PRESSEMITTEILUNG

Februar 2025

ERKENNTNISSE AUS DER WEGWEISENDEN STUDIE VON ATHENA ÜBER DIE MANIPULATION UND EINMISCHUNG AUSLÄNDISCHER INFORMATIONEN

Das ATHENA-Konsortium mit14 Partnern aus 11 Ländern hat sich auf die Initiative "Europäischer Demokratieschild" beworben. Basierend auf der Analyse von 32 Fallstudien zur “Manipulation und Einmischung in ausländische Informationen” (FIMI) und der Analyse der von Angreifern verwendeten Taktiken, Techniken und Verfahren (TTPs) erarbeitete das Konsortium politische Empfehlungen. Der ATHENA-Bericht über die Manifestationen der FIMI wurde mehr als ein Jahr lang ausgearbeitet und enthält 1.400 Fußnoten - ein Indikator für die zahlreichen Artikel, Zeitungsberichte, Blogs, Berichte und Reden, die von den Partnern konsultiert wurden - einschließlich ausführlicher Interviews mit mehr als 20 Experten, die originelle Beiträge zum europäischen Kampf gegen die FIMI geleistet haben.

Wichtige Erkenntnisse

Anpassung an die sich entwickelnden Taktiken: Wachsamkeit gegenüber den FMI-Akteuren

FIMI-Akteure nutzen eine breite Palette von TTPs und Plattformen, um sich der Entdeckung zu entziehen und ihre Botschaften zu verbreiten. Verteidiger müssen ständig wachsam sein und Gegenmaßnahmen anpassen, da sich die Taktiken böswilliger Akteure weiterentwickeln.

- Die Bandbreite der Fallstudien deutet auf eine Ausweitung und Innovation der TTPs hin, die von FIMI-Angreifern eingesetzt werden. Folglich ist die Attribution eine Herausforderung. Einige Angreifer sind gut darin ihre Spuren zu verwischen oder streiten ihre Beteiligung an den Angriffen ab. Die FIMI-Analyse erfordert ein Verständnis der verschiedenen Arten von Angreifern in Desinformationskampagnen, ihrer Motivationen und der von ihnen verwendeten TTPs. Das ATHENA-Konsortium analysierte FIMI-Fälle aus Russland, China, Nordkorea, der Türkei, Saudi-Arabien, dem Iran und Indien und stellte fest, dass Russland mehr als jedes andere Land FIMI betreibt.

Unwissentliche Verbündete von FIMI: Die Rolle der "nützlichen Idioten"

Der Erfolg dieser Kampagnen hängt oft von sogenannten "nützlichen Idioten" ab, also von Individuen, die unwissentlich eine Sache oder Agenda unterstützen – oft politisch oder ideologisch –, ohne ihre Auswirkungen vollständig zu verstehen, insbesondere wenn diese Sache manipulativ oder schädlich ist. Der Ausdruck wurde während des Kalten Krieges verwendet, um westliche Sympathisanten des Sowjetkommunismus zu beschreiben. In der Forschung wird der Begriff heutzutage weiter gefasst, um Menschen zu beschreiben, die in ihrem Enthusiasmus oder ihrer Naivität Bewegungen, Organisationen oder Regime unterstützen, die sie letztlich manipulieren oder ausbeuten.

Misstrauen verstärken und Bündnisse schwächen

Angreifer setzen Techniken der Informationskriegsführung (z. B. Inhaltsverzerrung und das Ausnutzen von Eilmeldungen) ein, um das Misstrauen innerhalb der EU zu verstärken, transatlantische Bündnisse zu schwächen und Politiker zu fördern, die mit ihren Anliegen sympathisieren.

- Verschiedene Bedrohungsakteure, darunter staatlich geförderte Gruppen, kriminelle Organisationen, sog. Hacktivisten und Einzelpersonen mit böswilligen Absichten, arbeiten manchmal ohne Vereinbarungen zusammen, weil es ihren gemeinsamen, aber unkoordinierten Zielen entspricht. Die FIMI-Angreifer finden in den sozialen Netzwerken einen fruchtbaren Boden, um ihre Propaganda zu kultivieren und zu verbreiten. Sie nutzen die dortige Infrastruktur aus, die es ihnen ermöglicht, ihre Identität durch Anonymität zu verbergen.

Obwohl FIMI häufig mit Wahlen in Verbindung gebracht wird, hat sie eine viel größere Reichweite und floriert auch nach den Wahlen zum Europäischen Parlament (EP) am 9. Juni 2024 weiter. Die demokratische Gesellschaft ist nach wie vor zunehmend bedroht. Die tatsächliche Wirkung einer FIMI-Kampagne ist ungewiss. Die Wirksamkeit und die Auswirkungen westlicher Gegenmaßnahmen sind nach wie vor Gegenstand laufender Analysen und Debatten.

Die ATHENA-Fallstudien zeigten, dass soziale Netzwerke eine Schlüsselrolle bei der Verbreitung von Desinformationen spielten, häufig gepaart mit der Verzerrung von Fakten (53,3 %) und dem Verstärken bestehender Narrative (50 %). Dies stärkt die Rolle der sozialen Medien als primärer Kanal für Desinformation, die darauf abzielt, Fakten zu verzerren, Nutzer zu überfordern und irreführende Inhalte zu verstärken.

Zu den besten Abwehrmaßnahmen gehören Transparenz, wirksame Kommunikation und der Einsatz von Gegennarrativen, die Desinformation gegen die Europäische Union in Frage stellen. Die Bewertung verschiedener Desinformationskampagnen setzt voraus, selbstkritisch zu sein und das Vertrauensverhältnis zwischen den europäischen Institutionen und den Gesellschaften in den verschiedenen Mitgliedstaaten ernst zu nehmen.

Die EU hat verschiedene Maßnahmen zur Bekämpfung von Desinformation entwickelt, darunter die EU-Cybersicherheitsstrategie[1] und Initiativen des Europäischen Exzellenzzentrums für die Abwehr hybrider Bedrohungen[2].

---

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

Empfehlungen

Eine vielschichtige Gegenmaßnahme gegen Desinformation Wirksame Gegenmaßnahmen gegen Desinformationskampagnen erfordern einen vielschichtigen Ansatz, der die Zusammenarbeit zwischen Regierungen, sozialen Medien, der Zivilgesellschaft und der Öffentlichkeit umfasst. Dieser gesamtgesellschaftliche Ansatz kann jedoch nur dann realistisch erreicht werden, wenn die Akteure, die sich mit der Bekämpfung der FIMI befassen, eine gemeinsame "Sprache" wie die Rahmenwerke DISARM[3] und STIX[4] zur Harmonisierung der Überwachung, Analyse, Bewertung und Reaktion auf FIMI-Operationen sprechen.

Aufbau einer kritischen Bürgerschaft :
Regierungen und zivilgesellschaftliche Organisationen (CSOs) sollten sich auf Initiativen zur Förderung der Medienkompetenz konzentrieren, um den Bürgern zu helfen, Nachrichtenquellen kritisch zu bewerten und die Glaubwürdigkeit und die Motive hinter den Informationen zu bewerten. Individuen sollten ermutigt werden, Informationen in öffentlichen Kampagnen zu hinterfragen. Für spezifische Maßnahmen, die als Reaktion auf FIMI-Angriffe ergriffen werden können, sollten Bürger und Praktiker gleichermaßen in der Lage sein, offizielle Quellen oder Berichte von glaubwürdigen Forschungseinrichtungen, Projektkonsortien und Denkfabriken zu konsultieren, die sich auf Desinformation und Cybersicherheit konzentrieren.

Förderung der Faktenprüfung Die EU-Mitgliedstaaten sollten die Fähigkeit zur Faktenprüfung von Bildern und Videos fördern, um Einzelpersonen dabei zu helfen, manipulierte Inhalte und andere Formen der digitalen Täuschung zu erkennen. Die Aufklärung der Bürger, einschließlich Kinder im schulpflichtigen Alter, über FIMI-Taktiken kann helfen, als erste Verteidigungslinie zu fungieren und die Verbreitung und Wirkung von Falschinformationen erheblich zu reduzieren.

- Schnelles Desinformationsteam Regierungen sollten schnelle Eingreifteams einrichten, die geschult darin sind FIMI zu entlarven, sobald sie auftaucht. Diese Teams sollten sich aus Regierungsbeamten, Akademikern, zivilgesellschaftlichen Organisationen und Journalisten zusammensetzen. Die Regierungen sollten die Überwachungsmechanismen stärken, die Transparenz verbessern und enger mit den Organisationen für Faktenprüfung zusammenarbeiten, um die Auswirkungen der FIMI abzumildern.

Dringende Investitionen in mehrsprachige
Programme Der Europäische Auswärtige Dienst (EAD), das Auswärtige Amt der EU, sollte Investitionen in mehrsprachige Nachverfolgungsprogramme, mit denen FIMI in verschiedenen Sprachen erkannt werden kann, Vorrang einräumen. Dies würde eine schnellere Identifizierung manipulativer Inhalte in verschiedenen sprachlichen und regionalen Kontexten ermöglichen.

Weitergabe von Erkenntnissen
Die Europäische Kommission sollte EU-finanzierte Projekte, die sich mit FIMI befassen, dazu ermutigen, sich mit anderen ähnlichen Projekten in den Mitgliedstaaten, den USA, Kanada, Australien, Japan, Lateinamerika und anderen Ländern, zu vernetzen und Wissen auszutauschen.

Die detaillierteren Schlussfolgerungen und Empfehlungen aus den Fallstudien finden Sie im **Briefing-Papier**, das auch auf der **ATHENA-Website** abgerufen werden kann.

[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.