PRESSMEDDELANDE

Januari 2025

INSIKTER FRÅN ATHENAS NYA STUDIE OM UTLÄNDSK INBLANDNING OCH INFORMATIONSMANIPULERING

Athena-konsortiet med 14 partner från 11 länder har svarat på initiativet European Democracy Shield. Baserat på analysen av 32 fallstudier av utländsk inblandning och informationsmanipulering (FIMI) och analysen av de taktiker, tekniker och förfaranden (TTP) som används av angripare, gav konsortiet policyrekommendationer. ny ATHENA-rapport som dokumenterar FIMI tog mer än ett år att utarbeta, har 1 400 fotnoter - en indikator på de många artiklar, tidningsartiklar, bloggar, rapporter, tal som konsulterats av partners - inklusive djupintervjuer med mer än 20 experter. Förhoppningen är att den kan bidra i den europeiska kampen mot FIMI.

Viktiga insikter

Anpassning till nya taktiker: vaksamhet mot FIMI-aktörerna

FIMI-aktörer använder ett brett utbud av TTP:er och plattformar för att undvika upptäckt och för att sprida sina budskap. Försvarare behöver ständig vaksamhet och anpassning av motåtgärder i takt med att illasinnade aktörers taktik utvecklas.

- Utbudet av fallstudier tyder på en spridning och uppfinningsrikedom av TTP:er som används av FIMI-angripare. Följaktligen är attribuering en utmaning. Vissa angripare döljer sina spår väl eller ägnar sig åt förnekelse. FIMI-analys kräver en förståelse för de olika typerna av angripare i desinformationskampanjer, deras motiv och de TTP:er de använder. ATHENA-konsortiet analyserade 32 FIMI-fall från Ryssland, Kina, Nordkorea, Turkiet, Saudiarabien, Iran och Indien och fann att Ryssland var mer engagerat i FIMI än något annat land.

Ovetande allierade till FIMI: rollen som "nyttiga idioter"

Framgången för dessa kampanjer hänger ofta på "nyttiga idioter", individer som omedvetet stöder en sakfråga eller specifik agenda – ofta politisk eller ideologisk – utan att fullt ut förstå dess konsekvense . Term"nyttiga idioter" användes för att beskriva västerländska sympatisörer till sovjetkommunismen under det kalla kriget. Termen används nu i vidare bemärkelse för att beskriva människor som i sin entusiasm eller naivitet stöder rörelser, organisationer eller regimer som i slutändan manipulerar eller utnyttjar dem.

Ökad misstro och försvagade allianser

Angriparna använder i själva verket informationskrigföringsteknik (t.ex. för att förvränga innehållet och utnyttja nyhetshändelser) för att öka misstron inom EU, försvaga de transatlantiska allianserna och främja politiker som sympatiserar med deras sak.

- Olika hotaktörer, inklusive statligt sponsrade grupper, kriminella organisationer, hacktivister och individer med onda avsikter arbetar ibland tillsammans utan några avtal eftersom det passar deras gemensamma, men inte samordnade mål. Genom att utnyttja en infrastruktur som gör det möjligt för dem att dölja sin identitet genom anonymitet, finner FIMI-angriparna i sociala nätverk en grogrund för att odla och sprida sin propaganda.

Även om FIMI ofta förknippas med val har det en mycket bredare räckvidd och fortsätter att blomstra även efter valet till Europaparlamentet den 9 juni 2024. Hotet mot demokratin kvarstår. Effektiviteten av FIMI kampanjer och effekterna av västerländska motåtgärder är fortfarande föremål för pågående analys och debatt.

Fallstudierna i Athena visade att sociala nätverk spelade en viktig roll för att sprida desinformation, ofta i kombination med förvrängning av fakta (53,3 %) och utnyttjande av befintliga narrativ (50 %). Detta skulle kunnan stödja hypotesen om de **sociala mediernas roll som en primär kanal för desinformation, som är utformad för att förvränga fakta, överväldiga användarna och förstärka vilseledande innehåll.**

Ett av de bästa försvaren mot desinformation är öppenhet, effektiv kommunikation och användning av motbudskap som utmanar desinformation som riktar sig mot Europeiska unionen. Att utvärdera olika desinformationsincidenter innebär att man måste vara självkritisk och ta förtroendeförhållandet mellan EU:s institutioner och samhällena i de olika medlemsstaterna på allvar.

EU har tagit fram olika åtgärder för att bekämpa desinformation, bland annat EU:s strategi för cybersäkerhet[1] och initiativ genom Europeiska kompetenscentrumet för motverkande av hybridhot[2].

[1] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[2] https://www.hybridcoe.fi/

Rekommendationer

- En mångfacetterad motåtgärd mot desinformation Effektiva motåtgärder mot desinformationskampanjer kräver en mångfasetterad strategi som inbegriper samarbete mellan regeringar, sociala medier, det civila samhället och allmänheten. Denna strategi som omfattar hela samhället kan dock endast uppnås på ett realistiskt sätt om de berörda parter som arbetar med att bekämpa FIMI har ett gemensamt "språk", t.ex. ramverken DISARM[3] och STIX[4], för att harmonisera övervakningen, analysen, bedömningen och reaktionen på FIMI:s verksamhet.

Regeringar och organisationer i det civila samhället bör fokusera på initiativ för medie- och informationskunnighet för att hjälpa medborgarna att kritiskt bedöma nyhetskällor och utvärdera trovärdigheten och motiven bakom informationen, t.ex. via via kampanjer. För specifika åtgärder som svar på FIMI-attacker bör både medborgare och yrkesverksamma kunna konsultera officiella källor eller rapporter från trovärdiga forskningsinstitutioner, projektkonsortier och tankesmedjor som fokuserar på desinformation och cybersäkerhet.

Främja faktagranskning: EU:s medlemsstater bör främja faktagranskning av bilder och videor för att hjälpa enskilda personer att identifiera manipulerat innehåll och andra former av digitalt bedrägeri. **Att utbilda medborgare, inklusive barn i skolåldern, om FIMI-taktik kan hjälpa dem att fungera som en första försvarslinje, vilket avsevärt minskar spridningen och effekten av desinformation.**

- Desinformationsteam för snabbinsatser Regeringar bör inrätta snabbinsatsgrupper som är utbildade för att avslöja FIMI så snart det dyker upp. Sådana grupper bör bestå av regeringstjänstemän, akademiker, civilsamhällesorganisationer och faktagranskande journalister. Regeringarna bör stärka övervakningsmekanismerna, förbättra transparensen och ha ett närmare samarbete med faktagranskande organisationer för att mildra effekterna av FIMI.

Brådskande satsningar på flerspråkiga verktyg Europeiska utrikestjänsten (EEAS), EU:s utrikestjänst, bör prioritera investeringar i flerspråkiga spårningsverktyg som kan upptäcka FIMI på olika språk. Detta skulle göra det möjligt att snabbare identifiera manipulativt innehåll i olika språkliga och regionala sammanhang

Kunskapsutbyte Kommissionen bör uppmuntra EU-finansierade projekt för att skapa nätverk och dela kunskap bland FIMI projekt i medlemsstaterna, USA, Kanada, Australien, Japan, Latinamerika och andra länder som motsätter sig utländsk informationsmanipulering och inblandning.

Mer detaljerade slutsatser och rekommendationer från fallstudierna finns i briefingdokumentet, som också finns på Athenas webbplats, där du kan läsa mer om projektet.

[3] https://disarmframework.herokuapp.com/
[4] https://oasis-open.github.io/cti-documentation/stix/intro.html

Konsortium

Kontakt

Email: athena.comms@trilateralresearch.com

Funded by the European Union (grant number 101132686). UK participants in Horizon Europe Project ATHENA are supported by UKRI grant number 10107667 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA) or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them. HORIZON-CL2-2023-DEMOCRACY-01.

D5.1:Dissemination, Communication & Exploitation Plan-v2

WP5

Report
Dissemination level: Public

Anna Pomortseva, Kristian Reeson - EOS
Selby Knudsen, Dr Richa Kumar - TRI

Funded by the European Union (grant number 101132686). UK participants in Horizon Europe Project ATHENA are supported by UKRI grant number 10107667 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA) or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them. Grant Agreement 101132686ATHENA HORIZON-CL2-2023-DEMOCRACY-01