Den ryska federationens taktiker för valpåverkan

Martin Kragh

November 2021

Rapport inom ramarna för projekt ”Sårbarheter för informationspåverkan - En forskningsöversikt inför det svenska valet 2022”. Rapporten ingår i skriftserien ”Det öppna samhället” vid Uppsala universitet (Skrift No 1, Redaktörer Sten Widmalm & Thomas Persson).

OBS. Ej slutredigerad version, smärre luckor samt avvikelser mot publicerad version kan förekomma.

Den västerländska demokratins grundstenar – pluralism, fria medier, öppenhet – förefaller vara under ökat tryck från auktoritära staters subversiva inflytande. Icke-demokratiska styren, i motsats till vad många antog i samband med kommunismens fall i Europa 1989–91, har snarare än att konvergera mot demokratiska normer i flera fall stärkt sina auktoritära karaktärsdrag. Även om världen blivit mer globaliserad och sammanlänkad än någonsin i mänskligheten historia har den liberala demokratins normativa kraft förskjutits och försvagats. År 2006 började mängden demokratier i världen att sjunka för första gången sedan 1945. Parallellt har de ledande auktoritära staterna med ökat självförtroende vänt sig utåt, i syfte att påverka det internationella systemet i en riktning mer gynnsam och anpassad för deras inrikes- och utrikespolitiska målsättningar (Walker, 2016; Pomerantsev 2015).

Under tjugohundratalet kom en ökad mängd stater att använda internet och sociala medier som ett verktyg för att angripa inhemska motståndare, granskande medier, och oberoende forskning. Enligt en studie vid Oxford University använde regeringar sådana taktiker i 81 olika länder 2020, en ökning från 70 länder 2019 (Bradshaw et al 2021). Över tid upptäckte vissa stater att samma verktyg också kunde användas mot andra länder. Med en relativt liten investering i personal och teknologi kan främmande makt använda sig av öppna och dolda kommunikationsverktyg för att förstärka existerande klyftor i ett lands valmanskår, sprida desinformation och konspirationsteorier, och underminera tilltron till demokratins institutioner och valsystem. Mellan hösten 2016 och våren 2019 registrerades 20 försök att påverka demokratiska val världen över (Posard et al, 2020). Påverkanskampanjer kan även bedrivas i koordination mellan stater (regeringar) och privata aktörer. Sedan 2018 har forskare kunnat dokumentera förekomsten av minst 65 företag verksamma internationellt inom digital påverkan å ett politiskt partis vägnar (Bradshaw et al, 2021).

Två händelser i modern tid förde upp frågan om ryska påverkanskampanjer på den politiska dagordningen i EU och Nato: den ryska Krimannekteringen i februari 2014, följt av en pågående ”hybridkrigföring” i östra Ukraina, och den ryska inblandningen i USA:s presidentval i november 2016. Även om händelserna särskiljer sig i relevanta hänseenden – inte minst avseende bruket av militära maktinstrument i Ukraina – belyser de också intressanta likheter, som bruket av cyberattacker, spridande av propaganda och desinformation, och förekomsten av så kallat plausibelt förnekande (där angriparen förnekar sin roll i de pågående skeendena). Påverkanskampanjer är sålunda uttryck för en form av hybridhot, som inte enkelt kan bemötas utan måste hanteras genom en kombination av samhälleliga, politiska och juridiska instanser.

I fokus för denna rapport står taktiker för valpåverkan som med en hög grad av säkerhet kan knytas till ryska myndigheter eller den ryska federationens politiska ledning, med särskild hänsyn till frågor med bäring på det demokratiska valsystemets integritet. Även om valpåverkan ofta stått i förgrunden i diskussioner om främmande makts påverkanskampanjer finns det inget som säger att sådana behöver begränsa sig till denna fråga. Påverkan utifrån kan rikta sig mot olika strategiska svenska intressen, nationellt och internationellt – och utöver landets demokratiska processer beröra exempelvis frågor om teknologiöverföring och investeringar, svenskt deltagande i multilaterala organisationer (som EU, Nato och OSSE), eller frågor som den europeiska säkerhetsordningen (som respekten för staters suveränitet och territoriella integritet).

Rapporten fördelar sig i tre avsnitt. Det första avsnittet ger en kort bakgrund till ämnet och dess rättsliga ramverk. Det andra avsnittet beskriver några av de mest kända taktikerna för valpåverkan. Det sista avsnittet listar rekommendationer på tillvägagångssätt för att bemöta valpåverkan.

Valpåverkan: allmänna karaktäristika och rättsliga ramverk

Termen valpåverkan syftar på taktiker som påverkar genomförandet av demokratiska val, och därmed dess integritet och legitimitet. Två ofta uppmärksammade exempel på taktiker är cyberattacker utförda av regeringar, eller av aktörer i nära koordination med dem, och aktiviteter i sociala medier utförda av så kallade trollfabriker. I båda fallen bedrivs kampanjerna i det fördolda, på ett sätt som är koordinerat och långsiktigt, och där den faktiska avsändarens identitet hemlighålls från allmänheten.

Det amerikanska presidentvalet 2016 utgör ett av de mest illustrativa exemplen på storskalig valpåverkan mot en demokrati. Inför valet användes cyberattacker och kampanjer i sociala medier på ett sätt som syftade till att skapa maximal påverkan. Ryska hackers, kopplade till landets militära underrättelsetjänst GRU, hackade epost från företrädare för det demokratiska partiets valkampanj. Denna epost läcktes sedermera till allmänheten genom ett falskt Twitter-konto benämnt ”DC Leaks”, och relaterade försök att få spridning genom Facebook och epostmeddelanden till utvalda journalister. En del av materialet spreds i koordination med Julian Assange, ledaren för Wikileaks, som i sin tur stod i kontakt med företrädare för republikanernas presidentkandidat Donald Trump. Valet av namnet ”DC Leaks” var

genomtänkt, och syftade till att förmedla intrycket av att läckornas ursprung var någon på insidan av Washingtons politiska system. Så kallade trollfabriker, däribland Internet Research Agency (IRA) i Sankt Petersburg, bidrog till att ge materialet spridning (XXXX).

Diskussioner om valpåverkan utifrån fastnar ofta i frågan om signifikans, eller distinktionen mellan intention och effekt. Frågan har inget enkelt svar, och effekt är i praktiken svårt att mäta (XXXX). Å ena sidan utgjorde de ryska kampanjerna i sociala medier enbart en försvinnande liten del av den totala digitala kommunikation som ägde rum i USA inför valet. Såtillvida hade de inte heller någon enkelt mätbar eller synlig påverkan på valet. Å andra sidan avgjordes valet med en mycket liten marginal, omkring 80 000 röster i tre delstater. Även om samlade påverkanskampanjerna mot valet enbart hade marginell effekt kan de, genom att påverka opinioner eller befolkningens grad av valdeltagande, ha varit betydelsefulla för valutgången (Jamieson, 2018).

Den mer betydelsefulla frågan är principiell: även om valpåverkan utifrån som sådan är marginell eller verkningslös bör en demokratisk stat ta hotet på allvar. Hotbilden som sådan avgörs inte av det specifika hotet utan av den potentiella splittring som hypotetiskt kan orsakas. Extern inblandning i ett demokratiskt val kan ha menlig inverkan på dess upplevda legitimitet, och skapa indirekta effekter i termer av inrikespolitisk polarisering. I USA har frågan om rysk påverkan i valet 2016 resulterat i långdragna rättsliga, politiska och mediala processer, som vid skrivande stund fortfarande pågår. Enligt en amerikansk Ipsos-mätning i juli 2018 uppgav 85 procent av demokraterna och 46 procent av republikanerna att Ryssland påverkat presidentvalet, en indikation på hur befolkningens upplevelser och tolkningar av händelsen fördelade sig partipolitiskt (Nieves, 2018). Snarare än konsensus kring och acceptans för en gemensam president betraktade en icke-negligerbar andel av valmanskåren Trump som illegitim (Associated Press/NBC News 2017). Med andra ord, en påverkanskampanjs effekt kan förstärkas ifall den förmår knyta an – avsiktligt eller oavsiktligt – till redan föreliggande spänningar, patologier och/eller klyftor i ett samhälle (Rid, 2020).

Det finns fullt legitima sätt för stater att kommunicera till målgrupper i andra länder, den så kallade offentliga diplomatin. Radiosändningar, tevekanaler och hemsidor på olika språk är ett numera vanligt sätt för enskilda länder att nå ut internationellt. Likaså har politiker i Land A rätt att uttrycka åsikter om vem de vill se som regeringsbildare i Land B. De folkrättsliga aspekterna av valpåverkan har förblivit outredda. Enligt Ohlin (2021) uppstår en folkrättslig kränkning när påverkan utifrån kränker en annan stats *domaine réservé*, ett lands suveränitet

och rätt till självbestämmande. I en demokratisk stat uttrycks självbestämmande bland annat genom allmänna val, vilket sätter gränser för exempelvis vem som har rätt att rösta i ett val. Men i praktiken är det i första hand nationell lagstiftning som aktualiseras i frågor om valpåverkan – exempelvis regelverk kring finansiella bidrag och transparens kring partier och andra aktörer som deltar i valet. När det amerikanska justitiedepartementet 2018 väckte åtal mot ryska invånare för att på uppdrag av sin regering ha blandat sig i 2016 års presidentval grundades åtalspunkterna i lagstiftning kring exempelvis identitetsstöld, bedrägeri och cyberintrång (Justice Department 2018). Det säkra antagandet är sålunda att de primära rättsliga skyddsvallarna torde förbli grundade i nationella lagstiftningar snarare än reglerade i internationella traktat, och därmed variera mellan länder.

Taktiker för valpåverkan

Till de vanligaste taktiker som kopplats till rysk valpåverkan hör propaganda och offentlig diplomati, desinformation, cyberattacker och *hack-and-leaks*, och finansiell påverkan. Taktikerna har kunnat användas i olika utsträckning, och med olika grad av koordination, varför uniforma och enhetliga mönster sällan upprepas mellan enskilda länder.

Propaganda och offentlig diplomati

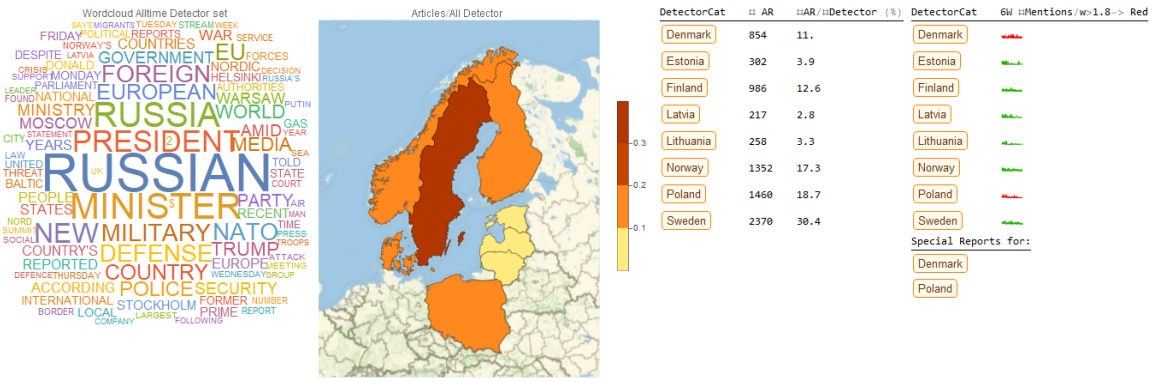
På ett grundläggande plan kan försök till påverkan ske genom offentlig diplomati, exempelvis uttalanden av politiker och statstjänstemän. Med hotfull retorik kan avsändaren söka uppnå en psykologisk effekt, som i sin tur avser övertyga mottagaren av budskapet att omvärdera sina strategiska vägval. Företrädare för den ryska regeringen förklarade 2015 att Ryssland skulle svara på finskt respektive svenskt närmande till Nato med militära motåtgärder. Rysslands ambassadör till Köpenhamn hävdade samma år att installationen av ett missilförsvarssystem i Danmark kunde bli föremål för ryska kärnvapenangrepp i händelse av konflikt (Benitez 2015; France25 2015). Huruvida diplomatiska påtryckningar och/eller hot uppnår avsedd effekt eller ej är förstås en öppen fråga, och beror på olika faktorer som mottagarlandets inrikespolitiska kultur och maktbalans mellan de inblandade staterna.

Ett annat instrument inom offentlig diplomati är propaganda och internationell media. Under tjugohundratalet investerade Ryssland i tevesändningar, radio och hemsidor på flera olika

språk, däribland RT (tidigare Russia Today) och Sputnik International. En kortvarig svenskspråkig version av Sputnik uppstod 2015, men avvecklades inom loppet av omkring ett år (sannolikt på grund av få besökare och lågt genomslag).

En systematisk studie av ryska statsmedier kan ge indikationer om Rysslands strategiska mål, såtillvida att landets statliga medier kan antas företräda regeringens intressen. Figur 1 visar omnämnanden av sju nordeuropeiska länder i engelskspråkiga Sputnik från 2016 till 2020. Sverige omnämns under tidsperioden på hemsidan 2370 gånger, eller 30,4 procent av alla omnämnanden. På andra plats kommer Polen, med 18,7 procent av alla omnämnanden, följt av Norge (17,3 procent), Finland (12,6 procent) och Danmark (11 procent). Sverige har med andra ord tilldragit sig ett förhållandevis stort intresse i jämförelse med sina grannländer. Ordmolnet visar de vanligaste orden för samtliga artiklar. Genom att avgränsa datainsamlingen för vissa temata eller tidsperioder är det möjligt att generera en mer högupplöst och detaljerad bild av ryska officiella synsätt på ett lands politiska system, exempelvis inför ett politiskt val.

Figur 1. Omnämnanden av sju länder i Sputnik International, 2016–20.



Källa: Pågående insamlingsprojekt. För mer information, vänligen kontakta rapportförfattaren. Datainsamlingen för föreliggande figur skedde från september 2016 till september 2020.

Desinformation

Desinformation är information som är falsk eller vilseledande, och som syftar till att uppnå en viss påverkanseffekt hos en målgrupp. Som taktik betraktad har desinformation sina rötter i

kalla krigets politiska krigföring mellan Sovjetunionen och västblocket. I kombination med digitala kommunikationsverktyg, som internet och sociala medier, kan desinformation spridas på ett sätt som tillåter anonymitet, döljande av ursprung, och bred spridning. Inför det svenska riksdagsbeslutet om ett närmande till Nato (2016 års så kallade värdlandsavtal) spreds falska dokument om svenska politiker, som anklagades för att konspirera med andra länder i syfte att försvaga Ryssland. Några svenska nyhetsmedier, däribland Dagens Nyheter och Expressen, gav spridning åt ett av de falska påståendena, liksom flera ryska statsmedier. En kontextuell analys av dokumenten attribuerade dokumenten till en rysk desinformationskampanj (Kragh & Åsberg 2017), något som sedermera bekräftades av Facebook, som använt sig av teknisk attribution (en digital spårning av dokumentens ursprung) för att knyta vissa konton i sociala medier till den ryska säkerhetstjänsten (Nimmo et al, 2020). En mindre kampanj inbegripandes falska dokument skapades även inför 2018 års riksdagsval, syftandes bland annat till att ifrågasätta Sverigedemokraterna, även om denna kampanj aldrig gavs någon större spridning (Kragh, 2018; Dagens Nyheter 2018).

Desinformation och spridande av konspirationsteorier kan skapa oro också i den fysiska världen. I januari 2016 gav ryska statsmedier spridning åt påståenden att en flicka med ryskt påbrå bosatt i Tyskland kidnappats och utnyttjats sexuellt av män från Mellanöstern. Fallet ådrog sig uppmärksamhet från Rysslands utrikesminister, Sergej Lavrov, som anklagade tyska myndigheter för undfallenhet avseende den ryska diasporans säkerhet. Ryska statsmedier gav nyheten stor spridning, också gentemot målgrupper i Tyskland. Innan det att nyheten kunde avslöjas som falsk hade gatuprotester och kampanjer mot den tyska regeringen, däribland organiserade av tyska högerextremister, ägt rum i Tyskland (XXXX).

Med hjälp av automatiserade konton – så kallade *bots* – och koordinerade kampanjer i sociala medier kan desinformation ges snabb och storskalig spridning inom en målgrupp. I vilken mån dylika kampanjer kan uppnå en verkan är, som noterades ovan, inte enkelt att utreda (Shane & Mazetti, 2018). Den ryska trollfabriken IRA skapade inför det amerikanska presidentvalet 470 oäkta Facebook-profiler i syfte att uppträda som autentiska amerikanska väljare och organisationer. Mellan januari och augusti 2017 producerade dessa profiler omkring 80 000 inlägg med en potentiell räckvidd om 29 till 126 miljoner användare. På Twitter skapades nära fyra tusen användarkonton som sammanlagt gjorde 176 000 inlägg med en potentiell räckvidd om 1,4 miljoner mottagare. Men den totala mängden inlägg på Twitter var vid tidpunkten cirka 350 000 inlägg varje minut, eller 500 miljoner inlägg varje dag. Av de sociala mediernas totala informationsflöde utgjorde IRA:s aktiviteter enbart en liten del.

Likväl bör riskerna med digitala kampanjer inte underskattas. Över en längre tidshorisont kan ihållande desinformationskampanjer förstärka misstro mellan olika grupper, vilket minskar demokratiska staters förmåga att hantera olika samhällsfrågor. Våren 2019 avslöjades digitala kampanjer, med dolda band till den ryska nyhetskanalen Sputnik, syftandes till att stödja ett antal polska högerextrema och nationalistiska politiker. När Facebook avlägsnade flera av deras hemsidor kunde de konstatera att kampanjen haft en förmodad räckvidd till över fyra miljoner polska användare (VSquare, 2019). Digitala kampanjer kan även användas för att avskräcka människor från att delta i demokratiska val. Inför det amerikanska presidentvalet 2020 hade ryska och iranska hackers kommit över register om amerikanska väljare, information som Iran använde sig av för att skicka hotfulla meddelanden via epost till demokratiska väljare. Bakom täckmanteln ”Proud Boys”, en högerextrem organisation, hotade de mottagarna med budskapet ”we will come after you” (New Atlanticist, 2020)

Enligt en analys av Facebook avlägsnade företaget över 150 hemliga påverkanskampanjer på sin plattform mellan 2017 och maj 2021. Twitter har sedan oktober 2018 attribuerat över 85 000 falska konton till manipulativa kampanjer i tjugo olika länder. Kampanjerna riktade in sig mot flera olika länder och målgrupper, kunde vara såväl utländska som inhemska, och vara styrda av såväl regeringar som företag, politiska aktörer eller andra aktörer. Storskaliga kampanjer som bedrivs bakom täckmantel benämns av Facebook icke-autentiskt beteende (Facebook 2021; Twitter 2021).

Cyberattacker och *Hack-and-Leaks*

Cyberattacker mot måltavlor inom politik, akademi och industri har varit ett växande problem under årtionden. På valdagen våren 2014 hackades den ukrainska valkommissionens hemsida av en enhet tillhörande den ryska militära säkerhetstjänsten GRU. Angriparna lade upp falsk information om att troliga segrare var en okänd högerextremist, trots att personen i verkligheten inte erhållit mer än 0,7 procent av rösterna. Även om valkommissionen kunde hantera och åtgärda angreppet gavs det falska resultatet spridning av rysk statstelevision, som vid tidpunkten nådde många tittare även i Ukraina, sannolikt i syfte att diskreditera landets politiska system (Rid, 2020).

De senaste åren har samma hackerkollektiv knutits till försök att hacka och påverka politiska val i flera västländer, däribland i Frankrike (2017) och Tyskland (2015 och 2021). De har

även knutits till angrepp mot icke-politiska organisationer, som det svenska riksidrottsförbundet och den internationella antidopingorganisationen WADA (Dagens Nyheter 2018). Hackade dokument och läckor kan användas för att utöva politiska påtryckningar, skapa partiella läckor, blanda autentiska och falska dokument, eller rikta falska anklagelser mot politiska motståndare. Med hjälp av sociala medier kan dokumenten ges snabb och storskalig spridning.

Läckor kan användas strategiskt för att skada en enskild individ, organisation, eller ett politiskt parti. Särskild påverkanseffekt kan uppnås ifall dokumenten ges spridning av etablerade medier. Hösten 2018 utsattes den brittiska tankesmedjan Integrity Initiative för en *hack-and-leak*-kampanj av ryska hackers, understödda av ryska statsmedier. Enligt ryska medier avslöjade dokumenten tankesmedjans hemliga band till den brittiska underrättelsetjänsten – påståenden som i Sverige gavs omfattande spridning av Aftonbladet. Trots att anklagelserna visade sig vara rysk desinformation skulle Aftonbladets ledning försvara publiceringarna med hänvisning till att de utgjorde en del av tidningens ”kulturdebatt” (Samuelsson, 2019; Ståhle, 2019). Falska påståenden kan sålunda få viss effekt, när konventionella pressetiska eller demokratiska instinkter överges eller kortsluts.

Politiskt inflytande

Den ryska politiska ledningen har på olika sätt sökt knyta an till politiska partier i EU där gemensamma och överlappande intressen kan föreligga. Olika politiska frågor, som migration, kultur och identitet, har kunnat användas av Kreml för att få stöd i andra länder. Påverkanskampanjer är sålunda inte enkelriktade. I enskilda länder kan det finnas målgrupper som också delar – i varierande utsträckning – avsändarens värderingar. I EU-länder som Tyskland, Frankrike, Italien och Österrike finns politiska partier inom ytterhögern som initierat formella samarbeten med Kreml eller maktpartiet Enade Ryssland, exempelvis italienska Lega (tidigare Lega Nord), Alternativ för Tyskland, det Österrikiska frihetspartiet (FPÖ), och franska Nationell samling (tidigare Front National). Men även företrädare för vissa vänsterpartier, som tyska Die Linke, har exempelvis öppet stöttat den ryska Krimannekteringen 2014 (Shekhovtsov, 2019).

I vissa sammanhang har det uppstått en symbios. Företrädare för ovan nämnda partier har exempelvis deltagit i ryska statsmedier, ofta under missvisande varudeklarationer som

”Syrienexpert” eller ”geopolitisk analytiker”, och alltid med ambitionen att försvara Rysslands agerande. Vidare har de regelbundet deltagit som ”valobservatörer” i ryska politiska val – vilka de omedelbart godkänt som demokratiska och fria. Inför den franska valkampanjen 2014 mottog Front National ett mångmiljonlån från en rysk bank, vilket aktualiserade två former av risk. Dels att partiet fick ett finansiellt beroende, dels att partiet sattes under tryck när ägarna av skuldbeloppet 2020 krävde återbetalning (RFERL, 2020).

Politisk samverkan kan även aktualisera korruptionsrisker. I maj 2019 imploderade Österrikes regering efter det att en videofilm avslöjat hur landets vicekansler och ledaren för Frihetspartiet under ett möte uttryckt en beredvillighet att samarbeta med ryska affärsintressen för politisk vinning. Det skulle senare framkomma att mötet var en fälla gillrad av en österrikisk privatdetektiv (Spiegel, 2019).[1] En snarlik men mer reell skandal snärjde Lega, efter det att en av partiets närmaste medarbetare avslöjades ha ingått en hemlig finansiell konspiration med ryska intressen. En läckt ljudupptagning från ett möte i Moskva avslöjade återkommande interaktioner mellan medarbetaren och ryska motparter i syfte att kanalisera stöd till Legas kommande valkampanjer, däribland genom falska affärsupplägg involverandes oljetransaktioner (XXXX).

Politisk samverkan med företrädare för auktoritära stater väcker frågor om det demokratiska samhällets gränser gentemot omvärlden – en problematik som även ställdes på sin spets i exempelvis rekryteringen av frivilliga EU-medborgare till terrorsekten IS under kriget i Syrien, eller inflytandet från radikal islamism från länder som Saudiarabien och Iran. Det finns även andra former av politisk subversion som kan användas för att destabilisera demokratiska system. Det kinesiska kommunistpartiet använde sig 2014 av provokatörer för att angripa demokratiaktivister i Taiwan, och i Montenegro sökte den ryska militära underrättelsetjänsten GRU åstadkomma en statskupp före 2016 års val. Påverkan kan även ske indirekt, som när den belarusiska regeringen sommaren och hösten 2021 lät transportera tusentals migranter till gränsen med Polen och Litauen, i syfte att utöva politiska påtryckningar mot EU (XXXX).

[1] https://www.spiegel.de/ausland/ibiza-affaere-um-heinz-christian-strache-ein-jahr-spaeter-der-abgrund-a-1c591f39-dca4-4aed-a9ea-08077f160ac5; https://www.ft.com/content/61921fbf-fe86-4e5b-89d7-3f4d0d6641a7; https://www.wienerzeitung.at/nachrichten/politik/oesterreich/2011275-Staatsanwaltschaft-ermittelt-in-der-Causa-Ibiza-Video.html

Demokratisk integritet och motståndskraft

Föreliggande rapport har överskådligt beskrivit olika taktiker som främmande makt kan använda i syfte att påverka ett politiskt val. Demokratiska stater måste skydda sig mot hybridhot, eller statliga påverkanskampanjer, utan att underminera sina egna värderingar. Utökad statlig kontroll över civilsamhället riskerar att göra det öppna samhället mer slutet. Inte heller kan demokratier spegla bruket av desinformation eller valpåverkan, eftersom sådana strategier enbart ytterligare skulle underminera liberala principer världen över. Försvagade demokratier skulle i sin tur vara mindre kapabla att möta olika former av hybridhot från auktoritära stater.

Det demokratiska samhällets potentiella svagheter är också dess styrkor. Principer om öppenhet, yttrandefrihet och tolerans är en form av mjuk makt som har utbredd legitimitet och attraktivitet. Genom att stärka förutsättningarna för och skyddet av det demokratiska samhället stärks även motståndskraften mot yttre påverkansförsök (Wigell, 2021).

Fokus för västerländska stater har varit att å ena sidan söka hindra och blockera, och å andra sidan svara och bemöta, påverkanskampanjer från främmande makt. Båda tillvägagångssätten bottnar i ett synsätt om att påverkanskampanjer handlar om oönskade informationsflöden, något som också begränsar det tänkbara responsutrymmet (Keating & Schmitt, 2020). Exempelvis har såväl nationella regeringar som EU och Nato skapat byråkratiska strukturer för att hantera och bemöta desinformation.

Att attribuera och bemöta påverkanskampanjer är ett första viktigt steg, men inte nödvändigtvis tillräckligt. Faktakontroll och etikettering av vilseledande material på sociala medier har visat sig ha liten effekt på människors benägenhet att tro eller inte tro på viss information (Clayton, et al, 2020). Att attribuera påverkanskampanjer kan även ta tid, vilket innebär att den centrala frågan är hur en befolkning hanterar och reagerar på ny information, snarare än förstår dess ursprung. Bemötandet av påverkanskampanjer måste i sin tur ske med hänsyn till att relevanta målgrupper av olika skäl – ideologiska, intellektuella, pekuniära, osv – kan vara attraherade av kampanjernas centrala budskap (Keating & Schmitt, 2020).

Det finns även en risk för att vissa påverkanskampanjers betydelse överdrivs. Att överreagera, exempelvis genom krav på förbud, inskränkningar eller censur, kan riskera att göra det öppna demokratiska samhället mer slutet. Inte heller förtjänar samtliga hot att bemötas, och hot kan även bemötas på olika nivåer – från den statliga (nödvändigt för att hantera exempelvis

avancerade cyberhot) till den rättsliga (med exempelvis krav på transparens och anti-korruption), samhälleliga (genom exempelvis media och akademi) och den politiska (politiska partier och civilsamhälle). Demokratins integritet kan enbart stärkas i samverkan mellan samhällets olika sfärer.

Referenser

Associated Press/NBC News (2017). https://www.nbcnews.com/news/us-news/majority-young-americans-view-trump-illegitimate-president-poll-n735426

Benitez, https://www.usnews.com/opinion/blogs/world-report/2015/08/06/russia-bullies-sweden-and-finland-away-from-joining-nato

Samantha Bradshaw, Hannah Bailey & Philip N. Howard. "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." (2021) Oxford, UK: Programme on Democracy & Technology.

Clayton, Katherine, et al (2020), Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media, *Political Behavior*, 42: 1073–1095.

Dagens Nyheter (2018), https://www.dn.se/sport/kreml-pekas-ut-bakom-cyberattack-mot-riksidrottsforbundet/

Facebook (2021), https://about.fb.com/news/2021/05/influence-operations-threat-report/

France24 (2015), https://www.france24.com/en/20150322-russia-denmark-nato-ambassador-nuclear-attack-ships

Jamieson, Kathleen Hall, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*, Oxford: Oxford University Press, 2018.

Justice Department (2018). https://www.justice.gov/file/1035477/download

Kragh, Martin, https://www.martinkragh.com/martin-kragh-blog/2018/12/2/disinformation-against-sweden-democrats-and-swedish-election

Nieves, https://www.politico.com/story/2018/07/18/poll-russia-meddling-election-mueller-investigation-730529

Nimmo, Ben, et al (2020), https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

Ohlin, 2021

Posard, et al, 2020 (RAND)

RFERL (2020), https://www.rferl.org/a/russian-firm-seeks-to-recover-11-million-loan-from-french-far-right-leader-s-party/30415776.html

Rid, Thomas, *Active Measures*

Samuelsson, Lena, (2019), https://www.aftonbladet.se/nyheter/kolumnister/a/3JKeEA/viktiga-principer-for-journalistiken-slas-fast

Twitter (2021), https://transparency.twitter.com/en/reports/information-operations.html

VSquare (2019), https://vsquare.org/disinformation-network-on-facebook-supported-by-polish-deputy-minister-of-digitization/