor).
- Försök att köpa eller reparera dual-use komponenter via tredjeland som nyligen ökat sin handel med Ryssland.
- Ovanligt ökade förfrågningar på svensk/europeisk försvars- och dual-use kompetens via mellanhänder.

### **Economic (E) – indikatorer**

- Skarp ökning av handel i “hög-risk-varukoder” (dual-use, elektronik, maskiner) till transitländer som samtidigt ökar export till Ryssland.
- Nya traderbolag med kort historik, stora volymer och otydliga ägarbilder i UAE/Turkiet/Hongkong med flera.
- Ovanliga rabatter, betalningsvillkor eller priskonstruktioner för energirelaterade kontrakt.
- Försäkrings- och finansieringsupplägg som snabbt flyttar mellan jurisdiktioner (“jurisdiction hopping”).

### **Social (S) – indikatorer**

- Samordnade kampanjer som kopplar energipriser/levnadskostnader till krav på att minska stöd till Ukraina eller att lämna EU/NATO-linjer.
- Snabb spridning av protestnarrativ med identiska memes/budskap över flera länder.
- Tydlig korrelation mellan energichocker och politisk polarisering (valrörelser, misstro mot institutioner).

**Information (I) – indikatorer**

- “Tekniska problem”-narrativ återkommer synkroniserat med strategiska leverans- eller prisförändringar.
- Plötslig ökning av “experter” och debattartiklar som normaliserar handel/beroende (“pragmatism”) och angriper sanktionspolitikens legitimitet.
- Desinformationsmönster som flyttar skuld från Ryssland till EU (energi, migration, inflation) med hög förnekbarhet.
- Koordinerad påverkan mot exportkontroll och försvarsindustrins legitimitet (“krigsprofitörer”, “onödigt”).

**Infrastructure (I) – indikatorer**

- Ökade ship-to-ship transfers i kända omlastningsområden och ökad “dark fleet”-aktivitet kopplad till EU-nära vatten.
- Plötsliga förändringar i lagerstrategi, terminalflöden eller rutt-mönster som saknar kommersiell logik.
- Ägar- eller driftsförändringar i logistiknoder (hamnar, lager, terminaler) via frontbolag eller otydliga koncernstrukturer.
- Upprepade cyber- eller sabotageincidenter i anslutning till energisystem, hamnar eller transportflöden (särskilt med svag attribuering).

**Indikatorer mappade mot svenska aktörer****Political (P)**

Indikatorer: krav på sanktionsundantag, bilaterala “speciallösningar”, koordinerad lobbying, röstningsmönster/tryck i internationella fora.

Primärt ansvar / ledning:

- Säpo: påverkan, otillbörlig påverkan, proxy-/frontkanaler, kopplingar till främmande makt.
- MCF: samordnad lägesbild om samhällspåverkan och resiliens (särskilt om P drivs av E/S).

Stöd/partners:

- Finansinspektionen: finansiell lobbying/kapitalpåverkan, marknadsbeteende som riskerar finansiell stabilitet.
- EI/PTS: sakunderlag som motverkar politiserad “teknisk” argumentation (energi/telekom).

## **Military (M)**

Indikatorer: export av “combat-proven” system, service-/underhållshubbar i tredjeländer, anskaffning av dual-use via mellanhänder, ovanliga förfrågningar till svensk industri.

Primärt ansvar / ledning:

- FMV: leverantörsled, kravställning, exportkontrollnära ”due diligence” i försvarsupphandling/industriell samverkan.
- Tullverket: gränskontroll av dual-use/strategiska varor (tillsammans med relevanta tillståndsmyndigheter).
- Säpo: kontra-proliferation, industrispionage, otillåten kunskapsöverföring.

Stöd/partners:

- MCF: samhällskonsekvenser vid incidenter, samverkanskonferenser, informationsdelning.

## **Economic (E)**

Indikatorer: high-risk varukoder till transitländer, nya traderbolag med otydliga ägare, rabatt-/betalningsvillkor utan marknadslogik, “jurisdiction hopping”.

Primärt ansvar / ledning:

- Finansinspektionen: finansiell stabilitet, exponeringar, regelefterlevnad i banker/fonder/försäkring.
- Tullverket: handelsmönster, varuflöden, avvikande export/import.
- Säpo: ekonomiska nätverk kopplade till främmande makt/undandragande.

Stöd/partners:

- Hamnmyndigheter: operativa flödesavvikelser, terminaldata, oklar lastinformation.
- MCF: samlad konsekvensbedömning för samhällsekonomi/beredskap.

## **Social (S)**

Indikatorer: samordnade protestnarrativ kopplade till energipriser/levnadskostnader, snabb polarisering, kampanjer mot Ukraina-stöd/EU-linje.

Primärt ansvar / ledning:

- MCF: psykologiskt försvar, resiliens, samordning av lägesbild om samhällspåverkan.
- Säpo: om social mobilisering kopplas till främmande makt/otillbörlig påverkan.

Stöd/partners:

- EI/PTS: faktaunderlag som neutraliserar “tekniska” falska påståenden (energi/telekom).

### **Information (I)**

Indikatorer: synkade “tekniska problem”-narrativ vid leverans-/prisförändring, plötslig “expertflora”, attacker mot exportkontroll/försvar, skuldskifte-narrativ.

Primärt ansvar / ledning:

- MCF: upptäckt och motverkanskommunikation, samordning med samhällsaktörer.
- Säpo: påverkansoperationer och kopplingar till främmande makt.

Stöd/partners:

- PTS: telekomrelaterade incidenter och informationsmiljö kopplat till operatörer.
- EI: energisystemrelaterade narrativ, händelseförklaringar.

### **Infrastructure (I) – kritisk infrastruktur**

Indikatorer: STS-omlastningar/dark-fleet-mönster, abrupta lager-/ruttförändringar, ägar-/driftsförändringar via frontbolag, cyber/sabotage med svag attribuering.

Primärt ansvar / ledning:

- EI: energiinfrastruktur, driftstabilitet, beredskapsåtgärder och systemrisk.
- PTS: elektronisk kommunikation, redundans, incidentrapportering.
- Hamnmyndigheter: hamn/terminal-drift, AIS-mönster, last- och anlöpsavvikelser.
- MCF: samordning av kritisk infrastruktur-resiliens och tvärsektoriell lägesbild.
- Säpo: säkerhetsskydd, sabotage/underrättelsehot mot skyddsobjekt och kritiska noder.
- Tullverket: kontrollpunkter i logistikledet (flöden, dokumentation, ursprung).

### **Övergripande syntes: företagen som modulära hybridverktyg**

Sett i PMESII-perspektiv fungerar ROSNEFT, GAZPROM och ROSTEC som specialiserade men samverkande moduler i risk hybridkrigföring:

- GAZPROM destabiliserar system och samhällsekonomi (E/I)
- ROSNEFT bygger politiska beroenden via kapital och energi (E/P)

- ROSTEC projicerar militärt inflytande via industri och export (M/E)

Tillsammans täcker de huvuddelen av PMESII-spektrumet utan att kräva öppen militär konfrontation. Detta förklarar varför rysk påverkan efter 2014 varit både svår att bemöta och långsiktigt effektiv: den sker sektorsvis, juridiskt fragmenterat och ofta under tröskeln för traditionella säkerhetspolitiska svar.

### **Sammanfattning**

- Strategiska företag i Ryssland är hybridinstitutioner – samtidigt bolag och statliga verktyg.
- Ekonomiska beslut (pris, leverans, investering) kan användas politiskt utan att bryta avtal.
- *Siloviki* fungerar som bryggor mellan säkerhet, ekonomi och politik.
- Kriminalitet och selektiv legalitet är inte avvikelser – de är styrmedel.

Detta är den modell som Ryssland senare projicerar externt i form av energipåverkan, sanktionsundandragande, proxy-bolag och ekonomisk infiltration i Europa

## **Sammanfattande hotbild: andra ryska statskontrollerade verksamheter med hög relevans för Sverige**

Utöver GAZPROM, ROSNEFT och ROSTEC finns flera ryska statskontrollerade eller statligt orkestrerade verksamheter som utgör jämförbara – och i vissa avseenden mer svårdetekterade – hot mot Sverige. Gemensamt för dem är att de verkar i gränslandet mellan civil verksamhet, statlig styrning och underrättelse-/påverkanslogik, och att de kan utnyttja öppenhet, marknadsformer och juridisk förnekbarhet i Sverige och EU.

### **Tre exempel i de mest kritiska branscherna enligt PMESII, där hotbilden mot Sverige bedöms vara störst.**

#### **1. Cyber, it och underrättelsenära teknik**

PMESII: Information / Infrastructure / Military

##### **Exempel: KASPERSKY (och underrättelsenära ekosystem)**

Den ryska cyber- och IT-sektorn, särskilt inom säkerhetsprogramvara, utgör ett systemhot i Informations- och Infrastrukturdomänen. Även när företag uppträder som kommersiella aktörer är de i praktiken underkastade rysk lagstiftning, inklusive krav på samarbete med säkerhetstjänster.

KASPERSKY är det mest välkända exemplet. Bolaget har under lång tid haft stark närvaro i Europa och Norden och erbjuder produkter som, per definition, kräver djup systemåtkomst. Även utan bevis för aktiv manipulation innebär detta en strukturell sårbarhet: uppdateringskanaler, telemetri och kodbas kan utnyttjas för underrättelseinhämtning, kartläggning eller i värsta fall förberedelse för sabotage.

För Sverige är hotet inte begränsat till enskilda produkter, utan till ekosystemet av IT-tjänster, konsulter, molnkopplingar och underleverantörer med ryska band. I ett PMESII-perspektiv innebär detta att informationsdomänen kan angripas via infrastrukturella beroenden, med potentiell militär relevans vid kris eller konflikt.

**Hotets kärna:** Inte aktiv cyberattack i vardagstid – utan strategisk åtkomst och förhandspositionering.

## 2. Kärnkraft, energi och kritisk teknik

PMESII: Infrastructure / Political / Economic

### Exempel: ROSATOM

ROSATOM är i PMESII-termer ett av de farligaste ryska instrumenten mot europeiska stater, eftersom verksamheten kombinerar kritisk infrastruktur, långsiktiga kontrakt, tekniskt beroende och politisk hävstång.

Bolaget erbjuder inte bara kärnbränsle och teknik, utan hela paket: finansiering, utbildning, driftstöd och avfallshantering. Detta skapar decennielånga beroenden. Även om Sverige inte bygger nya reaktorer med ROSATOM, påverkas Sverige indirekt genom EU:s och närområdets energisystem, bränslecykler och gemensam elmarknad.

ROSATOM har dessutom i flera länder fungerat som politisk påverkanskanal, där energisäkerhet kopplas till utrikespolitisk lojalitet eller återhållsamhet mot Ryssland. För Sverige innebär detta risk för strategisk inlåsning i ett europeiskt energisystem där ryska intressen fortfarande kan utöva påverkan, trots sanktioner.

**Hotets kärna:** Infrastrukturberoende som politiskt vapen, med extremt lång tidshorisont.

## 3. Transport, sjöfart och logistik

PMESII: Infrastructure / Economic / Military

### Exempel: rysk statskontrollerad sjöfart, hamn- och logistikintressen kopplade till staten (särskilt via ryska statliga transport- och handelsstrukturer)

Transport- och logistiksektorn är en underskattad men kritisk hotvektor för Sverige, särskilt i Östersjöregionen. Ryska statliga och statskontrollerade aktörer har historiskt haft intressen i sjöfart, rederier, hamntjänster, försäkring och bulktransporter.

I ett hybridperspektiv handlar hotet inte främst om militär blockad, utan om:

- I. kartläggning av flöden,
- II. åtkomst till hamn- och terminalinformation,
- III. möjlighet till sabotage, fördröjning eller desinformation vid kris.

I kombination med *dark fleet*-fenomenet, sanktionsundandragande och bristande transparens i ägarstrukturer utgör detta en systemrisk för Sveriges försörjningsberedskap.

Transportdomänen är dessutom central för militär rörlighet inom NATO, vilket ger direkt militär relevans.

**Hotets kärna:** Kontroll över tempo, riktning och sårbarhet i samhällskritiska flöden.

## Samlad analys – de största hoten i PMESII-perspektiv

De största hoten mot Sverige från andra ryska statskontrollerade verksamheter än GAZPROM, ROSNEFT och ROSTEC kan sammanfattas i tre övergripande mekanismer:

- I. **Förhandspositionering i kritiska system:**  
IT, energi och logistik används för att skapa latent åtkomst som kan aktiveras vid kris.
- II. **Långsiktig beroendebyggnad snarare än akut påverkan:**  
Kontrakt, teknikval och standarder låser in samhällen över tid.
- III. **Förnekbarhet genom marknadsform:**  
All verksamhet kan försvaras som kommersiell, teknisk eller juridisk – tills den används strategiskt.

I PMESII-termer är hoten mot Sverige i första hand koncentrerade till:

- **Infrastructure** (energi, IT, transport)
- **Information** (underrättelse, narrativ, systemåtkomst)
- **Economic** (flöden, beroenden, sanktionsresiliens)

Den militära effekten är oftast sekundär men avgörande i skarpt läge.

## KAPITEL 10 – SVERIGESPECIFIK HOTPRIORITERING – TOPP 10 (PMESII/HYBRID)

### **1. Förhandspositionering i IT/OT (informationsteknik/operational technology) i kritisk infrastruktur**

PMESII: Information / Infrastructure

Varför topp 1: Systemåtkomst i driftmiljöer (OT), identitetshantering, uppdateringskedjor och underleverantörer möjliggör kartläggning och sabotageförberedelse utan att något “händer” förrän i skarpt läge.

### **2. Påverkan och sabotage mot energisystemet (el, fjärrvärme, bränslelogistik)**

PMESII: Infrastructure / Economic / Political

Kärna: Störningar, desinformation vid incidenter, samt beroenden i import/logistik och prissignalers samhällseffekt.

### **3. Logistik och hamnar i Östersjö- och västkustflöden**

PMESII: Infrastructure / Economic / Military

Kärna: Tillgång till hamn/terminaldata, flödesstyrning, “legitima” aktörer som ger underrättelsenära åtkomst, samt sanktionsundandragande/dark fleet-relaterade mönster.

### **4. Dual-use och försvarsindustriellt kunskapsläckage via mellanhänder**

PMESII: Military / Economic / Information

Kärna: Komponentanskaffning, rekrytering av kompetens, konsultkedjor, återexport. Påverkar både svensk försvarsförmåga och Rysslands.

### **5. Finans, handel och AML – sanktionsundandragande och kapitalrörelser**

PMESII: Economic / Political

Kärna: Frontbolag, traders, nya ägarstrukturer, skenavtal, samt användning av EU/SE-jurisdiktion för legitimitet.

### **6. Underrättelseinhämtning via kommersiella ekosystem**

PMESII: Information / Political

Kärna: Affärsnätverk, event, konsultrelationer, akademi, teknikpartners, “due diligence”-luckor. Fokus på beslutsfattare, upphandlingar och sårbarheter.

### **7. Informationspåverkan riktad mot svensk sammanhållning och försvarsvilja**

PMESII: Information / Social / Political

Kärna: Narrativ om energi, inflation, NATO, Ukraina-stöd, “elit vs folk”, samt exploatering av lokala konflikter. Syfte: polarisering och beslutsförlamning.

## 8. Telekom- och satellitberoenden (inkl. underhåll/leverantörsled)

PMESII: Infrastructure / Information

Kärna: Redundans, incidenthantering, supply chain-risker och integritets-/signalspaningsrelevanta ytor.

## 9. Kommuner och kommunala bolag som “mjuka mål”

PMESII: Infrastructure / Economic / Social

Kärna: Upphandlingar, fastigheter, hamnar, energi, IT-drift. Ofta lägre säkerhetsskyddsmognad och stora konsekvenser vid störning.

## 10. Strategiska råvaror, avancerad tillverkning och FoU

PMESII: Economic / Military / Infrastructure

Kärna: Indirekta beroenden, teknologiska flaskhalsar, exportkontroll, samt långsiktig försvagning av svensk industriell bas.

### Exempel på svenska verksamheter som är exponerade för Topp-10 risker

Exemplen är konkreta, verklighetsnära exempel på företag och verksamheter i Sverige vilka illustrerar respektive Topp-10-risk, utan att antyda någon form av otillbörligt beteende. Syftet är att peka på riskexponering och sårbarhet, inte anklagelse.

Exemplen är valda för att de är systemiskt relevanta i PMESII-mening och välkända för svenska beslutsfattare.

### Svenska exempel per top-10-risk (PMESII/hybrid)

#### 1. Förhandspositionering i IT/OT (informationsteknik/operational technology) i kritisk infrastruktur

PMESII: Information / Infrastructure

Svenska exempel:

- Vattenfall – elproduktion, nät och industriella styrsystem (OT).
- E.ON Sverige – el- och värmedistribution med komplex leverantörskedja.

Varför relevant: OT-miljöer kräver fjärrsupport, uppdateringar och underhåll – attraktiva ytor för underrättelsenära förhandspositionering via leverantörsled.

#### 2. Energisystempåverkan (el, värme, bränslelogistik)

PMESII: Infrastructure / Economic / Political

Svenska exempel:

- Svenska kraftnät – systembalans, driftsäkerhet.
- Preem – raffinering och bränsleförsörjning.
- OKQ8 – distributionsled med samhällskritisk betydelse.

Varför relevant: Energiincidenter får omedelbara samhällseffekter och är tacksamma mål för informationspåverkan (“tekniska problem”, “marknadslogik”).

### **3. Logistik, hamnar och försörjningsflöden**

PMESII: Infrastructure / Economic / Military

Svenska exempel:

- Göteborgs Hamn – Sveriges största hamn.
- A.P. Møller – Maersk (stor närvaro i Sverige).
- Stena Line – ro-ro, passagerare, gods.

Varför relevant: Hamn- och terminaldata, ruttplanering och lastinformation är strategiskt värdefullt vid kris eller mobilisering.

### **4. Dual-use och försvarsindustriellt kunskapsläckage**

PMESII: Military / Economic / Information

Svenska exempel:

- Saab – avancerad försvars- och sensorsystemkompetens.
- Ericsson – dual-use teknik, radio, kryptering.
- ABB Sverige – industriell automation, kraftsystem.

Varför relevant: Kompetensrekrytering, konsulter, underleverantörer och återexport är vanliga gråzonsvektorer.

### **5. Finans, handel och AML – sanktionsundandragande**

PMESII: Economic / Political

Svenska exempel:

- SEB, Swedbank, Nordea – exponering mot handel, rederier, energi.
- Handelsbanken – företagskunder i känsliga sektorer.
- Carnegie – förmögna kunder och family offices.
- Nasdaq och NGM – handelsplatser för noterade bolag och aktier, verktyg för penningtvätt.

Varför relevant: Frontbolag, traders och transitjurisdiktioner kan nyttja svenska finansiella ekosystem för legitimitet ekonomisk brottslighet och penningtvätt.

## 6. Kommersiell underrättelseinhämtning via affärs ekosystem

PMESII: Information / Political

Svenska exempel:

- Almega (branschforum).
- IVA (policy/teknikdialog).
- Större management- och teknikkonsulter verksamma i Sverige.

Varför relevant: Event, nätverk, rådgivning och upphandlingar ger mjuk åtkomst till beslutsmiljöer.

## 7. Informationspåverkan mot sammanhållning och försvarsvilja

PMESII: Information / Social / Political

Svenska exempel (arenor snarare än bolag):

- Sociala plattformar, alternativa medier, kommentarsfält kopplade till energi, NATO och levnadskostnader.
- Mediestrukturer där innehåll kan amplificeras via bot-nät eller koordinerade narrativ.

Varför relevant: Låg kostnad, hög räckvidd, stark effekt på beslutsvilja.

## 8. Telekom och satellitberoenden

PMESII: Infrastructure / Information

Svenska exempel:

- Telia – nationell operatör.
- Telenor Sverige.
- Ericsson – leverantörsled.

Varför relevant: Redundans, mjukvara och leverantörsrelationer är avgörande i kris.

## 9. Kommuner och kommunala bolag

PMESII: Infrastructure / Economic / Social

Svenska exempel:

- Stockholm Exergi – fjärrvärme.
- Göteborg Energi.
- Kommunala hamn- och fastighetsbolag.

Varför relevant: Ofta lägre säkerhetsskyddsmognad, stora konsekvenser vid störning.

## 10. Strategiska råvaror, avancerad tillverkning och FoU

PMESII: Economic / Military / Infrastructure

Svenska exempel:

- LKAB – kritiska mineraler.
- Sandvik, SSAB – avancerad tillverkning.

Varför relevant: Långsiktiga beroenden, teknikval och leverantörspositioner.

### Viktig slutmarkering

*Dessa exempel illustrerar var hot kan uppstå, inte att hot redan föreligger. Den gemensamma nämnaren är systemisk betydelse i PMESII-termer: där civila marknader möter nationell säkerhet. Just därför krävs säkerhetsskydd, bolagsstyrning och Totalförsvaretänk även i verksamheter som formellt är kommersiella.*

### Koppling till säkerhetsskyddslagstiftning och bolagsstyrning

#### Säkerhetsskyddslagen: vad den i praktiken behöver fånga i dessa hot

Säkerhetsskydd handlar inte bara om hemlig information – utan om säkerhetskänslig verksamhet, vilket i svensk kontext ofta är drift, system, leveransförmåga och samhällskritiska flöden. De största glappen brukar uppstå när företag/organisationer:

1. Underskattar OT och leverantörskedjor som säkerhetskänsliga ("det är bara drift/IT").
2. Gör affärer/upphandlingar där kontroll och inflytande flyttas via driftavtal, fjärrsupport, underhåll, licenser eller molnkopplingar.
3. Har stark informationssäkerhet men svag personalsäkerhet och säkerhetsskyddade upphandlingar.

Konsekvens: För att möta Topp 10-listan behöver säkerhetsskyddsarbetet vara "system- och flödesorienterat", inte bara "klassningsorienterat".

Praktisk brygga: Topp 10 skapar behov av en styrmodell (kort)

- I. Om hotet rör Infrastructure/OT/telekom/energi/logistik: behandla som säkerhetsskyddad verksamhet och kräv säkerhetsskyddad upphandling + kontinuitetskrav.
- II. Om hotet rör Economic/AML/sanktioner: skala upp due diligence, transaktionsmonitorering och ägargranskning som strategiskt riskområde.
- III. Om hotet rör Information/Social: integrera psykologiskt försvar-resiliens i krisledning och kommunikation (inte bara PR).

## **Bolagsstyrning: styrelsens miniminivå i en hybridmiljö**

För svenska bolag (även privata) i kritiska sektorer bör styrelsen behandla detta som enterprise risk (strategisk risk), inte IT-risk.

### **Tre styrelsekrav som ofta saknas:**

- a. **Ägar- och kontrollanalys** i leverantörsled (beneficial ownership, jurisdiktion, inflytandekanaler).
- b. **Sanktions- och exportkontroll som styrelsefråga**, inte bara compliance.
- c. **Resiliens-KPI:er**: redundans, återstartstid, beroende av enskilda leverantörer, fjärråtkomstpunkter, logistikberoenden.

### **Styrelseformat som fungerar:**

- a. Inrätta ett "Security & Resilience Committee" eller tydliggör mandat i revisionsutskottet.
- b. Kräv kvartalsvis rapportering på: (i) leverantörsrisk, (ii) incidenttrend, (iii) geopolitisk exponering, (iv) säkerhetsskyddade avtal.

## **Förslag till styrelsepolicy för att möta de krav som den geopolitiska situationen kräver**

### **Hybridrisk, säkerhetsskydd och bolagsstyrning**

Syfte och tillämpning

Denna policy fastställer hur bolaget ska identifiera, styra och följa upp hybridrisker som påverkar säkerhetskänslig verksamhet, kritisk infrastruktur och långsiktig affärsresiliens. Policyn gäller styrelse, ledning och samtliga verksamheter inklusive dotterbolag och kritiska leverantörer.

### **Riskdefinition**

Hybridrisk avser påverkan som sker under tröskeln för öppen konflikt och kombinerar ekonomiska, tekniska, informationsmässiga och infrastrukturella metoder. Riskerna uppstår ofta via marknadsformer, kontrakt och leverantörsled, med hög förnekbarhet.

### **Styrelsens ansvar**

Styrelsen ansvarar för att hybridrisk behandlas som strategisk företagsrisk. Styrelsen ska årligen fastställa riskaptit för säkerhetskänslig verksamhet, besluta om resiliensmål samt säkerställa att säkerhetsskydd integreras i affärsstrategi, upphandling och investeringar.

### **Ledningens ansvar**

VD ansvarar för genomförande. COO (Chief Operating Officer) ansvarar för infrastruktur, kontinuitet och logistik. CFO (Chief Financial Officer) ansvarar för finansiell exponering, sanktioner och AML. CTO (Chief Technology Officer)/CISO (Chief Information Security

Officer) ansvarar för IT/OT, leverantörsled och teknisk resiliens. CHRO (Chief Human Resource Officer) ansvarar för personalsäkerhet och kompetensskydd.

### **Säkerhetsskydd i praktiken**

Säkerhetsskydd ska tillämpas på verksamheter där drift, system, flöden eller åtkomst är kritiska för samhällsfunktion eller försvar. Säkerhetsskyddad upphandling ska användas när leverantörer får faktisk kontroll eller åtkomst, inklusive fjärrsupport, licenser och molntjänster.

### **Bolagsstyrning och uppföljning**

Styrelsen ska kvartalsvis få rapportering om: (i) leverantörs- och ägarrisk, (ii) incidenter och indikatorer, (iii) geopolitisk exponering, (iv) resiliens-KPI:er (redundans, återstarttid, single-points-of-failure).

Ett Security & Resilience-utskott bör inrättas eller mandat ges till revisionsutskottet.

### **Beslutsprinciper**

Affärsbeslut som skapar långsiktigt beroende i kritiska system kräver styrelsebeslut. Ekonomisk nytta får inte prioriteras över förlust av kontroll, insyn eller återtagbarhet. Avtal ska innehålla exit-, audit- och incidentklausuler.

### **Samverkan**

Bolaget ska ha etablerade kontaktvägar med relevanta myndigheter och branschorgan för lägesbild, indikatorutbyte och incidenthantering

### **Strategisk slutsats för Sverige**

Sveriges sårbarhet ligger inte i brist på militär förmåga, utan i öppenhet, teknisk komplexitet och beroenden i civila system. Rysk statskapitalism och statligt orkestrerad näringsverksamhet riktar in sig just där: där civilt och militärt möts, men ansvaret är splittrat. Detta gör att hoten bäst möts inte med enskilda förbud, utan genom:

- a. systematisk PMESII-analys,
- b. starkare koppling mellan Totalförsvaret och näringslivet,
- c. tidig indikatorbaserad styrning snarare än reaktiv krishantering.
- d. löpande kunskapshöjande åtgärder för ledande befattningshavare i näringsliv, politik och statligt kontrollerade verksamheter
- e. införandet av obligatoriska krav som till exempel bakgrundskontroller och säkerhetscertifiering av alla styrelseledamöter, ledande befattningshavare och valberedningar i börsnoterade bolag.

## KAPITEL 11 – SVERIGE I FOKUS: TRE MARKNADER FÖR PÅVERKAN

I den hybridmiljö som beskrivits i detta kapitel kan näringslivet inte längre betraktas som en neutral arena skild från säkerhetspolitiken. Svenska företag är inte bara potentiella offer för ekonomisk brottslighet, utan kan – medvetet eller omedvetet – bli plattformar för strategisk påverkan.

Acta Publicas analys visar hur företag används för att etablera närvaro, bygga relationer och skapa ekonomiska beroenden. För näringslivet innebär detta ett behov av att utveckla säkerhetsmedveten bolagsstyrning. Det handlar inte om politisering av affärsbeslut, utan om att förstå att ägarstruktur, finansiering, partnerskap och leverantörskedjor i dag har säkerhetspolitiska implikationer.

Här finns en tydlig parallell till efterkrigstidens utveckling i andra europeiska länder, där företag successivt integrerats i totalförvarstänkandet. För svensk del innebär detta att due diligence, compliance och riskhantering behöver kompletteras med **geopolitisk riskanalys** – särskilt i sektorer med strategisk betydelse eller hög exponering mot internationella flöden

### **Näringslivet – ägande, partnerskap och leverantörskedjor**

Den första marknaden som identifieras i Acta Publicas material är näringslivet. I den ryska hybridmodellen utgör företag inte enbart ekonomiska enheter, utan potentiella underrättelseplattformar och inflytandekanaler. Detta sker sällan genom öppna övertaganden eller fientliga handlingar, utan genom gradvis integration i affärsnätverk, kapitalflöden och leverantörskedjor. Ett företag som etableras eller förvärvas i Sverige kan fungera som kontaktpunkt mot leverantörer, kunder, kommuner och myndigheter. Genom dessa relationer skapas tillgång till information, påverkan över beslut och möjlighet att identifiera sårbarheter. Den strategiska vinsten ligger därför inte i kortsiktig lönsamhet, utan i långsiktig positionering.

### **Åtgärder för att minska påverkan i näringslivet**

- a. För att minska påverkan i näringslivet behöver Sverige och svenska företag stärka sin förmåga att bedöma risk utifrån strategisk effekt snarare än enbart legala formalia. Först och främst krävs en tydligare normbildning där geopolitisk risk blir en del av företagsstyrning, särskilt i branscher som är infrastrukturbärande eller teknologiskt känsliga. Detta bör operationaliseras genom att styrelser och ledningar ges ett tydligt ansvar för säkerhetsrelaterad risk, i linje med hur man hanterar finansiell och regulatorisk risk. När ansvar är tydligt blir det också möjligt att följa upp.
- b. En central åtgärd är att utveckla due diligence från traditionell compliance till säkerhetsinformerad due diligence, där ägarstrukturer, finansieringskällor, affärspartners och leverantörskedjor granskas utifrån kopplingsrisker, återkommande mellanled och mönster som tyder på proxy- eller frontbolagsupplägg. Här är målet inte att kriminalisera affärsrelationer, utan att reducera exponering och undvika långsiktiga

beroenden som senare kan utnyttjas. I praktiken kräver detta att företag har tillgång till relevant underrättelse- och riskinformation, vilket motiverar en mer formaliserad dialog mellan näringsliv och ansvariga myndigheter inom ramen för skyddsvärd verksamhet.

- c. Vidare behöver Sverige skapa tydligare och mer praktiska mekanismer för att hantera risk vid investeringar, förvärv och kritiska leverantörsavtal. Detta handlar inte nödvändigtvis om generella förbud, utan om att bygga processer som fångar upp risk tidigt och möjliggör villkor, säkerhetskrav eller i vissa fall avrådan. Det innebär också att företagens interna säkerhetsfunktioner måste stärkas: informationssäkerhet, personsäkerhet, resiliensplanering och incidentberedskap bör ses som delar av affärskontinuitet, inte som sidofunktioner.
- d. Slutligen behöver näringslivet förmåga att hantera påverkan i gränslandet mellan ekonomi och opinion. Informationspåverkan riktar sig ofta mot varumärken, leveranser och sociala konfliktytor. Företag måste därför ha beredskap för att identifiera och hantera koordinerade narrativangrepp, särskilt i samband med geopolitisk kris, sanktioner eller leveransstörningar. Den mest effektiva motåtgärden är förmågan att agera snabbt, transparent och konsekvent, och att minska risken för intern polarisering genom tydlig kriskommunikation och robusta rutiner.
- e. Bolags- och individcertifiering för att verka på börs. Nasdaq och NGM måste uppdatera sina villkor för emittenter och ställa motsvarande krav på riskutbildning som man har avseende börsregler med mera.

### **Finanssektorn – kapitalflöden, penningtvätt och gråzoner**

Den andra marknaden är finanssektorn, där hotet är särskilt komplext eftersom det ofta uppträder som fullt legitima transaktioner. Acta Publicas material visar hur kapital kan röra sig genom flera led, jurisdiktioner och bolag utan att någon enskild aktör bryter mot gällande regelverk. I hybridlogik är detta avgörande. Finansiella flöden fungerar som blodomloppet för andra påverkansmedel: cyberoperationer, informationskampanjer, logistik och proxies kräver finansiering. När kapital kan tvättas, omstruktureras och återinvesteras i legala verksamheter suddas gränsen mellan kriminalitet och geopolitik ut.

### **Åtgärder för att minska påverkan i finanssektorn**

- a. Den finansiella motståndskraften behöver bygga på en övergång från transaktionscentrerad kontroll till nätverks- och mönstercentrerad kontroll. Det viktigaste steget är att stärka kapaciteten att identifiera strukturer som återkommer över tid: samma möjliggörare, samma bolagskedjor, samma jurisdiktioner, samma typer av mellanhänder. Detta kräver analytiska metoder som i högre grad liknar underrättelseanalys än traditionell regelefterlevnad. För att detta ska fungera måste informationsdelning mellan banker, tillsynsmyndigheter och brottsbekämpande myndigheter vara praktiskt möjlig, snabb och rättssäker.

- b. En andra åtgärd är att säkerställa att riskbedömningar integrerar sanktionsevason och hybridkopplingar som explicit riskkategori. Sanktionsevason är inte enbart ett internationellt regelbrott; det är en möjliggörare för fortsatt aggression och destabilisering. Finansiella aktörer behöver därför ha interna processer som inte bara kontrollerar sanktionsträffar på individ- eller bolagsnamn, utan även fångar upp indirekta upplägg via ägarkedjor, bulvaner och ompaketerade flöden.
- c. Vidare behöver Sverige fokusera på de delar av finanssystemet där transparensen är strukturellt lägre och möjliggörarindustrin större: komplexa bolagsstrukturer, vissa typer av investmentupplägg, gränsöverskridande transaktioner med svag insyn och tjänster som kan användas för att dölja verkligt huvudmannaskap. Här handlar åtgärderna om att höja friktionen: ökad kravställning på dokumentation, tydligare ansvar hos mellanhänder och skärpt tillsyn där riskbilden motiverar det.
- d. Slutligen måste finanssektorn ses som en del av Sveriges totala motståndskraft. Ett väl fungerande system för rapportering av misstänkta transaktioner är nödvändigt men otillräckligt om responsen blir långsam och fragmenterad. För att minska påverkan behöver det finnas snabbare mekanismer för samordnad prioritering av ärenden med tydlig säkerhetspolitisk dimension, där målet inte bara är lagföring utan att bryta flöden, stoppa möjliggörare och reducera angriparens handlingsutrymme.

### **Offentlig sektor – kommuner, regioner och upphandling**

Den tredje marknaden är offentlig sektor. Här uppstår hybridmodellens mest känsliga dilemma. Svenska myndigheter och kommuner är bundna av lag, transparens och likabehandling. Dessa principer är grundläggande för demokratin, men de kan också exploateras av aktörer som agerar strategiskt under lagens yta. Acta Publicas rapport visar hur företag och individer med kopplingar till ryska kriminella nätverk kan delta i upphandlingar, etablera verksamhet och skapa beroenden utan att formella hinder uppstår. Detta innebär inte nödvändigtvis att regelverket är felaktigt, utan att det ofta saknar säkerhetspolitisk dimension.

### **Åtgärder för att minska påverkan i offentlig sektor**

- a. Den mest avgörande åtgärden i offentlig sektor är att integrera säkerhetsperspektiv i verksamheter som traditionellt betraktats som administrativa eller ekonomiska. Kommunal och regional upphandling, IT-drift, fastighetsförvaltning, omsorgstjänster och infrastrukturtjänster måste i större utsträckning analyseras som potentiella angreppsytor. Det innebär att upphandlings- och leverantörsstyrning behöver kompletteras med säkerhetskrav och riskbedömningar som går bortom pris, kapacitet och formell regelefterlevnad.
- b. För att detta ska vara möjligt krävs tydligare nationellt stöd till kommuner och regioner. I dag varierar säkerhetskompetens och resurser kraftigt. En effektiv motåtgärd är därför att utveckla gemensamma riskmodeller, vägledningar och praktiska stödstrukturer som kan användas i upphandling, leverantörskontroll och avtalsuppföljning. Detta bör

kombineras med en förbättrad förmåga att genomföra bakgrundskontroller och ägandekontroller när verksamheten är skyddsvärd eller när leverantören får tillgång till kritiska system.

- c. En andra åtgärd är att stärka tillsyn och uppföljning under avtalets hela livscykel. Hybridpåverkan sker ofta genom gradvis etablering: först ett kontrakt, därefter underleverantörer, därefter teknisk åtkomst eller ekonomiskt beroende. Offentlig sektor behöver därför bygga rutiner som inte enbart granskar leverantören vid upphandlingstillfället, utan löpande bedömer förändringar i ägarstruktur, personal, underleverantörskedjor och incidentmönster.
- d. Slutligen måste den juridiska formalismen kompletteras med en praktisk förmåga att agera på riskindikationer även när brott inte kan styrkas. Detta kräver inte att rättssäkerheten överges, men att man bygger beslutskedjor där säkerhetsbedömningar kan leda till proportionella åtgärder: krav på åtgärdsplan, begränsad åtkomst, förstärkt kontroll, eller i vissa fall avveckling av beroenden. Den offentliga sektorns motståndskraft vilar i slutänden på dess förmåga att minska sårbarheter innan de kan utnyttjas.

## KAPITEL 12 – STRATEGISKA IMPLIKATIONER FÖR SVERIGE OCH EUROPA

Förslag till 12 reformspår som tillsammans minimerar påverkan i Marknad I–III och samtidigt binder ihop cyber, FIMI och fysisk sabotageproblematik:

- a) **Nationellt “gråzonsmandat” för samordning**  
Etablera en tydlig operativ modell för hur svaga signaler över sektorer ska vägas samman (ekonomi + cyber + FIMI + fysisk påverkan). Acta understryker att fragmentering gynnar motståndaren.
- b) **Säkerhetsinformerad due diligence som norm i strategiska sektorer**  
Komplettera juridisk/finansiell DD med ägarkedjeanalys, möjliggörarled, sanktionskopplingar och underrättelseperspektiv.
- c) **Skifte i finans: från kundrisk till systemrisk**  
Byggkrav och metoder för nätverksanalys (återkommande möjliggörare, kedjor, jurisdiktioner), i linje med Actas kärnsikt.
- d) **Kommunal/regional miniminivå för cybersäkerhet i kritiska funktioner**  
Särskilt vatten, fastighet, vårdnära system och IT-drift; koppla upphandling till faktiska säkerhetskrav.
- e) **“Informationsresiliens” som obligatorisk del i krisledning**  
FIMI hanteras parallellt med teknisk incident, inte efteråt.
- f) **Upphandling som säkerhetsinstrument**  
Inför standardiserade säkerhetsklausuler: ägartransparens, underleverantörskontroll, förändringsplikt, revisionsrätt, incidentrapportering, exit-klausuler. Acta pekar ut upphandling som frontlinje.
- g) **Stärkt investering- och ägargranskning i skyddsvärd verksamhet**  
Sverige har redan FDI-screening via ISP; nyttja det som praktiskt nav och integrera erfarenheter i kommunal/bolagsstyrning.
- h) **Kritisk infrastruktur till havs: juridik + övervakning + respons**  
Utveckla lagstiftnings- och samverkanslinjer för undervattenskablar där attribution är svår; SIPRI pekar på rättsliga hinder och behov av lagstiftningsvägar.
- i) **Kompetenslyft i offentlig sektor (geopolitik + ekonomisk brottslighet + underrättelsemetodik)**  
Acta: utbildning är akut och offentlig sektor är särskilt utsatt.
- j) **Möjliggörarbekämpning: målvakter, bolagskedjor, identitetsmissbruk**  
Flytta fokus från “enstaka bolag” till ekosystem: registrering, verklig huvudman, kontroll över flera led.

**k) Sanktionsevasion som säkerhetshot i praktiken**

Bygg operativa processer där sanktionsefterlevnad, exportkontroll och ekonomisk brottslighet knyts till hybridbilden.

**l) Övning och mätning: “kampanjlogik” i stället för incidentlogik**

Inför återkommande övningar som simulerar kedjor: cyber → desinformation → leverantörskris → fysisk störning.

**m) Verifiering och certifiering av ledande befattningshavare, styrelser och valberedning****Policypaket – från åtgärder till sammanhållen svensk policy****Policy 1:** Erkänn statstjänande kriminalitet som nationellt säkerhetshot

Sverige bör formellt erkänna organiserad brottslighet och ekonomisk infiltration kopplad till främmande makt som ett nationellt säkerhetshot. Detta kräver att säkerhetsperspektivet integreras i politikområden som näringsliv, finans, upphandling och regional förvaltning – inte enbart i försvar och underrättelse.

**Policy 2:** Säkerhetsinformerad due diligence som nationell standard

I strategiska sektorer ska due diligence omfatta ägarkedjor, verkligt huvudmannskap, finansiering, möjliggörarstrukturer och geopolitisk risk. Detta bör införas som norm i statliga bolag, kommunala bolag och verksamheter av samhällskritisk betydelse.

**Policy 3:** Skifte från kundrisk till systemrisk i finanssektorn

Finansiell tillsyn ska prioritera nätverks- och mönsteranalys. Informationsdelning mellan banker, tillsynsmyndigheter och brottsbekämpande organ ska möjliggöra snabb identifiering av återkommande möjliggörare, målvakter och strukturer.

**Policy 4:** Upphandling som säkerhetsinstrument

Offentlig upphandling ska systematiskt inkludera säkerhetskrav, ägar- och underleverantörskontroller samt rätt till uppföljning och hävning vid förändrad riskprofil. Upphandling betraktas därmed som en del av totalförsvaret.

**Policy 5:** Nationell baslinje för cybersäkerhet i kommuner och regioner

Alla kommuner och regioner ska uppfylla en gemensam miniminivå för cybersäkerhet i kritiska funktioner (vatten, fastighet, IT-drift, vårdnära system), med statligt stöd för kompetens och implementering.

**Policy 6:** Informationspåverkan som del av krisledning

FIMI ska hanteras parallellt med tekniska och fysiska incidenter. Kommuner, regioner och myndigheter ska ha rutiner för snabb faktapublicering, rykteshantering och samordnad kommunikation.

**Policy 7: Stärkt skydd mot ekonomisk infiltration i offentlig sektor**

Kommuner och regioner ska ges tydliga mandat och stöd för att beakta säkerhetsrisk vid tillstånd, etablering, bidrag och driftavtal – även när formella lagöverträdelser inte kan styrkas.

**Policy 8: Fokus på möjliggörarstrukturer**

Åtgärder ska riktas mot målvakter, skenbolag, identitetsmissbruk och professionella möjliggörare. Bekämpning av dessa strukturer ger hög säkerhetseffekt till relativt låg kostnad.

**Policy 9: Sanktionsevasion som operativt säkerhetshot**

Sanktionsefterlevnad ska integreras i nationell säkerhetsplanering. Sanktionsundandragande ska mötas med snabba, samordnade åtgärder för att bryta flöden, inte enbart med efterhandsjuridik.

**Policy 10: Utbildning som kärna i motståndskraft**

Obligatorisk utbildning i hybridkrigföring, ekonomisk brottslighet och säkerhetsrisk ska införas för nyckelroller i kommuner, regioner, statliga bolag och strategiska företag.

**Policy 11: Kampanjlogik i övning och planering**

Övningar och beredskapsplanering ska utgå från kampanjlogik, där cyber, påverkan, ekonomi och fysisk subversion samverkar över tid, snarare än isolerade scenarier.

**Policy 12: Sammanhållen nationell tillämpning**

Slutligen krävs en sammanhållen nationell tillämpning där fragmentering motverkas genom gemensamma hotbilder, samordning och tydligt politiskt ansvar.

## AVSLUTANDE ANALYS, SAMMANFATTNING OCH REKOMMENDATION

Denna rapport har genom ett långt historiskt, institutionellt och systemanalytiskt perspektiv visat att rysk organiserad brottslighet inte kan förstås som ett avvikande eller parasitiskt fenomen vid sidan av staten. Tvärtom framträder kriminalitet, informella nätverk och gråzonsekonomier som återkommande och funktionella komponenter i rysk statlig maktutövning. Från tsartidens *razboyniki* via Gulags tvångsekonomi och *vory v zakone* till dagens hybridkrigföring.

Under krigströskeln löper en tydlig kontinuitet: när formella institutioner varit svaga, ineffektiva eller politiskt oprioriterade har informella och ofta kriminella strukturer ersatt, kompletterat eller absorberats av staten. Det är denna strukturella logik – snarare än enskilda aktörer – som utgör kärnan i hotbilden.

Rapportens samlade analys visar att den moderna ryska staten bör förstås som en hybridstat, där gränsen mellan lagligt och olagligt, offentligt och privat, statligt och kriminellt är medvetet flytande. Denna flytande gräns är inte ett tecken på systemkollaps, utan på systemfunktion. Organiserad brottslighet används modulärt: som verktyg för kapitalackumulation, sanktionsundandragande, informationspåverkan, fysisk subversion och strategisk påverkan på andra staters samhällsstrukturer. I detta perspektiv blir kriminalitet inte ett ordningsproblem utan en styrningsmetod, integrerad i statens sätt att skapa handlingsfrihet och strategisk effekt.

För Sverige och Europa innebär detta ett fundamentalt analytiskt skifte. Hotet från Ryssland manifesteras sällan genom öppna militära angrepp (med undantag av Ukraina) eller tydliga brottsliga handlingar. I stället verkar det genom vardagliga strukturer: bolagsägande, kapitalflöden, leverantörskedjor, upphandlingar, informationsmiljöer och juridiska gråzoner. Var och en av dessa företeelser kan framstå som isolerad, laglig eller administrativt hanterbar. Först när de betraktas som delar av ett sammanhängande system framträder deras strategiska betydelse. Det är ackumulationen av små, förnekbara handlingar som skapar systemisk effekt och undergräver motståndskraft, tillit och strategiskt handlingsutrymme.

Rapportens slutsats är därför att Sverige inte står inför ett framtida hot, utan befinner sig mitt i ett pågående strukturellt angrepp. Ett reaktivt, incidentbaserat förhållningssätt – där varje händelse bedöms för sig och inom snäva sektorsramar – är otillräckligt. Så länge analys och styrning bygger på västerländska antaganden om en tydlig åtskillnad mellan stat och brott riskerar centrala delar av hotbilden att förbli osynliga eller felklassificerade.

### **Mot denna bakgrund är den övergripande rekommendationen tydlig:**

1. Sverige behöver utveckla ett sammanhållet, säkerhetspolitiskt raster för analys och styrning av ekonomiska, juridiska och institutionella processer.

2. Detta innebär att frågor om ägande, finansiering, upphandling, infrastruktur och informationsmiljö inte enbart kan behandlas som marknads-, förvaltnings- eller rättsfrågor, utan måste bedömas utifrån deras potentiella strategiska funktion.
3. Tillsyn och regelverk behöver kompletteras med riskbaserad analys som tar höjd för statstjänande kriminalitet och hybridpåverkan, även när dessa verkar inom lagens formella ramar.
4. Vidare krävs ett systematiskt kunskapslyft inom näringsliv, finanssektor och offentlig förvaltning. Förmågan att identifiera strukturella mönster, förstå långsiktiga beroenden och tolka gråzonsbeteenden måste stärkas genom utbildning, gemensamma analysramar och bättre samverkan mellan myndigheter och samhällssektorer.
5. Slutligen bör Sverige, i nära samarbete med europeiska partners, utveckla gemensamma normer och verktyg för att hantera denna typ av systemhot, som per definition överskrider nationella och sektoriella gränser.

Sammanfattningsvis visar rapporten att hotet inte ytterst ligger i den ryska statens militära kapacitet eller i enskilda kriminella nätverk, utan i en historiskt rotad styrningslogik där brottslighet, informella strukturer och statlig makt samverkar.

Att möta detta hot kräver därför inte bara fler regler eller hårdare straff, utan en djupare systemförståelse och ett medvetet skifte från reaktiv rättsstat till proaktiv strategisk resiliens.

Tillsammans utgör dessa policys en övergång från reaktiv försvarshållning till strategisk resiliens. De är utformade för att bevara rättsstatens principer samtidigt som Sverige anpassar sig till en säkerhetsmiljö där hot verkar genom laglighetens gränser.

Stockholm 2026

**CORPSEC INTERNATIONAL AB**

Jörgen Holmlund  
Styrelseordförande och medgrundare

Thomas Ahlerup  
VD och medgrundare

## BILAGA – BEDÖMNING AVSEENDE FÖREKOMST AV RYSK BROTTLIGHET MED KOPPLING TILL TRE SVENSKA RÄTTSFALL

Denna rapport utgår från en jämförande analys av tre svenska brottmålsdomar – en från Södertörns tingsrätt (2025), Luleå tingsrätt (2023) och en från Solna tingsrätt (2017) – vilka behandlar avancerade upplägg av grov organiserad penningtvätt och bedrägeribrottslighet. Genom en systematisk genomgång av domarnas faktiska omständigheter identifieras återkommande strukturer, däribland användning av målvakter, bolagskonstruktioner, osanna fakturor samt utnyttjande av kreditbaserade tillgångar såsom fordon, vilka omsätts, vidareförsäljs och i vissa fall exporteras utomlands.

Analysen visar att brottsuppläggen präglas av en funktionell arbetsdelning och en tydlig ekonomisk logik, där syftet är att generera, omsätta och dölja brottsvinster genom flerledade transaktioner och gränsöverskridande flöden. Särskilt framträdande är användningen av näringspenningtvätt genom bolagsstrukturer och konton i flera led, vilket möjliggör integrering av illegala medel i den legala ekonomin.

Mot bakgrund av tidigare forskning och myndighetsrapporter, bland annat från Polismyndigheten och Brottsförebyggande rådet, kan dessa mönster förstås som förenliga med etablerade former av organiserad brottslighet med ryskspråkig anknytning. Samtidigt bör kopplingen till Bratva och andra transnationella nätverk göras med analytisk försiktighet, då domarna i sig inte nödvändigtvis fastställer en sådan tillhörighet, utan snarare indikerar likheter i modusoperandi och strukturella kännetecken.

I enskilda fall med bolag finns det också kopplingar till ryska statliga intressen och med upplägg kring företag och fastigheter.

Sammantaget pekar materialet på att organiserad ekonomisk brottslighet av denna typ kan uppvisa en hög grad av systemintegration och anpassningsförmåga inom den svenska kontexten, samtidigt som den underliggande systematiken inte alltid framträder tydligt i enskilda rättsfall. Detta understryker behovet av att analysera brottmålsdomar i ett bredare sammanhang, där enskilda avgöranden förstås som delar av större kriminella nätverk och ekonomiska flöden.

## Översikt av brottsmål i svenska domstolar:

### Fall 1:

- Domstol: Solna tingsrätt
- Datum: 13 juni 2017
- Mål nr: B 7679–15
- Antal tilltalade: 16 personer

### Fall 2:

- Domstol: Luleå tingsrätt
- Datum: 2025-12-04
- Mål nr: B 1621–23
- Antal tilltalade: 3 personer

### Fall 3:

- Domstol: Södertörns tingsrätt
- Datum: 7 november 2025
- Mål nr: B 13688–25
- Typ av mål: Grovt organiserad näringspenningtvätt
- Omfattning: ca 384,9 miljoner kronor i transaktioner

## Så här ser kopplingen ut, punkt för punkt:

### 1. Ledarstyrd men flexibel cellstruktur

Domen beskriver VS som chef över verksamheten, med PM och AW i ledningsfunktioner under honom, medan JB skötte administrationen och SK den operativa kontorsfunktionen. Det är en tydlig kärna och specialiserade underfunktioner snarare än ett löst kompisgäng.

Det liknar välkända mönster i ryskspråkig organiserad brottslighet i Europa: inte alltid en stel pyramid, men ofta en stark kärna som styr modulära team, särskilt i penningtvätt, bedrägeri och ekonomisk brottslighet. Europol beskriver dagens mest hotfulla nätverk i EU som flexibla, gränsöverskridande och uppbyggda kring specialiserade roller snarare än traditionell maffiahierarki.

### 2. Målvakter, bolagsköp och frontbolag

Domstolen beskriver hur 22 bolag användes som penningtvättsbolag, att styrelserna bestod av målvakter, att transaktioner genomfördes med deras BankID och att bolagen saknade legitim verksamhet. Det är en nästan skolboksmässig användning av shell companies / straw directors /nominee fronts.

Det här är en central metod i ryskspråkiga penningtvättsnätverk. NCA<sup>9</sup> pekar uttryckligen på ryska/rysktalande penningtvättsnätverk som arbetar via företagsstrukturer, bulvaner och komplexa lager för att flytta brottsvinster. Europol lyfter också fram användningen av legala affärsstrukturer som brottsverktyg.

### 3. Falsk fakturering som “service”

Åklagarens och domstolens beskrivning är att kundbolag beställde falska fakturor, betalade in pengar till penningtvättsbolag och sedan fick tillbaka värdet genom kontanter, bilar eller andra utbetalningar minus en procentsats. Det är inte bara penningtvätt, utan en tjänstebaserad ”tvättplattform”.

Det här ligger mycket nära den typ av industriell penningtvätt som i Europa ofta kopplas till ryskspråkiga nätverk: de fungerar som kriminella finansiella serviceleverantörer åt andra brott=aktörer, inte bara åt sig själva. NCA och deras bedömning<sup>2025</sup> säger att ryskspråkiga penningtvättsnätverk i mycket stor skala tvättar åt annan allvarlig brottslighet.

### 4. Hög grad av professionalisering

I domen framgår att verksamheten hade särskilda Telegram-chattar för fakturor, bankkonton, saldon, betalningar och instruktioner. JB redovisade saldon; kontorstelefonen tog emot beställningar; andra alias skötte fakturering; olika personer förmedlade kunder.

Detta liknar arbetsdelad, nästan företagslik brottsdrift, vilket är typiskt för avancerade ryskspråkiga nätverk: ekonomi, logistik, kundkontakt, tekniskt stöd och riskhantering skiljs åt. Europol framhåller att den mest hotfulla organiserade brottsligheten i EU drivs mer som affärsverksamhet än som gatukriminalitet.

### 5. Telegram, alias och operativ säkerhet

Domstolen lägger stor vikt vid Telegram-chattar, frekventa byten av alias och att samma personer använder flera namn i olika grupper. VS kopplas till flera alias, och verksamheten drevs i separata chattar för olika funktioner.

Detta passar in i ryskspråkig organiserad brottslighet där digital OPSEC<sup>10</sup> är central: alias, chattsegmentering, rolluppdelning och begränsad synlighet mellan deltagare. Det är inte unikt ryskt, men det är mycket vanligt i ryskspråkiga bedrägeri- och penningtvättsmiljöer.

### 6. Kontanter, bilar och internationella flöden

Domstolen konstaterar omfattande kontanthantering, valutaväxling, bilköp finansierade från ”tvättbolag” och att majoriteten av bilarna förts utomlands eller avregistrerats. Det förekom också utbetalningar till utländska konton.

Den kombinationen med bankflöden, kontanter, bilar, internationella överföringar — är mycket typisk för ryskspråkiga nätverk eftersom den blandar snabb omsättning med tillgångar som kan flyttas eller omsättas över gränser. Europol och NCA beskriver just sådana hybridflöden som centrala i modern organiserad penningtvätt.

---

<sup>9</sup> National Crime Agency

<sup>10</sup> Operations Security (operativ säkerhet) är en metod för att identifiera, skydda och kontrollera information som kan användas av en motståndare för att förstå bland annat intentioner, kapacitet, sårbarheter eller operationer. Grunden i OPSEC är: att även små informationsfragment kan sammanfogas till en större underrättelsebild

## 7. Målvaktsmarknad som affärsresurs

Domen nämner uttryckligen handel med målvakter och köp av företag. I chattmaterialet finns uppgifter om att VS “köper företag och handlar med målvakter”, och att bolag väljs utifrån hur länge de kan användas innan de “bränns”.

Det här är ett mycket starkt typtecken. I ryskspråkig organiserad ekonomisk brottslighet behandlas bolag, direktörer, konton och identiteter ofta som förbrukningsbara resurser i ett kriminellt produktionssystem. NCA:s material om ryska “laundromat”-liknande upplägg och shell companies ligger nära detta.

## 8. Ryskspråkig miljö, men inte bevisad “klassisk *Bratva*<sup>11</sup>”

Utredningen byggde till stor del på meddelanden på ryska och översatta Telegram-chattar. Flera centrala personer hade bakgrund i Lettland, Belarus, Ukraina eller ryskspråkiga miljöer, och Soloviev hade - enligt chattmaterialet kopplingar mot St. Petersburg.

Det gör kopplingen till ryskspråkig brottsmiljö stark. Men det räcker fortfarande inte för att säga att detta är en klassisk “*vory v zakone*”- eller “*Bratva*”-struktur. Det som kan sägas med hög säkerhet är att målet passar post-sovjetisk organiserad ekonomisk brottslighet mycket bättre än exempelvis svensk gängkriminalitet eller en ren lokal ekobrottsgrupp.

### Avslutningsvis

Sammanfattande kan sägas att de påvisar användande av ett klassiskt diasporanätverk och med typiska tecken på relationsbaserad brottslighet. AV domen från Södertörn kan också påvisas en grad av industrialiserat penningtvättssystem både vad det gäller teknik och omfattning. Tillsammans påvisar det en utveckling från informell till professionell organiserad brottslighet

---

<sup>11</sup> I väst används ”Bratva” ibland nästan synonymt med “ryska maffian”. Men på ryska är betydelsen bredare och mer kulturell än strikt organisatorisk.

## REFERENSER OCH LITTERATUR

- *Applebaum, Anne. Gulag: A History.*
- *Fitzpatrick, Sheila. The Russian Revolution; samt arbeten om Stalinismen och vardagsliv under sovjetsystemet.*
- *Figes, Orlando. A People's Tragedy: The Russian Revolution.*
- *Galeotti, Mark. The Vory (och andra arbeten om rysk organiserad brottslighet och stat-brott-symbios).*
- *Getty, J. Arch. Arbeten om terrorn och sovjetisk statsstyrning.*
- *Gregory, Paul R. Arbeten om sovjetisk planekonomi och styrning.*
- *Gregory, Paul R. & Lazarev, Valery (red.). The Economics of Forced Labor: The Soviet Gulag.*
- *Khlevniuk, Oleg. Arkivbaserade arbeten om Stalinperioden och Gulag.*
- *Kotkin, Stephen. Magnetic Mountain; Stalin (biografiserien).*
- *Leggett, George. The Cheka (klassisk studie om den tidiga säkerhetsapparaten).*
- *Viola, Lynne. Arbeten om kollektivisering, deportationer och social ingenjörskonst.*
- *Varese, Federico. Arbeten om rysk maffia och kriminella nätverk i institutionella vakuum.*
- *Everything Was Forever, Until It Was No More*
- *Russia's Economy of Favours (för kontinuitet i nätverkslogik)*
- *Everything Was Forever, Until It Was No More (sen-sovjetisk kultur som bakgrund till 1990-talet)*
- *The Politics of Economic Reform in the Soviet Union (reformlogik och institutionell obalans; använd kritiskt)*
- *Russia's Economy of Favours*
- *Everyday Stalinism (för kontinuitet i vardagspraktiker och normer som bär in i efterkrigstiden)*
- *Everything Was Forever, Until It Was No More (för sen-sovjetisk normalitet, informell kultur och systemets "som-om"-logik)*
- *The Politics of Economic Reform in the Soviet Union (för reformlogik och incitamentsproblem kring perestrojka; använd selektivt och kritiskt)*
- *Soviet Criminal Justice Under Stalin (för rättssystemets instrumentella roll och dess arv i senare perioder)*

## Ytterligare referenslitteratur

- *Baker, P. & Glasser, S. (2005). Kremlin Rising: Vladimir Putin's Russia and the End of Revolution. New York: Scribner.*
- *Boycko, M., Shleifer, A. & Vishny, R. (1997). Privatizing Russia. Cambridge MA: MIT Press.*

- *Brown, A. (2001). Gorbachev, Yeltsin, & Putin: Political Leadership in Russia's Transition. Washington, DC: Carnegie Endowment for International Peace.*
- *Brown, A. (2007). Seven Years That Changed the World: Perestroika in Perspective*
- *Brzezinski, M. (2002). Casino Moscow: A Tale of Greed and Adventure on Capitalism's Wildest Frontier. New York: Free Press.*
- *Dixelius, M. & Konstantinov, A. (1994). Rysslands undre värld. Stockholm: Fischer & Co.*
- *Ericson, C. (2008). Ryssland nu: Trender i skuggan av Kreml. Stockholm:*
- *Felshtinsky, Y. (2008). The Age of Assassins: How Scary Are Russia's New Rulers? London: Gibson Square Books.*
- *Fortescue, S. (2006). Russia's Oil Barons and Metal Magnates: Oligarchs and the State in Transition. Basingstoke: Palgrave Macmillan.*
- *Freeland, C. (2000). Sale of the Century: Russia's Wild Ride from Communism to Capitalism. New York: Crown Business.*
- *Friedman, R. I. (2000). Red Mafia: How the Russian Mob Has Invaded America. New York: Little, Brown and Company.*
- *Furuhagen, B. (red.) (1995). Ryssland – Ett annat Europa. Stockholm: SNS Förlag.*
- *Goldfarb, A. & Litvinenko, M. (2007). En dissidents död: Mordet på Aleksandr Litvinenko och KGB:s återkomst. Stockholm: Prisma.*
- *Goldman, M. I. (1996). Lost Opportunity: What Has Made Economic Reform in Russia So Difficult. New York: W. W. Norton & Company.*
- *Goldman, M. I. (2003). The Piratization of Russia: Russian Reform Goes Awry. London: Routledge.*
- *Goldman, M. I. (2008). Petrostate: Putin, Power, and the New Russia. Oxford: Oxford University Press.*
- *Hoffman, D. E. (2002). Oligarchs: Wealth and Power in the New Russia. New York: PublicAffairs.*
- *Hollingsworth, M. & Lansley, S. (2009). Londongrad: From Russia with Cash London: HarperCollins.*
- *Jack, A. (2004). Inside Putin's Russia London: Granta Books.*
- *Jeffries, I. (2002). The New Russia: A Handbook of Economic and Political Developments. London: Routledge.*
- *Klebnikov, P. (2000). Godfather of the Kremlin The Decline of Russia in the Age of Gangster Capitalism. New York: Harcourt.*
- *Meier, A. (2003). Black Earth: A Journey Through Russia After the Fall. New York: W. W. Norton & Company.*
- *Reddaway, P. & Glinski, D. (2001). The Tragedy of Russia's Reforms: Market Bolshevism Against Democracy Washington, DC: United States Institut of Peace.*
- *Satter, D. (2003). Darkness at Dawn: The Rise of the Russian Criminal State. New Haven: Yale University Press.*

- Shevtsova, L. (1999). *Yeltsin's Russia= Myths and Reality*. Washington, : Carnegie Endowment for International Peace.
- Shevtsova, L. (2007). *Russia Lost in Transition: The Yeltsin and Putin Legacies* Washington, DC: Carnegie Endowment for International Peace.
- Stürmer, M. (2008). *Putin and the Rise of Russia*. London: Weidenfeld & Nicolson.
- Varese, F. (2001). *The Russian Mafia: Private Protection in a New Market Economy*= Oxford: Oxford University Press.
- Åslund, A. (2007). *Russia's Capitalist Revolution: Why Market Reform Succeeded and Democracy Failed*. Washington, DC: Peterson Institute for International Economics.

### Sammanställning av böcker som behandlar utveckling av KGB och rysk underrättelsetjänst

- Christopher Andrew & Oleg Gordijevskij (1988), *KGB inifrån – Del 1: Från Tjekan till Potsdam* ISBN: 91-0047304-0, *KGB inifrån – Del 2: Spionskandalerna tid* ISBN: 91-0047305-9
- Christopher Andrew & Vasili Mitrokhin (1999) *The Sword and the Shield – The Mitrokhin Archive and the Secret History of the KGB* ISBN: 978-465003105
- Catherine Belton (2020) *Putins People – How the KGB Took Back Russia and Then Took On the West* ISBN: 978-007578818
- Vadim J. Birstein (2011) *SMERSH Stalin's Secret Weapon* ISBN: 978-849541084
- Gordon Corera (2020) *Russians Among Us – Sleeper Cells, Ghost Stories and the Hunt for Putin's Spies* ISBN: 978-062889423
- Brian D. Dailey & Patrick J. Parker (1987) *Soviet Strategic Deception* ISBN: 978-669132083
- John Earl Haynes, Harvey Klehr & Alexander Vassiliev *Spies (2009): The Rise and Fall of the KGB in America* ISBN: 978-300123906
- Thomas Rid (2020) *Active Measures – The Secret History of Disinformation and Political Warfare* ISBN: 978-0374287269

### Referenslitteratur specifikt underrättelsetjänst

- |                  |                                   |
|------------------|-----------------------------------|
| ▪ Adams (1995)   | <i>Sell Out (Aldrich Ames)</i>    |
| ▪ Agrell (2000)  | <i>Fred och fruktan</i>           |
| ▪ Agrell (2002)  | <i>Konsten att gissa rätt</i>     |
| ▪ Agrell (2004)  | <i>Tre spioner i kallt krig</i>   |
| ▪ Agrell (2007)  | <i>Moskvas spioner</i>            |
| ▪ Agrell (2010)  | <i>Stockholm som spioncentral</i> |
| ▪ Agrell (2013)  | <i>Maskerad front</i>             |
| ▪ Agrell (2020)  | <i>Sprickor i järnridån</i>       |
| ▪ Agrell (2021)  | <i>U 137 och ubåtskrisen</i>      |
| ▪ Almgren (2011) | <i>Inte bara Stasi</i>            |
| ▪ Alvarez (2002) | <i>Spies in the Vatican</i>       |

- *Andrew (2018)* *The Secret World*
- *Andrew (2009)* *Defence of the Realm*
- *Andrew (2005)* *World Was Going Our Way*
- *Bamford (2002)* *Spies*
- *Batvinis (2007)* *Origins of FBI Counterintelligence*
- *Clark (2013)* *Intelligence Analysis*
- *Coll (2018)* *Directorate S*
- *Crumpton (2013)* *The Art of Intelligence*
- *Dorril (2000)* *MI6*
- *Dulles (1963)* *Craft of Intelligence*
- *Earley (1997)* *Enemy Within*
- *Fredholm (2022)* *Hemligstämplat*
- *Fry (2023)* *Women in Intelligence*
- *Gehlen (1972)* *The Service*
- *George & Bruce (2014)* *Analyzing Intelligence*
- *Gieseke (2011)* *Stasi*
- *Hastings (2015)* *The Secret War*
- *Heuer (1999)* *Psychology of Intelligence Analysis*
- *Heuer & Pherson (2011)* *Structured Analytic Techniques*
- *Herman (1996)* *Intelligence Power in Peace and War*
- *Hoffman (2015)* *Billion Dollar Spy*
- *Jervis (2011)* *Why Intelligence Fails*
- *Jeffreys-Jones (2013)* *In Spies We Trust*
- *Koehler (1999)* *Stasi: The Untold Story*
- *Lowenthal (2016)* *Intelligence: From Secrets to Policy*
- *Macintyre (2018)* *Spy and the Traitor*
- *Macintyre (2014)* *Spy Among Friends*
- *Macintyre (2010)* *Operation Mincemeat*
- *Magnusson (red.) (2023)* *Guide till spionernas Sverige*
- *Martin (1980)* *Wilderness of Mirrors*
- *Masterman (1972)* *Double-Cross System*
- *McDowell (2008)* *Strategic Intelligence*
- *Mundy (2023)* *The Sisterhood*
- *Olson (2019)* *To Catch a Spy*
- *Olson (2021)* *Art of Counterintelligence*
- *Prunckun (2012)* *Counterintelligence Theory and Practice*
- *Shulsky (2011)* *Secret World of Counterintelligence*
- *Singh (1999)* *The Code Book*
- *Weiner (2008)* *Legacy of Ashes*
- *Whipple (2018)* *The Spymasters*
- *Wise (2002)* *Spy (Hanssen)*
- *Wolf (1997)* *Man Without a Face*

## Om SäkerhetsBranschen

SäkerhetsBranschen är en medlems- och branschorganisation för säkerhetsföretag. Vi samlar aktörer inom säkerhet och arbetar för att synliggöra branschen, driva viktiga frågor och bidra till ett tryggare och säkrare Sverige.

Tillsammans med våra medlemmar och deras kunder ser vi hur hotbilder förändras i praktiken, och hur ett mer komplext geopolitiskt läge ökar behovet av kunskap, medvetenhet och gemensam förståelse.

Genom att sprida denna rapport vill vi bidra till en mer nyanserad och informerad diskussion om de strukturer och hot som påverkar både Sverige och Europa. Vi är övertygade om att ökad kunskap på sikt stärker samhällets motståndskraft och bidrar till att reducera risker.

Vår förhoppning är att rapporten ska vara ett stöd för såväl beslutsfattare som praktiker. I en tid där hoten blir mer komplexa behöver också vår förståelse bli det – och där vill SäkerhetsBranschen vara en aktiv del av lösningen.

