atlant

Info no.3 – Maj 2024

RUSLANDS HYBRIDKRIG IMOD VESTEN. HVORNÅR ER NOK NOK?

LARS BANGERT STRUWE

HYBRIDKRIG EN TRUSSEL IMOD DANMARK OG NATO

Danmark og vores allierede i NATO og EU er udsat for en hybridkrig. Hybridkrig udvisker de klare skel imellem fred og krig og skaber en gråzone, hvor der er usikkerhed over, hvad der sker. Usikkerheden bruges af ens modstandere til at underminerer tilliden til staten, myndigheder, politikere og demokratiet.

I hybridkrig påtager angriberen sig typisk ikke ansvaret for angreb, og angrebene holder sig på et niveau under konventionel krig.

NATO ser hybride trusler som en kombination af militære og ikke-militære såvel som skjulte og åbenlyse midler, herunder desinformation, cyberangreb, økonomisk pres, udsendelse af irregulære væbnede grupper og brug af regulære styrker.

Målet er at destabilisere og underminere samfund. Vigtige elementer er derfor at distrahere, afskrække, forvrænge og miskreditere. Der er foretaget tusinder af cyberangreb og mere end 17.000 sager med disinformation. Så det er massive angreb vi står over for som samfund.

Konventionel krig kan være målet for en hybridkrig, hvor man har brugt de hybride værktøjer til at svække den stat man angriber. Derfor må man ikke se hybridkrig som en udelukkelse af konventionel krig.

NATO har gjort det klart, at hybridkrig kan udløse artikel 5 og derved et selvforsvar fra NATO's side. Men hvornår er nok nok? Hvornår er vi i en artikel 5 situation? Hybridkrig gør, at det er svært at erkende, hvornår skal vi sætte et modsvar ind, som stopper angrebene, og hvordan kan vi gøre det?

I NATO må man også overveje, om man selv skal tage hybridkrig til sig, og anvende det til at underminerer vores modstandere. Vi er i en førkrigs-periode, som den polske premierminister Donald Tusk har beskrevet det.

Der sker konfrontationer i cyber, der sker manipulation, der er konsekvent angreb på Danmark og vores allierede. Derfor må vi overveje, hvordan vi selv kan tage dele af hybridkrigens elementer til os.

Dette Atlant Info samler både nogle af de centrale definitioner og søger at skabe et overblik over nogle af de operationer, som har ramt NATO- og EU-stater over de seneste mange år.

I dette Atlant Info beskriver vi episoder, hvor der er sket spionage, sabotage, påvirkningsoperationer, økonomisk pres eller påvirkning, spoofing, cyberkrig og likvideringer. Dette er alle elementer i hybridkrig, som man må overveje i hvilken grad vi vil tage til os, for at kunne vinde over vores modstander.

INDHOLDSFORTEGNELSE

NATO'S UDMELDING OM HYBRIDKRIG

Der er lige nu ikke nogen direkte klassisk krig imellem Rusland og NATO. Imidlertid er Rusland kommet med en række udtalelser, der klart indikerer, at det på den ene eller anden måde ser sig i en konflikt med Vesten. 4. april 2024 meddelte Kremls talsmand Dmitry Peskov "*In fact, relations have now slipped to the level of direct confrontation*."[1] Putin har afvist, at Rusland har planer om et angreb på NATO.[2] Imidlertid opretholder han konstant et konfrontatorisk sprog og truer bl.a. med brug af taktiske våben.[3] Han har således meddelt, at Rusland og NATO kun er et skridt fra Tredje Verdenskrig.[4]

Tilsyneladende udkæmpes der er mindre synlig krig under overfladen – en hybridkrig. NATO meddelte den 2. maj 2024, at man støttede allierede i Tjekkiet, Estland, Tyskland, Letland, Litauen, Polen og Storbritannien, der havde oplevet fjendtlige hybride aktiviteter.[5] Der er således en række aktiviteter i Europa, der kobles til Rusland og Ruslands krig i Ukraine.

Statsminister Mette Frederiksen har advaret imod yderligere russiske hybridangreb. Hun meldte meget klart ud:

> *"- Jeg tror, at nogle europæere stadig tænker, at krigen kun foregår i Ukraine, men lige nu ser vi mere og mere aggressivitet fra Rusland.*
>
> *- Vi vil formentlig se hybridangreb på forskellige områder. Det kan være kritisk infrastruktur, tilføjer hun. "*[6]

På NATO's topmøde i Bruxelles i 2018 blev det i punkt 21 i slutdeklarationen gjort helt klart, at et hybridangreb kan udløse NATO's artikel 5 om gensidigt forsvar.[7] Det betyder, at en stat, der bruger hybridangreb over for en NATO-stat risikerer at udløse et selvforsvar fra det samlede NATO imod sig. Dette er direkte rettet imod Ruslands ageren imod Ukraine og Vesten.

Spørgsmålet er derfor, hvad er hybridangreb, hvad har fundet sted, og hvad gør vi i fremtiden?

HVAD ER HYBRIDKRIG?

Hybridkrig er ikke nyt, der findes utallige historiske eksempler, der rækker tilbage til antikken. Danmark brugte hybride metoder i sin udenrigspolitik i 1700-tallet, hvor vi bl.a. med en blanding af gaver, pensioner, bestikkelser og militær mobilisering søgte at sikre den svenske tronfølgertitel til den danske konge ellers hans søn.[8]

Den amerikanske National Defence Strategy i 2005 udvidede dets syn på trusler. [9] Det blev endda antydet, at man havde brugt for mange kræfter på konventionelle styrker.

På baggrund af udviklingen fra 9/11 og frem diskuterede man i såvel militære som sikkerhedspolitiske kredse, hvad det var for en ny form for krig man stod over for.

Hizbollah angreb Israel 2006, og dette udløste en række analyser af, hvorfor Israel havde så store problemer med at nedkæmpe en modstander som Hizbollah.[10]

I 2007 definerede den amerikanske forsker og tidligere officer Frank Hoffman begrebet for første gang. Det skete i artiklen "Conflict in the 21st Century. The Rise of Hybrid Wars".[11] Hoffman tog udgangspunkt i Hizbollah. Han definerede hybridkrig på følgende vis:

> "*…different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of nonstate actors.*" [12]

NATO definerer hybridkrig på følgende vis:

> *"Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies.*"[13]

Hybridkrig fik særlig opmærksomhed efter Rusland invasion af Ukraine. Her var den russiske brug af specialoperationsstyrker uden nationale kendetegn en del af den hurtige sejr. Disse "små grønne mænd" tændte virkelige for diskussionen om hybridkrig.

Den russiske generalstabschef Valery Vasilyevich Gerasimov havde i et militært tidsskrift skrevet en artikel, der beskrev moderne krig som han så det efter Det Arabiske Forår, og de farvede revolutioner. Artiklen udkom i 2013, og dannede grundlag for det som oftest kaldes Gerasimov doktrinen – på trods af, at det ikke er det.[14]

Gerasimov startede artiklen med at iagttage, at en velfungerende stat i løbet af meget kort tid fra dage til måneder kan være involveret i en voldsom væbnet konflikt, blive et offer for udenlandsk intervention og synke ned i et net af kaos, humanitær katastrofe og borgerkrig.[15]

I artiklen beskriver Gerasimov, hvordan moderne kriser og krige bygger på en meget bred brug af politiske, økonomiske, påvirkninger, humanitære og andre ikke-militære foranstaltninger. Dette kan spille på befolkningen og eventuelt mindretal eller potentielle protester. Til dette kan man anvende militære midler af skjult karakter (klandestine operationer), herunder udførelse af informationsoperationer og specialoperationer. Herved talte Gerasimov ind i den eksisterende vestlige debat om hybridkrig.

Hybridkrig udvisker således de klassiske skel imellem krig og fred. Der opstår en gråzone, hvor en stat eller en anden aktør bruger alle sine midler til at undergrave et samfund og omstyrte eller overtage det. Særligt bruges efterretningstjenester og

specialoperationsstyrker til at gennemføre de skarpeste dele af hybridkrigen. Hybridkrigen søger man hele tiden at holde under niveauet for en reel konventionel krig. Derved kan man destabilisere modstanderen, men undgå en krig eller håbe på, at modstanderen af frygt for eskalation ikke svarer igen med stærke konventionelle midler.

Konventionel krig kan være målet for en hybridkrig, hvor man har brugt de hybride værktøjer til at svække den stat man angriber. Derfor må man ikke se hybridkrig som en udelukkelse af konventionel krig.

SPIONAGE OG SABOTAGE

Polen afslørede i 2023 et spionnetværk, der overvågede polske jernbanelinjer og planlagde sabotage imod våbenleverancer igennem Polen til Ukraine. Et af de overvågede mål var Rzeszow-Jasionka lufthavnen, der er central i forsyningerne til Ukraine. Denne lufthavn har nu sit eget Patriot-batteri til beskyttelse.[16] Der var ni anholdte, og de sigtes bl.a. for at have forsøgt at placere GPS-sporing på våbenleverancerne. De skulle ave arbejdet for den russiske efterretningstjeneste og modtaget midler derfra.

Medier kobler anholdelserne i Polen til nye anholdelser i april 2024 i Bayern. Her er to personer med tysk-russisk baggrund blevet anholdt. De er sigtet for at rekognoscere amerikanske baser og andre steder.[17] Den første af de anholdte er sigtet for at planlægge en eksplosion, brandstiftelse og opretholdelse af kontakt med russisk efterretningstjeneste. Derved falder han ind under tyske spionagelovgivning. Han har en fortid som kæmper på russisk side i Ukraine fra 2014 til 2018. Hans makker er sigtet for at have hjulpet ham med at identificere mål. Målene skulle have forbindelse til den store tyske våbenhjælp til Ukraine.

Fem mænd er i Storbritannien anklaget for lave brandstiftelse i London for den russiske Wagner-gruppe. De satte ild til to steder i Leyton i Storbritannien den 20. marts 2024. Disse var virksomheder med en forbindelse til Ukraine.[18] De anklagede anklages for at have modtaget penge for denne operation, der håndteres som en terroroperation, der falder ind under den nye spionagelov i Storbritannien. Navne på de anklagede antyder, at de ikke er russere.

Jernbanesabotage forbinder vi med Anden Verdenskrig, men tilsyneladende er bl.a. svenske jernbaner blevet udsat for sabotage.[19] Det drejer sig om en række angreb på bl.a. signalskabe. Derved forsinkes trafikken.[20] Det er den vigtige svensk-norske malmtransport, der er ramt. SÄPO er involveret i opklaringen. Imidlertid er der endnu ikke nogen spor, der knyttes til Rusland. Der er også tale om reelle afsporinger, som man undersøger om er sabotage.[21] Det bekymrer de svenske, norske, britiske og tyske efterretningstjenester.

I Norge har chefen for efterretningstjenesten PST i et sjældent interview fortalt om markant øget russisk efterretningsvirksomhed siden 2022. dette er særligt sket i

områder med flådebaser og olieindustri. Man frygter i Norge, at Rusland planlægger sabotage af kritisk infrastruktur.[22]

PÅVIRKNINGSOPERATIONER – OG SÆRLIGT VALG

Rusland har forsøgt at påvirke valg i Vesten. Det gjorde at PET og FE i 2022 kom med en fælles vurdering af truslen fra russisk påvirkning af folketingsvalg.[23] I den fælles trusselsvurdering anså man det for en klart, at Rusland har kapaciteten til at lave en påvirkningskampagne, men at pga. krigen i Ukraine ikke havde ressourcerne til en stor kampagne over for Danmark.

FBI har efterlyst 12 russiske militære efterretningsofficerer for at søge at påvirke det amerikanske præsidentvalg i 2016.[24] Præsident Putin skulle direkte have beordret Project Lakhta igangsat. Denne operation skulle sikre Trump valgsejren over Hillary Clinton. Samtidigt skulle operationen underminerer det amerikanske demokrati. Man benyttede sig bl.a. af en række falske profiler, der både var republikanere og demokrater. Helt centralt var ønsket om at radikaliserer debatten i USA.[25]

Troldefarme blev en del af den russiske kampagne. Det russiske firma Internet Research Agency i Skt. Petersborg fik placeret mere end 5.000 falske politiske annoncer på Facebook.[26] Internet Research Agency skulle i henhold til amerikanske efterretningsanalyser først støtte Ruslands operationer i Ukraine, men i 2015 fik man også til opgave at støtte Donald Trumps kampagne.[27]

Af den såkaldte Mueller-rapport, fremgår det, at Internet Research Agency iværksatte en kampagne på sociale medier. Denne skulle favorisere Donald J. Trump og miskreditere Hillary Clinton.[28]

En del af kampagnen blev hacking af det demokratiske parties computere. Dette stod den russiske militære efterretningstjeneste GRU bag. Oplysningerne blev så lækket til WikiLeaks og via to falske profiler kaldet DCLeaks"og Guccifer 2.0.[29] Dette var med til at skade og så tvivl om Hillary Clinton.

Nogenlunde samtidigt med det amerikanske præsidentvalg fandt der også Brexit-valgkampen sted. Denne synes at have været udsat for russiske påvirkningsforsøg. Den britiske parlamentsrapport om emnet er noget vag i sine formuleringer. Man tør ikke sige, om afstemningsresultatet var påvirket af Rusland, men konstaterede, at Rusland havde sgt at påvirke den skotske afstemning i 2014.[30]

Frankrig følger meget med i de russiske påvirkningsoperationer. VIGINUM er den tekniske og operationelle tjeneste i den fransk stat, der er ansvarlig for overvågning og beskyttelse mod udenlandsk digital interferens. Her har man identificeret næsten 200 websteder, der massivt videresender vildledende indhold, designet til at legitimere invasionen af Ukraine og påvirke støtten til Kiev i Frankrig.[31]

Ved præsidentvalget i 2017 var Frankrig forberedt på, at Rusland ville forsøge at påvirke valget. Under valgkampen blev der både lavet en disinformationskampagne imod Emanuel Macron og hans valgkampagne, og i dagene op til valget skete der et stort læk af oplysninger. Det lykkedes i Frankrig at undgå, at valget blev påvirket, og den russiske kampagne fremstår som fejlslagen.[32]

Den franske succes byggede bl.a. på, at man lærte af andre, viste beslutsomhed, lagde pres på digitale platforme og slog tilbage på sociale medier.[33]

Det danske udenrigsministerium har haft en gruppe, der fulgte valg og demokrati på baggrund af de erfaringer man gjorde sig fra 2014 og fremefter. De europæiske og amerikanske erfaringer gør, at man frygter for påvirkningsoperationer rettet imod EU-parlamentsvalget i juni 2024.

Myndigheder i hele Europa har med bekymring set på, hvordan nyhedsmediet Voice of Europe er blevet brugt til russisk propaganda. Det sker på baggrund af, at tjekkisk efterretningsvirksomhed af afdækket et russisk påvirkningsnetværk. Tilsyneladende har man derfra givet russiske midler videre til europæiske politikere.[34]

I Belgien har premierminister, Alexander De Croo, meddelt, at medlemmer af EU-Parlamentet er blevet betalt af Rusland for at promovere russisk propaganda.[35] Navnene er ikke blevet offentliggjort, men der peges på højre side af parlamentet.

Danmark har været ramt af misinformation, hvor en russisk iscenesat operation hævdede, at der var dyrebordeller i Danmark.[36] Kampagnen ramte med en vis undren Danmark, men den var mest af alt rettet imod det russiske hjemmepublikum, der kunne se det dekadente Vest, der ikke hylder ”normale” værdier.

EU har sat ind over for russisk disinformation. EUvsDisinfo er en EU enhed, der har skabt East Stratcom Task Force, der rummer kommunikationseksperter, journalister, forskere og Ruslands specialister. De har frem til maj 2024 indsamlet og afsløret 17.077 sager med russisk disinformation.[37]

ØKONOMISK PRES ELLER PÅVIRKNING

Europæisk og amerikansk økonomi er nøje koblet til en række undersøiske kabler og rør. NATO advarer imod, at denne undersøiske kritiske infrastruktur er mål for russiske operationer. Det drejer sig f.eks. om kabler fra vindmøller, kommunikationskabler og gasledninger.[38]

Et sådant angreb har tilsyneladende allerede fundet sted. Balticconnector forbinder Finland med Estland i form af en undersøisk gasledning. Den blev ramt af skader i oktober 2023. Fra finsk side koblede man ødelæggelser på Balticconnector til Rusland.[39] Senere har peget på at ødelæggelserne blev forvoldt af et kinesisk skib, der med sit anker ødelagde dele af Balticconnector og kommunikationskabler.[40]

Igennem mange år har Rusland brugt energi, som et våben over for Europa. Man har lukket op og ned for tilførslen af gas, og derved søgt at presse russisk politik igennem. Fra EU's side har man siden 2022 haft øje for dette, og lagt planer for en reduktion af gasafhængigheden fra Rusland.[41] Europas gasafhængighed fra Rusland er faldet fra 45% i 2021 til 15 % i 2023.[42] Et meget markant fald, der har gjort Europa mindre påvirkeligt økonomisk fra Rusland.

SPOOFING OG JAMMING TIL SØS OG I LUFTEN

Igennem længere tid er det blevet rapporteret, at gps-systemet jammes. Det betyder, at man ikke kan få et signal. Der er også rapporteret en del tilfælde, hvor GPS-signaler er blevet spoofet. Spoofing er et begreb, der bruges inden for cyberdomænet, men som også bruges om forstyrrelser a GPS-signaler. I cyber bruges det om en situation, hvor en person eller et program med succes udgiver sig som en anden ved at forfalske data for at opnå en illegitim fordel. I luften eller til havs betyder det, at man får et signal, der indikerer, at man er et andet sted, end der hvor man rent faktisk er.

Spoofing kan bruges til at skabe uklarhed, og reel fare for fly eller skibe. Det kan måske også bruges til at placere fly eller skibe i områder, hvor de ikke må værre. I værste fald kan det bruges til at udløse en krise eller krig, fordi man derved kan manipulere skibe eller fly forkerte steder hen.

I luftfarten har man oplevet, at GPS-signaler i luftrummet over særligt Østersøen, i Polen og op til Finland.er blevet forstyrret. Det har ramt den civile luftfart, bl.a. hen over julen 2023.[43] Det er fortsat frem til i dag, og den civile luftfart forventer, at en række systemer ikke virker.[44] I Norge rapporterer man om næsten daglige forstyrrelser af GPS-signaler. De norske tal viser klart stigningen. I 2019 var der seks jamminger, men det steg til 122 i 2022 og 294 i 2023.[45]

Spoofing bruges militært til at sikre, at fjendtlige missiler eller droner har forkerte GPS-oplysninger, så de ikke rammer deres mål.[46]

Den britiske forsvarsminister oplevede, at Rusland jammede hans militære fly. Det skete på en flyrejse tilbage fra Polen. Tæt på den russiske enklave Kaliningrad oplevede man i en halv time at være udsat for russisk jamming. Det gjorde dele af kommunikationssystemerne ombord ubrugelige. Det truede dog ikke flyets sikkerhed.[47]

Til søs oplever man, at russiske skibe slukker deres AIS – automatic identification system.[48] Det gør, at de prøver at sløre deres position og sejlads. Noget så fredeligt, som Molslinjen oplevede, at et russisk krigsskib ikke svarede på opkald og havde slukket sit AIS. Et russisk spionskib er også rapporteret i danske farvande, hvor det sejlede i mærkelige zizag-mønstre.[49]

Slukkede AIS-signaler har i øvrigt mulligjort russisk omgåelse af sanktioner. Man har bl.a. transporteret olie på skibe, der slukkede deres AIS, så man ikke kunne sporer leverancer.[50] Derved blev dette til en del af Ruslands økonomiske krig eller økonomiske overlevelse.

CYBERANGREB

Rusland står bag en lang række cyberangreb. Center for Cybersikkerhed anser truslen imod Danmark på cyberområdet som meget høj, og peger direkte imod Rusland, som en af de vigtigste trusler.[51]

Siden angrebet på Ukraine har den europæiske energisektor været udsat for tusinder af cyberangreb.[52] Russiske grupper har søgt ved hjælp af phishing, at udføre spionage imod vigtige personer i Europa, fra NGO'er over politikere til militært personel meddeler Googles Threat Analysis Group.[53] Dette skulle nu være udvidet til også at installerer mallware, så man kan skade de ramtes computere.

Seneste offentliggjorte cyberangreb var rettet imod Tyskland og Tjekkiet. De tyske myndigheder offentliggjorde, at de tilskrev det den russike militære efterretningstjeneste GRU.[54] Samme dag den 3. maj 2024 gik Josep Borrell, EU's højtstående repræsentant for udenrigsanliggender ud og advarede Rusland om, at:

> *"The EU will not tolerate such malicious behaviour, particularly activities that aim to degrade our critical infrastructure, weaken societal cohesion and influence democratic processes, mindful of this year's elections in the EU and in more than 60 countries around the world. The EU and its Member States will continue to cooperate with our international partners to promote an open, free, stable and secure cyberspace."*[55]

I Tyskland har efterforskere kunnet koble tyske leverancer af våben til Ukraine med russiske cyberangreb. Da Tyskland diskutere leverancer af Leopard2 kampvogne til Ukraine, så angreb cybergruppen APT28 tyske hjemmesider og informationssystemer. APT28 er sponseret af den russiske militære efterretningstjeneste.[56]

LIKVIDERINGSPLANER

Præsident Zelensky er mål for en række attentatforsøg. I Ukraine har man senest i maj 2024 anholdt personer med tilknytning til russisk efterretningstjeneste og to ukrainske oberster, der skulle have lækket fortrolige oplysninger til russerne om beskyttelsen af Zelensky.[57]

Likvideringsplaner har også fundet sted uden for Ukraine. I Polen har man anholdt en person i april 2024 for at have tilbudt sin tjeneste til russisk efterretningsvirksomhed. Han skulle have observeret Rzeszow-Jasionka lufthavnen, der har været brugt af præsident Zelensky med henblik på et attentat mod ham.[58] Ved brug af sociale medier

har russiske agenter fundet estere, der var villige til at lave et angreb på den estiske minister Lauri Läänemets og en redaktør.[59] Det er således ikke kun den ukrainske præsident, der er målet for russiske likvideringsplaner.

To ukrainske soldater er blevet dræbt i Tyskland af en russisk mand. De tyske myndigheder er forsigtige med at forbinde det med krigen i Ukraine.[60]

HVORNÅR ER NOK NOK, OG HVAD GØR VI?

Danmark og vores allierede i NATO og EU er udsat for en hybridkrig særligt fra Rusland. Vi er blevet udsat for spionage, sabotage, påvirkningsoperationer, økonomisk pres eller påvirkning, spoofing, cyberkrig og likvideringer på dansk eller allieret territorium.

Hybridkrig udvisker de klare skel imellem fred og krig og skaber en gråzone, hvor der er usikkerhed over hvad der sker. Usikkerheden bruges af Rusland til at underminerer tilliden til staten, myndigheder, politikere og demokratiet.

Konventionel krig kan være målet for en hybridkrig, hvor man har brugt de hybride værktøjer til at svække den stat man angriber. Derfor må man ikke se hybridkrig som en udelukkelse af konventionel krig.

NATO har gjort det klart, at hybridkrig kan udløse artikel 5 og derved et selvforsvar fra NATO's side. Men hvornår er nok nok? Hvornår er vi i en artikel 5 situation? Hybridkrig gør, at det er svært at erkende, hvornår skal vi sætte et modsvar ind, som stopper angrebene, og hvordan kan vi gøre det?

I NATO må man også overveje, om man selv skal tage hybridkrig til sig, og anvende det til at underminerer vores modstandere. Vi er i en førkrigs-periode, som den polske premierminister Donald Tusk har beskrevet det.[61] Hvordan undgår vi, at det bliver til en krig og hvordan afskrækker og stopper vi vores modstandere?

Vi må overveje, hvordan vi selv kan tage dele af hybridkrigens elementer til os. Vi må erkende, at vi står over for en markant trussel, som vi må ikke blot forsvare os imod, men også stoppe.

Lars Bangert Struwe

Generalsekretær, ph.d

NOTER

[1] https://www.reuters.com/world/russia-nato-relations-level-direct-confrontation-kremlin-says-2024-04-04/
[2] https://www.aa.com.tr/en/asia-pacific/putin-calls-statements-about-moscows-alleged-plans-for-war-with-europe-nato-nonsense/3176935#
[3] https://www.reuters.com/world/europe/russia-practice-tactical-nuclear-weapon-scenario-deter-west-defence-ministry-2024-05-06/
[4] https://www.reuters.com/world/europe/putin-warns-west-russia-nato-conflict-is-just-one-step-ww3-2024-03-17/
[5] https://www.nato.int/cps/en/natohq/official_texts_225230.htm
[6] https://ekstrabladet.dk/nyheder/politik/statsministeren-venter-flere-russiske-hybridangreb/10223088
[7] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf
[8] Struwe, Lars Bangert: *"Jeg er sikker på, at Danmark har onde hensigter over for Sverige. Kriserne i Norden i 1740'erne".* (U.pub. ph.d. , SDU, 2009)
[9] https://apps.dtic.mil/sti/pdfs/ADA431214.pdf
[10] https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/
[11] https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
[12] https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf s. 8.
[13] https://www.nato.int/cps/en/natohq/topics_156338.htm
[14] https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
[15] https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
[16] https://www.bbc.com/news/world-europe-64975200
[17] https://www.bbc.com/news/world-europe-68843541
[18] https://www.independent.co.uk/news/uk/crime/dylan-earl-arson-russian-spy-allegations-b2535337.html
[19] https://www.nwt.se/2023/08/29/polisen-misstanker-jarnvagssabotage-i-dalsland-3fc76/
[20] https://www.aftonbladet.se/nyheter/a/gEGoVL/uppgifter-jarnvag-i-dalsland-saboterade-for-att-forsvara-tagtrafiken
[21] https://www.nrk.no/tromsogfinnmark/etterforsker-togavsporinger-som-mulige-sabotasjeaksjoner-1.16871705
[22] https://www.nrk.no/vestland/pst-har-avdekket-russisk-etterretningsvirksomhet-i-vest-1.16868180sabo
[23] https://pet.dk/pet/nyhedsliste/truslen-fra-russisk-paavirkning-af-det-kommende-folketingsvalg/2022/10/07
[24] https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
[25] https://www.gmfus.org/news/target-usa-key-takeaways-kremlins-project-lakhta
[26] https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/
[27] https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf
[28] https://www.justice.gov/archives/sco/file/1373816/dl

[29] https://theintercept.com/2019/04/18/annotating-special-counsel-robert-muellers-redacted-report/
[30] https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf
[31] https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/ce-que-l-on-sait-de-portal-kombat-le-reseau-de-sites-de-desinformation-pro-russes-denonce-par-la-france_6362980.html
[32] https://www.csis.org/analysis/successfully-countering-russian-electoral-interference
[33] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf
[34] https://www.bbc.com/news/world-europe-68685604
[35] https://nyheder.tv2.dk/udland/2024-03-29-politikere-kraever-undersoegelse-af-russisk-indflydelse-i-eu-parlamentet
[36] https://www.dr.dk/nyheder/indland/russiske-medier-spreder-falske-nyheder-om-dyresex-i-danmark
[37] https://euvsdisinfo.eu
[38] https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns
[39] https://www.theguardian.com/world/2023/oct/10/undersea-pipeline-damage-appears-to-be-deliberate-says-finland
[40] https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/
[41] https://ecfr.eu/article/conscious-uncoupling-europeans-russian-gas-challenge-in-2023/
[42] https://energy.ec.europa.eu/news/focus-eu-energy-security-and-gas-supplies-2024-02-15_en
[43] https://ing.dk/artikel/gps-konflikt-i-oestersoeen-flere-fly-ramt-af-avanceret-spoofing-over-baltikum
[44] https://www.flightradar24.com/blog/videos/a350-longhaul-behind-the-scenes-in-the-cockpit-with-sas/
[45] https://www.tu.no/artikler/markant-okning-i-russisk-jamming-mot-norge/544076
[46] https://www.newscientist.com/article/2415318-ukraine-will-spoof-gps-across-the-country-to-stop-russian-drones/
[47] https://www.independent.co.uk/news/uk/politics/russia-ukraine-grant-shapps-war-b2512675.html
[48] https://www.defenseone.com/threats/2024/04/russias-gps-meddling-baltic-sea-demands-nato-action-swedens-naval-chief-says/395607/
[49] https://danwatch.dk/saadan-sejlede-bevaebnede-spioner-paa-hemmelig-mission-i-danmark/
[50] https://www.cnbc.com/2023/09/26/russian-dark-ships-vessels-fake-their-locations-to-move-oil-around-the-world.html
[51] https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-denmark-2023.pdf
[52] https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/
[53] https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/
[54] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/05/aktuelle-Cyberangriffe.html
[55] https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/

[56] https://www.theguardian.com/world/article/2024/may/03/germany-says-russians-behind-intolerable-cyber-attack-last-year
[57] https://afp.omni.se/kyiv-says-two-ukraine-officials-held-over-plot-to-kill-zelensky/a/VzRWA1
[58] https://www.bbc.com/news/world-europe-68848317
[59] https://www.politico.eu/article/estonia-thwarts-russian-hybrid-operation-arrests-10/
[60] https://www.dw.com/en/germany-2-ukrainians-killed-over-weekend-were-soldiers/a-68944661
[61] https://www.dw.com/en/europe-has-entered-pre-war-era-polands-tusk-says/a-68702657