Informationskampen och Ukraina — memo 1

Folkets underrättelsetjänst — öppna källor "OSINT" och Ukraina

Ivar Ekman och Per-Erik Nilsson

Kriget i Ukraina är på många sätt ett chockerande gammaldags krig. En brutal invasion av ett slag som många trodde inte kunde ske i dagens Europa. Men samtidigt är det ett krig som åtminstone delvis utspelar sig i en slående modern miljö: den digitaliserade informationsmiljön. I en serie memon kommer FOI berätta om, beskriva och analysera hur det här utspelar sig — den kamp som pågår kring och med information, på såväl som bortom det fysiska slagfältet. Krig och kommunikation har alltid hängt nära samman, men med kriget i Ukraina är den kopplingen starkare än någonsin.

Utifrån ett medie- och kommunikationsperspektiv omtalas det ryska invasionskriget[1] av Ukraina som historiskt.[2] Månader innan invasionen fylldes sociala medieplattformar av bilder och filmer på ryska stridsvagnar, truppförflyttningar och spekulationer om vad som var på väg att hända. I vissa kretsar kom den videobaserade mikrobloggen TikTok snabbt att benämnas som TankTok.[3]

Precis i början av invasionen utspelade sig en kuriös — men talande — debatt i sociala medier om ryska intentioner och förmågor. Det handlade om ifall Ryssland skulle göra en stor landstigning nära Mariupol från Azovska sjön. På ena sidan stod en anonym, högt uppsatt tjänsteman på USA:s försvarshögkvarter Pentagon, som citerades av flera medier.[4] Tjänstemannen hävdade att en landstigning med tusentals ryska soldater var nära förestående. På den andra sidan stod en bloggande, pensionerad belgisk marinofficer, som inte hade tillgång till några hemligstämplade underrättelser —men väl en mängd öppet tillgänglig data och information från kommersiella satelliter och sociala medier. Han hävdade med bestämdhet att någon stor landstigning inte var aktuell. Belgaren fick rätt.[5]

Att belgaren hade rätt kan ju förstås ha varit ren tur — och det går inte att veta vad tjänstemannen från Pentagon visste och inte visste, eller vad syftet med hans uttalande egentligen var. Men händelsen pekar på en viktig utveckling kring hur information sprids och samlas i samband med ett krig. Belgaren är nämligen bara ett exempel av många på hur engagerade civila, både med och utan militär bakgrund, med hjälp av lättillgängliga digitala verktyg har kunnat producera slående precisa och väl underbyggda analyser om kriget i Ukraina. Det här fenomenet har i media och av individerna själva ofta kommit att benämnas med en term från underrättelsevärlden — OSINT, från engelskans *Open Source INTelligence* (underrättelse baserat på öppna källor).

Men, är det som görs öppet och av amatörer och icke-statliga organisationer verkligen OSINT — alltså att betrakta som underrättelseverksamhet?[6] Svaret är på ett plan enkelt: nej. Begreppet som används är sedan länge en vedertagen del av

1 Här åsyftas invasionskriget som startade den 24 februari 2022. Invasionen bör förstås som den andra vågen av den ryska invasionen som startade med annekteringen av Krim 2014.

2 Se t.ex: Matthew Moran (2022), ”Open-Source Intelligence: How Digital Sleuths Are Making the Mark on the Ukraine War”, The Conversation, 18 mars: https://theconversation.com/open-source-intelligence-how-digital-sleuths-are-making-their-mark-on-the-ukraine-war-179135/; Leo Schwartz (2022), ”Amateur open- source researchers went viral unpacking the war in Ukraine”, *Rest of World*, 7 mars: https://restofworld.org/2022/osint-viral-ukraine/; The Economist (2022), “A new era of transparent warfare beckons: Russia’s manoeuvres are a coming-out party for open-source intelligence”, 19 februari.

3 Verity Bowman (2022), “Russia-Ukraine crisis: Will this be the ‘First TikTok War’”, *The Telegraph*, 29 januari: https://www.telegraph.co.uk/world-news/2022/01/29/russia-ukraine-crisis-will-first-tiktok-war/.

4 Se t. ex.: Tara Copp (2022), “‘Amphibious Assault is Underway’: Russian Troops Are Landing In Eastern Ukraine, Pentagon Says”, *Defense One*, 25 februari: https://www.defenseone.com/threats/2022/02/amphibious-assault-underway-russian-troops-are-landing-eastern-ukraine-pentagon-says/362452/.

5 Alison Bath, “Open source intelligence observers gain growing role in how war is observed”, *Stars and Stripes,* 29 mars, https://www.stripes.com/theaters/europe/2022-03-29/citizen-osint-analysts-chronicle-russian-navy-role-in-war-in-ukraine-5513788.html

6 Se: Bowman H. Miller (2018), ”Open Source Intelligence (OSINT): An Oxymoron?”, *International Journal of Intelligence and Counterintelligence* 31(4): 702-719.

FOI Memo: 7888
Projektnummer: I1498503
Godkänd av: Anders Norén

Juni 2022

den indelning som görs inom underrättelsevärlden, vid sidan av kategorier som HUMINT, SIGINT och GEOINT.[7] Det som saknas i den här högteknologiska amatörversionen av ”OSINT” är en tydlig beställare och mottagare av informationen och analysen, vilket är en förutsättning för att något ska vara *intelligence,* alltså underrättelser. De mer etablerade aktörerna i den här världen, som Bellingcat, är också noggranna med att inte kalla det de gör för OSINT. De beskriver det snarare som en avancerad form av grävande journalistik — inte minst för att göra tydligt att det inte sker på uppdrag av en statsmakt, och med det minska risken för att ses som en part i den konflikt man bevakar.[8]

Vad är då denna märkliga, moderna kombination av glada amatörer och underrättelsemetodik som trots att det är något annat ofta kallas ”OSINT”? Fenomenet är inte nytt för Ukraina-kriget. Det har gradvis vuxit fram som en effekt av de senaste tre decenniernas digitalisering — spridningen av sociala medier, smarta telefoner med alltmer avancerade sensorer, och en allt större tillgänglighet till en sorts data som tidigare varit reserverad för statsaktörer, som satellitdata och transponderdata från flygtrafik.[9] Fenomenet tog form och fick struktur under det sena 00-talet och tidiga 10-talet, med den gröna revolutionen i Iran 2009, den arabiska våren och framförallt kriget i Syrien som viktiga händelser.[10] I Syrien dokumenterades olika former av krigsbrott, med hjälp av filmer och bilder från sociala medie-konton, som sedan verifierades med hjälp av annan information, som kommersiellt tillgängliga satellitbilder.[11]

”OSINT” i Ukrainakriget

Redan tidigt under kriget i Ukraina blev bredden och styrkan i den här verksamheten iögonfallande tydlig. Utöver bilder och videor på alltifrån truppförflyttningar till tidsstämplad geolokalisering av mördade civila sker även en grupp-baserad verifiering av data, informationskällor och dessas pålitlighet. I flertalet fall har resultaten varit både tydliga och slående precisa.

Den här världen består av en bred variation av såväl hobbyanalytiker — till exempel en 20-årig amerikansk student med Twitter-kontot @intelcrab — som mer etablerade organisationer som brittiska Bellingcat. Det har också uppstått flera semi-strukturerade mötesplatser på nätet, där en stadigt växande grupp amatöranalytiker möts för att diskutera, verifiera och utvärdera händelser och ny information i realtid. Ett sådant exempel är Project Owl, en server på den sociala medieplattformen Discord där verksamheten delats upp i specialområden — såsom satellitinformation från kommersiella aktörer (”#geospatial”), transponderinformation (”#aviation”) och generell analys av öppna källor (”#general-osint”). Verksamheten på Discord och liknande plattformar är tydligt samarbetsinriktad — information publiceras med specifika frågor som sedan besvaras av deltagare med tid och specialkunskaper. Det är med andra ord fråga om en form av ”crowd wisdom”, eller massans visdom.[12] Mycket av informationen och analysen delas sedan på mer publika plattformar, framförallt Twitter, där de största kontona under kriget vuxit till att få hundratusentals följare. Även traditionella medier har i allt större utsträckning börjat både hänvisa till information som sprids i de här kanalerna, och även att göra egna analyser av samma slag.[13]

Några av de mest uppmärksammade exemplen under krigets första månader är: de bilder och filmer som spreds av den ryska invasionsstyrkan innan kriget bröt ut, i synnerhet på Telegram, TikTok och Twitter, som gav en tydlig bild av den nära förestående invasionen; sammanställningar av ryska militära förluster som i den så kallade Oryxlistan, som visat hur omfattande dessa varit; verifieringen av massakern i Butja via satellitbilder; och den kollektiva jakten på ryska oligarkers yachter i västvärldens hamnar.

7 Se: Gasper Hribar, Iztok Podbregar och Teodora Ivanusa (2014), ”OSINT: A ’Grey-Zone’?”, *International Journal of Intelligence and CounterIntelligence* 27(3): 529-549; Arthur S. Hulnick (2010), “The Dilemma of Open Sources intelligence: Is OSINT Really Intelligence?”, i *The Oxford Handbook of National Security Intelligence*, redigerad av Loch K. Johnsson: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.001.0001/oxfordhb-9780195375886-e-0014

8 Se: Gasper Hribar, Iztok Podbregar och Teodora Ivanusa (2014), ”OSINT: A ’Grey-Zone’?”, International Journal of Intelligence and CounterIntelligence 27(3): 529-549; Arthur S. Hulnick (2010), “The Dilemma of Open Sources intelligence: Is OSINT Really Intelligence?”, i The Oxford Handbook of National Security Intelligence, redigerad av Loch K. Johnsson: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.001.0001/oxfordhb-9780195375886-e-0014

9 Se: Lars D. Nicander (2011), ”Understanding Intelligence Community Innovation in the Post-9/11 World”, *International Journal of Intelligence and CounterIntelligence* 24(3): 534-568.

10 Se: Cameron Colquhoun, ”A Brief History of Open Source Intelligence”, *Bellingcat,* 160614, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

11 För en studie av fenomenet och metoder för att arbete med öppna källor i samband med konflikt, se: Jeff Deutch och Hadi Habal (2018), ”The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms”, *State Crime Journal* 7(1): 46-76.

12 Se: James Surowiecki (2005), *The Wisdom of Crowds* (New York: Knopf).

13 New York Times använde till exempel öppet tillgängliga satellitbilder för att motbevisa ryska påståenden att massakern i Butja var iscensätt av Ukraina och Nato, se: Malachy Browne, David Botti och Haley Willis (2022), ”Satellite Images Rebut Russia’s Claim on Bucha”, *The New York Times*, 4 april: https://www.nytimes.com/2022/04/04/world/bucha-ukraine-bodies.html.

Det finns — trots styrkorna — tydliga potentiella och verkliga problem med den här typen av verksamhet. Eftersom den inte är institutionaliserad och systematiskt följer etablerade metoder finns utmaningar med sådant som verifikation och källkritik.[14] Vidare sker mycket av verksamheten i sociala medier som drivs av kommersiellt inriktade algoritmer, vilket premierar uppseendeväckande innehåll framför saklig analys.[15] Verksamheten är inte heller riktad, vilket innebär att det är svårt att veta värdet av det som analyseras i ett större perspektiv; små, oviktiga händelser kan ges större vikt än de förtjänar. Slutligen finns en uppenbar risk för manipulation i form av desinformation och felaktigheter.[16]

Utmaningar för underrättelseverksamheten

Den här utvecklingen lyfter flertalet frågor till och utmaningar för den traditionella underrättelseverksamheten. Det är tydligt i forskningslitteraturen att det länge funnits en medvetenhet inom underrättelsevärlden att digitaliseringen och det ökade öppna informationsflödet skapat ett behov av att bättre kunna ta hand om öppen information och förädla den till genuin OSINT.[17] Men att analysera de enorma mängder öppen information som nu finns tillgänglig är en både arbets- och teknikintensiv verksamhet. Den skiljer sig också på många sätt från den traditionella underrättelseprocessen, och litteraturen tydliggör att nödvändiga reformer av arbetssätt och syn på kompetens tar tid att realiseras.[18]

En risk för den klassiska underrättelseverksamheten är därför att den, i konkurrens med utvecklingen som beskrivits ovan, i både allmänhetens och beslutfattares ögon ser sig ifrånsprungen. Att snabbheten och detaljrikedomen i underrättelseliknande information som sprids i sociala medier och andra kanaler upplevs som en ersättning för mer arbetsintensiva, underbyggda och ofta tidskrävande analyser.[19] Hur ska då underrättelseorganisationer förhålla sig till den här utvecklingen? Det går att se flera alternativ.

Ett är att göra ingenting. Då finns risken att en process upprepas som synts i många andra informationstäta verksamheter under de senaste två decennierna, som i musik- och mediebranschen. Där har etablerad verksamhet först utmanats av teknikkunniga amatörer, försök till anpassning har skett och sedan har många etablerade aktörer, statliga som kommersiella, om inte sett sig ersatta av helt nya strukturer, så åtminstone fått helt nya konkurrenter att förhålla sig till. I OSINT-fallet skulle det exempelvis kunna handla om kommersiella aktörer som bygger upp en än bättre förmåga att strukturerat ta hand om öppen information och bearbeta den för betalande kunder — som då skulle kunna vara stater.

Ett annat alternativ är att helt försöka återskapa den process som vuxit fram organiskt i digitala forum. Det har hittills visats sig mycket svårt, även för resursstarka statsaktörer som USA.[20] Redan innan den digitala revolutionen förändrade förutsättningarna för mänsklig interaktion och kommunikation, kunde inte en enskild myndighet rymma all den kunskap och kompetens som krävs för att hantera öppna informationskällor.

En variant av detta är att systematiskt ta vara på den utveckling som skett i digitala medier, men att man tar hänsyn till de problem och brister som finns i den publika verksamheten och därför lägger på ett systematiserat lager av verifikation och analys. Detta kan till exempel vara tilltalande för ett mindre land med begränsade resurser, men det skulle också innebära utmaningar med tanke på hur snabbt utvecklingen sker i den här miljön.

En annan viktig fråga som aktualiseras av ”OSINT”-explosionen är den allmänt bredare spridningen av information som tidigare varit begränsad till stater och ofta är hemligstämplad. Förutom spridningen av publik underrättelseliknande information har Ukrainakriget även sett en större offentlig roll för genuina underrättelser i offentligheten – USA:s offentliggöranden av underrättelsematerial under tiden före krigsutbrottet

14 Se t.ex.: (2018), ”The Myth of Makarov”, *Valenta,* 13 maj: https://www.velenta.co.uk/post/the-myth-of-makarov.

15 Om kommunikation i digitala miljöer och dess fallgropar, se: Azeem Azhar (2021), *The Exponential Age: How Accelerating Technology is Transforming Business, Politics, and Society* (Diversion Books); *James Bridle* (2019*), New Dark Age: Technology and the End of Future* (London: Verso).

16 Om desinformation och felaktig information, se: Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume och Janina Herrera (2018), *Information Manipulation: A Challenge for Our Democracies,* Centre d’analyse, de prévision et de stratégie (CAPS) och Institut de recherche stratégique de l’École militaire, Paris.

17 Se: Christopher Eldrigde, Christopher Hobbs och Matthew Moran (2018), ”Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of ‘Big Data’”, *Intelligence and National Security* 33(3): 391-406.

18 Se: Heather Williams och Iliana Blum (2018), ”Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise”, Rand Corporation, RR-1964-OSD.

19 För en diskussion om detta, se: Emily Harding (2022), "Move Over Jarvis, Meet Oscar: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community", Centre for Strategic & International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220119_Harding_MoveOverJARVIS_MeetOSCAR_0.pdf?NqfrbU05ULzzcySzNHB0pTzsNYw3HdfK

20 Se t.ex: Heather Williams & Iliana Blum (2018), “Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise”, *Rand Corporation* RR1964.

är ett exempel, brittiska underrättelsetjänsters twittrande ett annat. Här syns en utveckling där den globala informationskampen har hårdnat, och där konkurrensen om vem som snabbast kan publicera relevant — men även tilltalande, spännande — information ökat.[21] Detta väcker frågor om hur en traditionellt skyddad och begränsad verksamhet ska förhålla sig till offentligheten, där så kallad ”OSINT” är en viktig del av en större utveckling.

”OSINT” och allmänheten

Vad innebär då ”OSINT:s” breda genomslag för informations-miljön mer generellt — för vanliga medborgare som konsumerar sociala medier och andra digitala kanaler där informationen och analyserna sprids? På ett sätt visar den här utvecklingen på demokratiseringspotentialen i transnationella och multiplattforma digitala medier. Under invasionskriget i Ukraina har till exempel ryska desinformationskampanjer och rena lögner kunnat motbevisas gång efter annan,[22] vilket har synliggjort för en bredare publik inte bara att desinformationskampanjer pågår, utan även vilken form de tar.

Samtidigt förefaller den här utvecklingen inte gå statliga aktörer obemärkt förbi. I skrivande stund har invasionskriget varat i drygt tre månader. Under det här korta tidsspannet har flera inbladade statsaktörer sökt anpassa sig till den nya så kallade OSINT-verksamheten. Flertalet ryska konton som utger sig för att vara ”OSINT”-konton har till exempel startats på digitala plattformar. I dessa konton sker dock en förment publik verksamhet som följer samma övergripande narrativ som sprids via ryska Kremltrogna nyhetskanaler som Russia Today och Sputnik News.[23] I många uttalat ukrainskvänliga konton kan det också misstänkas att analysen är vinklad för att tjäna ukrainska intressen som att bibehålla försvarsvilja och motståndskraft. Generellt kan antas att med ”OSINT:s” spridning så ökar försöken att kontrollera och manipulera det råmaterial som samlas in och analyseras – de bilder och filmer som dyker upp i det digitala flödet från krigszonen. Utöver detta finns det också en risk att den övergripande, mer strategiska förståelsen av invasionen drunknar i alla detaljer om förstörda stridsfordon, enskilda strider på Mariupols gator och var en oligarks yacht befinner sig just nu.

Sammantaget är publik så kallad OSINT-verksamhet en realitet som å ena sidan understryker vikten av att konsumenter av information förmedlad via digitala medier inte bara har, utan också ständigt utvecklar sin digitala läskunnighet och källkritik. Å andra sidan visar denna utveckling både potentialen hos ”crowd wisdom” för klassisk underrättelseverksamhet – och utmaningarna med att institutionalisera den. ■

Ivar Ekman är analytiker vid FOI:s enhet för asymmetriska hot.
Per-Erik Nilsson är forskare vid FOI:s enhet för asymmetriska hot.

21 För en diskusion om OSINT och teknikutveckling, se: Emily Harding (2022), "Move Over Jarvis, Meet Oscar: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community", Centre for Strategic & International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220119_Harding_MoveOverJARVIS_MeetOSCAR_0.pdf?NqfrbU05ULzzcySzNHB0pTzsNYw3HdfK

22 Se: Ciarán O'Connor (2022), "After Bucha, Here's What to Expect from the Next Phase of Russian Disinformation in Ukraine", *Institute for Strategic Dialogue,* 6 maj: https://www.isdglobal.org/digital_dispatches/next-phase-russian-disinformation-in-ukraine/; Stuart A. Thomson (2022), "4 Falsehoods Russians Are Told About the War", *The New York Times,* 10 mars: https://www.nytimes.com/2022/03/10/technology/disinformation-russia-ukraine.html.

23 Se: Justin Ling (2022), "Russia Is Mimicking Open-Source Intelligence Methods to Discredit Bucha Atrocities
The Kremlin is desperate to muddy the waters around its war crimes", *Foreign Policy,* 12 april: https://foreignpolicy.com/2022/04/12/russia-open-source-intelligence-bucha-atrocities/; Chris Stokel-Walker (2022), "Russia co-opts grassroots intelligence to spread propaganda", *New Statesman*, 18 mars: https://www.newstatesman.com/internet-social-media/2022/03/russia-co-opts-grassroots-intelligence-to-spread-propaganda.