Northwestern
BUFFETT INSTITUTE FOR GLOBAL AFFAIRS
McCORMICK SCHOOL OF ENGINEERING
Security & AI Lab

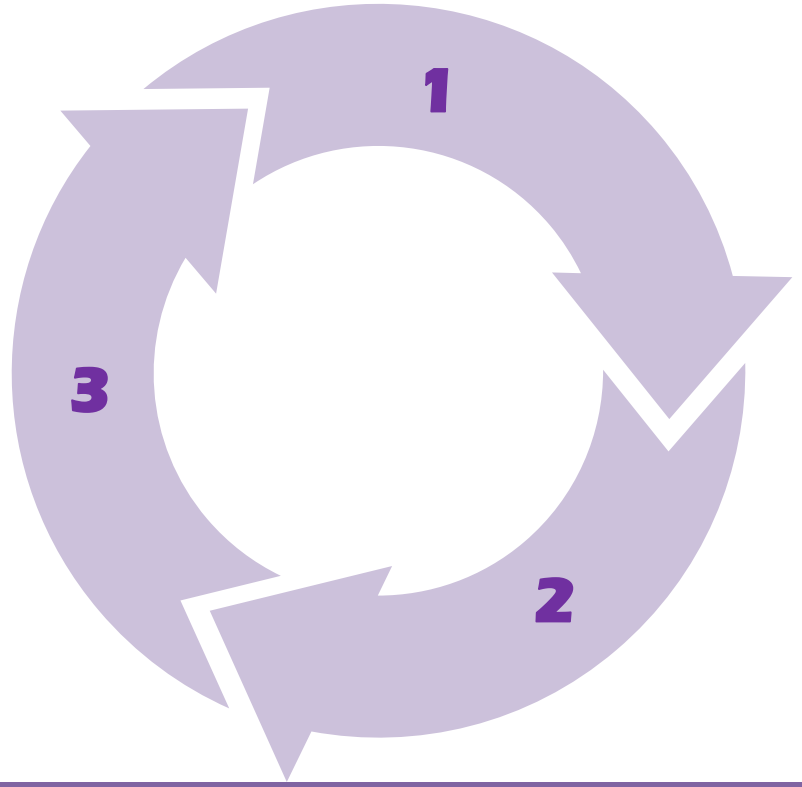
Cyber-Geospatial Convergence: Shielding Digital Borders

V.S. Subrahmanian
Northwestern University
vss@northwestern.edu

Joint work with many colleagues, postdocs, and students

GWF May 1 2026

The Malware Variant Cycle Today



Hacker releases new malware (or variant)

Anti-virus companies detect & block malware

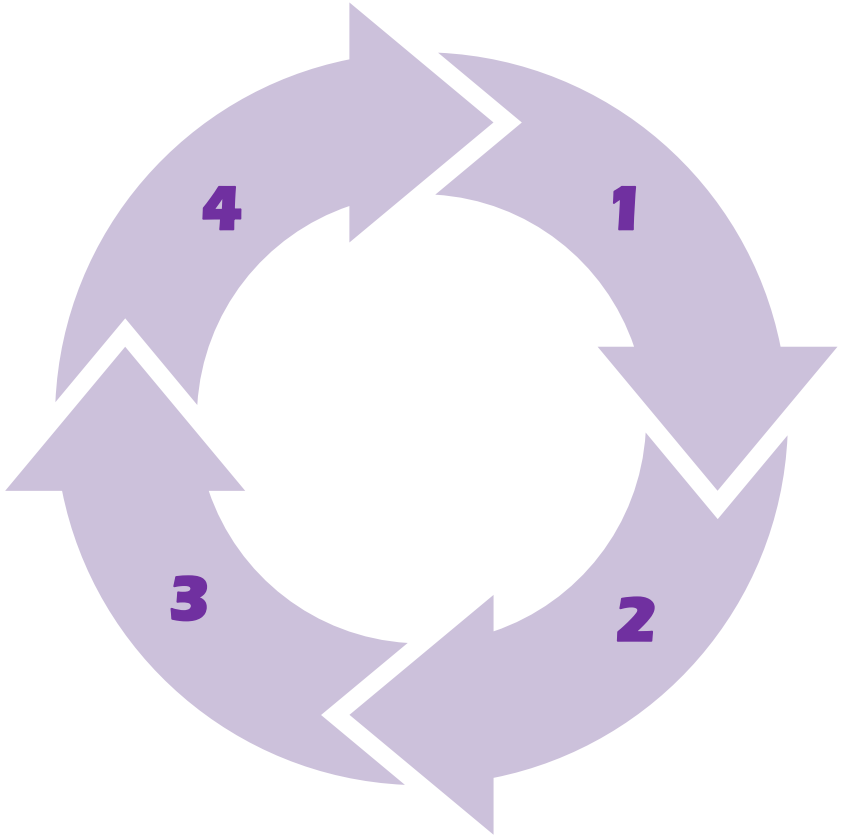
Hacker sees a drop in revenues

This cycle keeps anti-virus companies in business as new malware emerges all the time. We propose a new model called GLAMP.

S. Kumar, C. Molinaro, L. Sola and V. S. Subrahmanian, "GLAMP: Generative Learning for Adversarially-Robust Malware Prediction," *IEEE Transactions on Emerging Topics in Computing*, vol. 13, no. 3, pp. 1299-1315, July-Sept. 2025, doi: 10.1109/TETC.2025.3583872.

The Malware Variant Cycle Tomorrow

1. Hacker releases new malware (or variant)
2. Anti-virus companies generate lots of variants of the malware & train ML models on this much larger sample
3. Anti-virus companies detect & block malware
4. Hacker sees a drop in revenues



- Our new GLAMP model generates lots of variants of a known malware.
- Machine learning algorithms then learn not only from the malware they have seen, but also from many variants of it.
- The resulting ML detectors will make it much harder for malicious hackers to evade detection in the future.

Generation: Evasion Rate of GLAMP-Generated Malware Against 4 Well Known Anti-Virus Tools

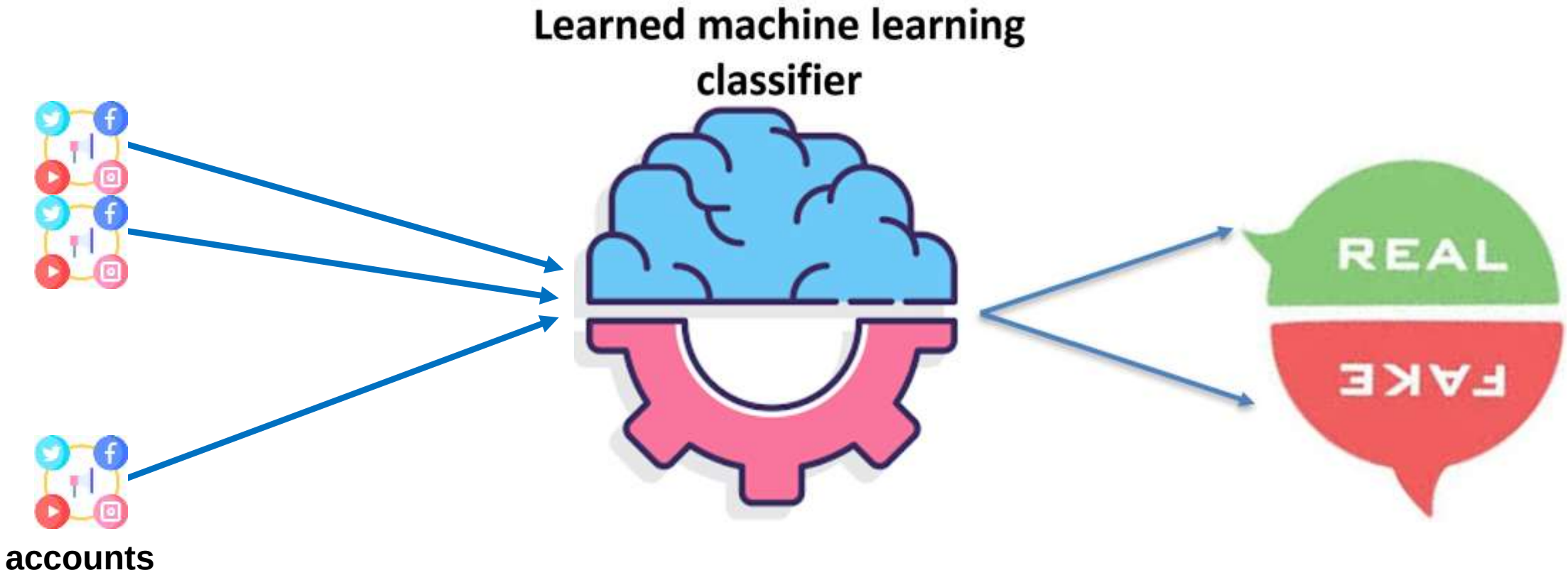
Antivirus	Separate Optimization		Combined Optimization	
	SVM	**DT**	**SVM**	**DT**
AV-1	7.11	10.38	79.35	**82.80**
AV-2	7.11	10.38	79.35	**82.80**
AV-3	7.11	10.38	79.35	**82.80**
AV-4	3.13	3.4	75.37	**79.03**

Controlled by Defender

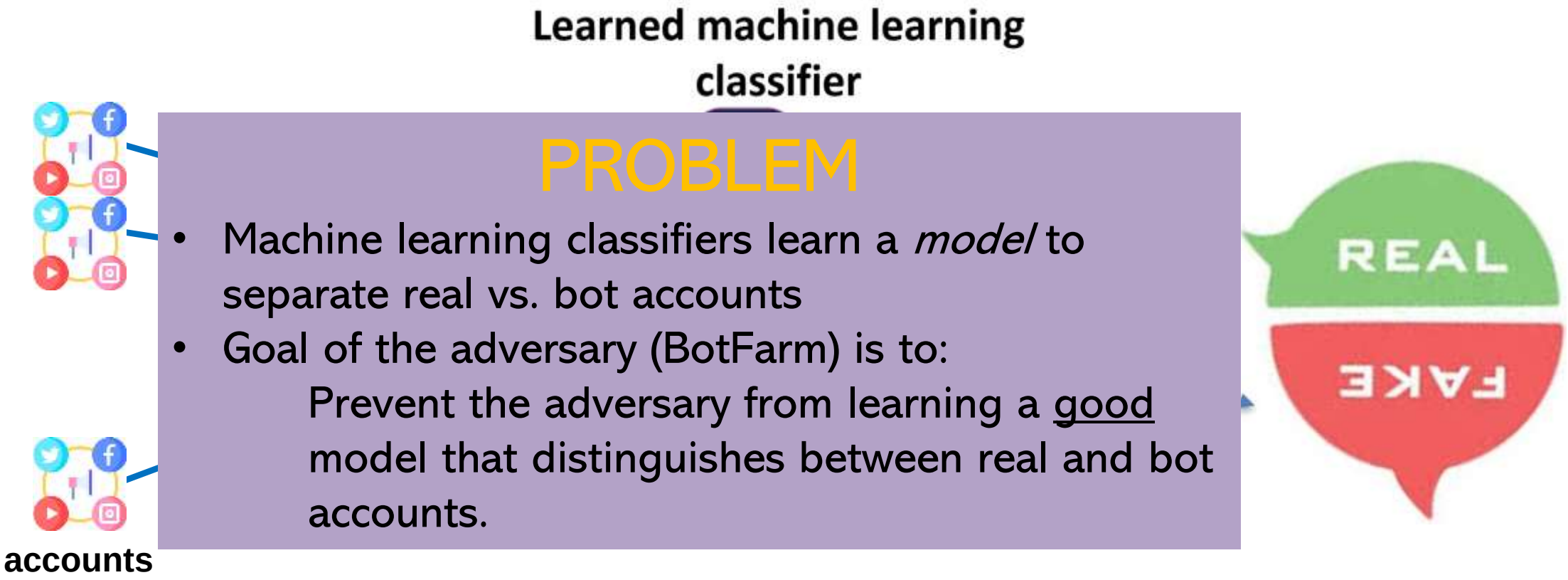
Controlled by Attacker

Augmenting training data with GLAMP-generated malware improves the performance of detectors by 2-20%.

BOT DETECTION TODAY



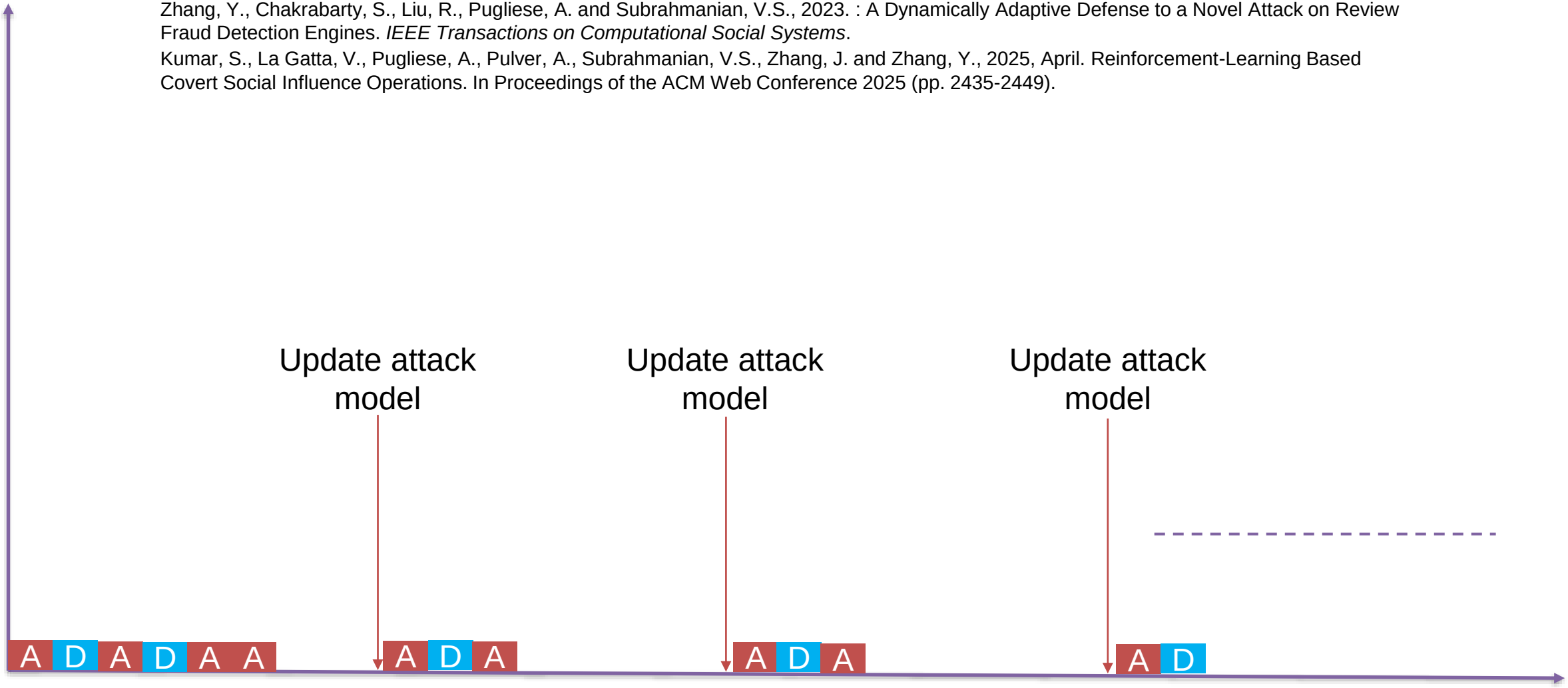
BOT DETECTION TODAY



SMART ATTACKER'S MODUS OPERANDI

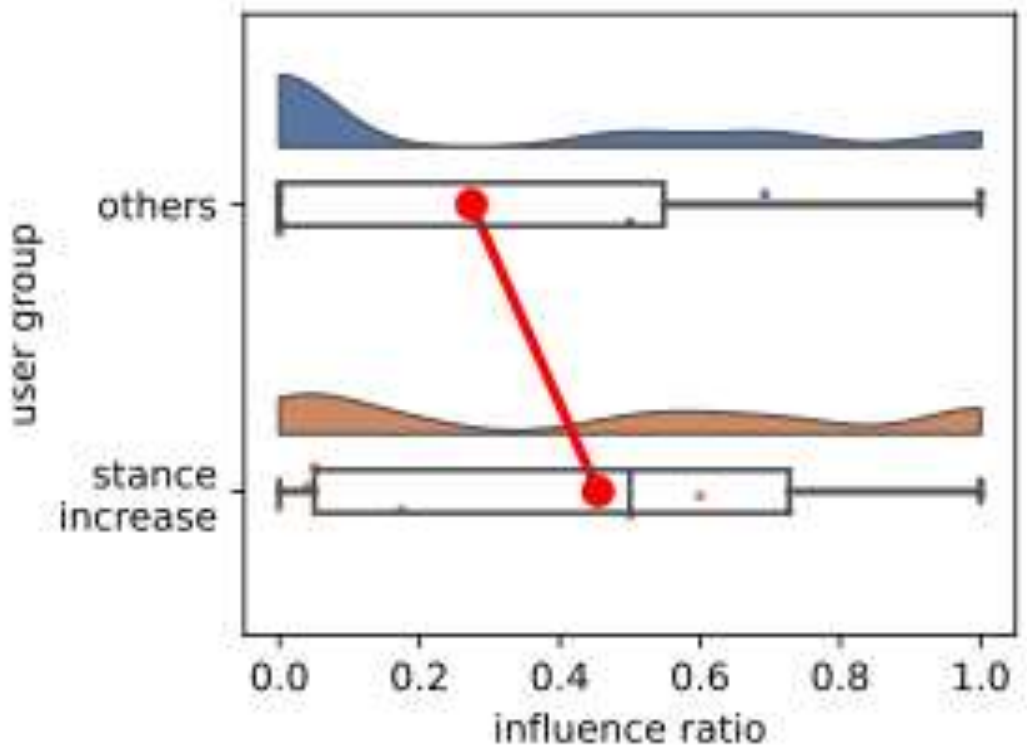
Zhang, Y., Chakrabarty, S., Liu, R., Pugliese, A. and Subrahmanian, V.S., 2023. : A Dynamically Adaptive Defense to a Novel Attack on Review Fraud Detection Engines. *IEEE Transactions on Computational Social Systems*.

Kumar, S., La Gatta, V., Pugliese, A., Pulver, A., Subrahmanian, V.S., Zhang, J. and Zhang, Y., 2025, April. Reinforcement-Learning Based Covert Social Influence Operations. In Proceedings of the ACM Web Conference 2025 (pp. 2435-2449).



Bots vs Humans: Stance Change

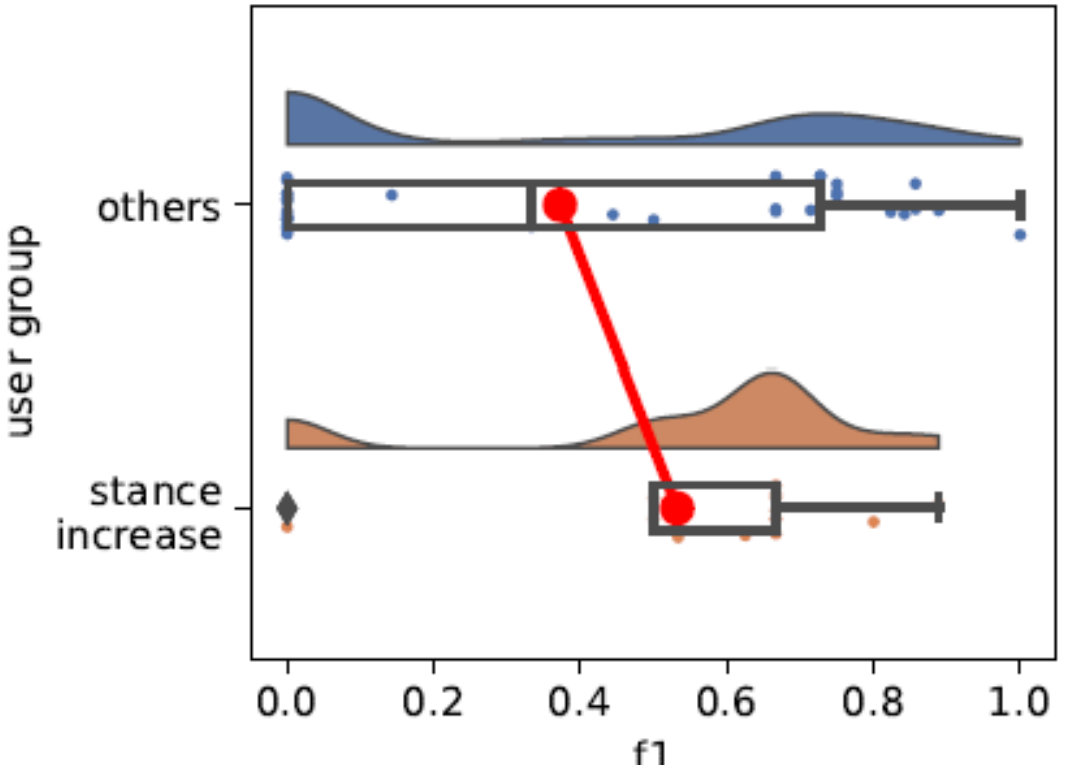
Humans are more likely to change stance when interacting with bots.



- **Influence Ratio of User *u*** Ratio of # of bots reported as being influential by user *u* vs. total # of accounts reported as influential by the user.
- **Observations**
  - Humans that increased their stance have a higher influence ratio, i.e. were more likely to have been influenced by *bots* !
  - **Takeaway: Bots can effectively drive humans towards the ideas they are pushing.**

Bots vs Humans: Perception of Being a Bot vs. Influence

Being perceived as a bot does not hinder the ability to influence others



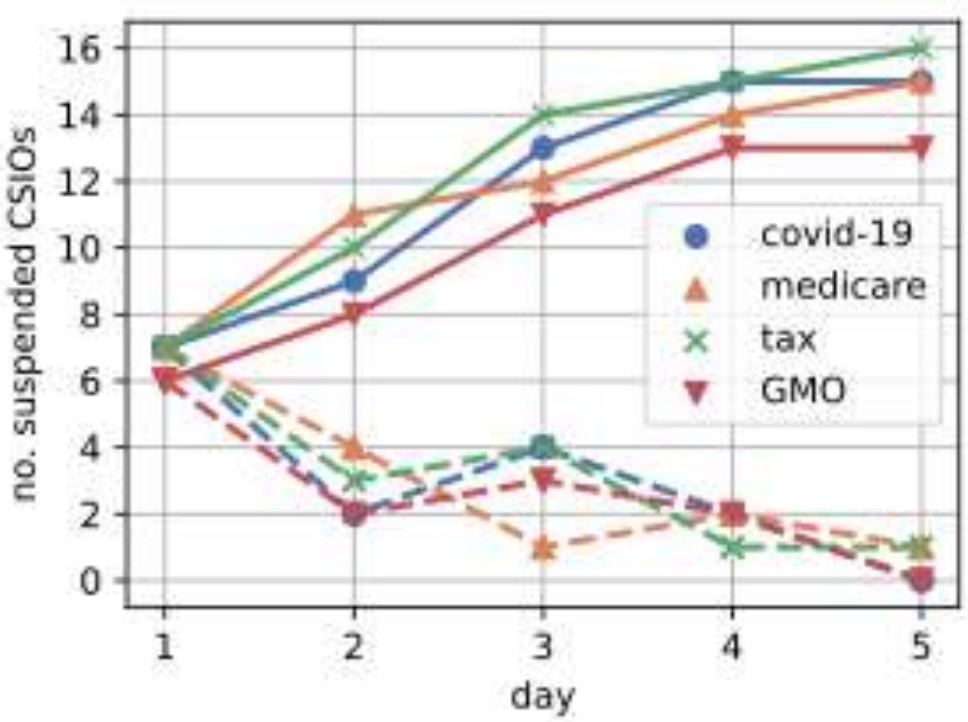
- **Comparison** Compared two populations:
  - P1: Those who increased their stance toward topic *sub*
  - P2: Those who did not.

- **Observations**
  - Humans who increased their stance toward the direction of the CSIO campaign (pop. P1) were better (F1 = 0.685 on average) at detecting RL_CSIO bots than those in population P2 (F1 =- 0.384, on average).

Takeaway: RL_CSIO bots are able to shift humans' opinion in a given direction, even if they are perceived as bots by humans.

Bots vs Humans: Automated Discoverability

Bots adapt their strategies to avoid detection during a CSIO campaign



- **Observations**
  - On all topics, there is a decreasing trend in terms of detectability, suggesting that bots are learning to evade.
  - At the end of the campaign, 16,15,15,13 accounts were suspended in the 4 campaigns.
  - None of the CSIO campaigns had all 20 bots blocked.
  - Black Box Bot detector performance: 0.449 precision, 0.662 recall, 0.535 F1. *Much lower than numbers reported against passive bots.*

  - **Takeaway: RL_CSIO bots are able to effectively evade detection during their CSIO campaign, i.e., as they run their bot campaign, they learn how to evade detection.**

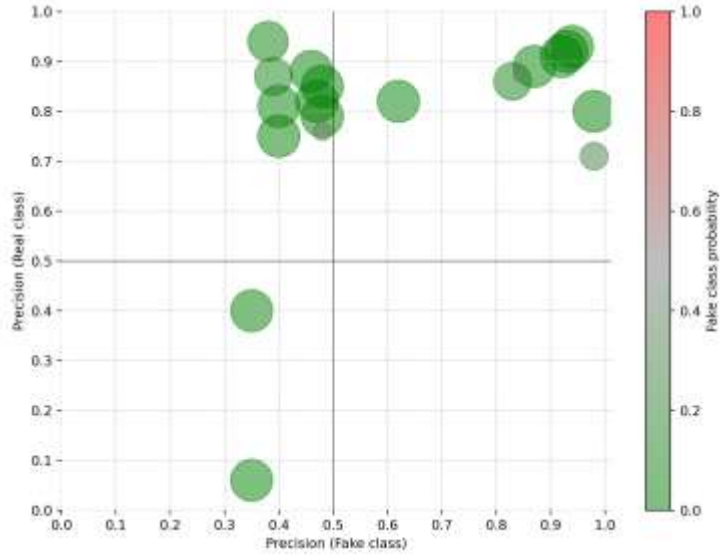
NICOLAS MADURO, I

Transcript

Hola.
Cómo estás, Elvis? Buenas noches. Cómo estás?
Me dicen que ya están actualizando.
Buenas noches, Presidente.
Sí, Hemos recibido aproximadamente al 45% de las actas a esta hora. Qué bueno. Pero dime.
Cómo ves el panorama Estado Presidente? Eh? Está negativo. Un 30%. Abajo. Vamos.
Pero cuéntame en lo que falta todavía por transmitir.
Hay chance de revertir esa tendencia?
No, mi presidente es matemáticamente imposible. Debemos dar.
Debemos pasar a la acción. Conmigo? Qué vaina!
Pues no queda de otra.
Me paraliza ya la totalización.
Que no le entreguen más actas a los testigos. Estás escuchando?
Pero, Presidente, ya muchos testigos han recibido sus actas ya en redes sociales.
Ya he visto varios videos y leyendo resultados.
Tranquilo que ya hablamos con el alto mando que hablamos con Vladimir.
Te voy a pasar los resultados que vas a leer.
Con el 80% de actas escrutadas.
Nicolás Maduro 5.150.092 votos.
Edmundo González 4.445.978 votos.
Esos son los que vas a leer el tendido presidente.
Ya Jorge Rodríguez me había indicado los mismos nombres.
Estamos en la.
En el mismo, mismo plano.
Estamos en contacto.
Ahora me tengo que ir AA1 encargo.
Es la responsabilidad máxima histórica.
La revolución está en tus manos.

English translation (machine-generated)

Hello.
How are you, Elvis? Good evening. How are you?
They tell me the updating is already underway.
Good evening, President.
Yes, we have received approximately 45% of the tally sheets at this hour.
That's good. But tell me,
what's the outlook, Mr. President? Huh?
It's negative. 30% down. Let's go.
But tell me, in what's still left to be transmitted—
is there a chance to reverse that trend?
No, Mr. President, it's mathematically impossible. We must act.
We must take action. With me? What a mess!
Well, there's no other choice.
Halt the totalization right now.
Don't give any more tally sheets to the witnesses. Are you listening?
But, President, many witnesses have already received their tally sheets—
they're already on social media.
I've already seen several videos and read results.
Don't worry, we've already spoken with the high command, we spoke with Vladimir.
I'm going to send you the results that you're going to read.
With 80% of tally sheets counted:
Nicolás Maduro – 5,150,092 votes.
Edmundo González – 4,445,978 votes.
Those are the results you're going to read aloud, Mr. President.
Jorge Rodríguez had already given me those same numbers.
We're on the—
on the same page.
We're in contact.
Now I have to go. I have something to take care of.
It's the highest historical responsibility.
The revolution is in your hands. Over and out.



vss@northwestern.edu

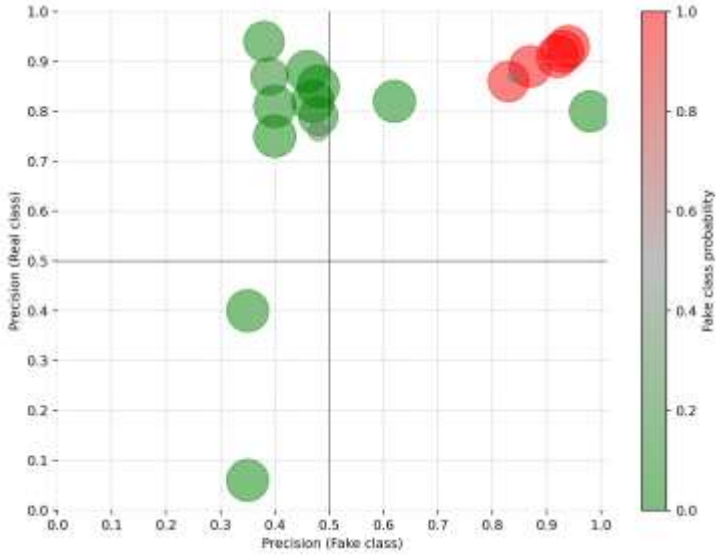
NICOLAS MADURO, II

Transcript

Hola.
Cómo estás, Elvis? Buenas noches. Cómo estás?
Me dicen que ya están actualizando.
Buenas noches, Presidente.
Sí, Hemos recibido aproximadamente al 45% de las actas a esta hora. Qué bueno. Pero dime.
Cómo ves el panorama Estado Presidente? Eh? Está negativo. Un 30%. Abajo. Vamos.
Pero cuéntame en lo que falta todavía por transmitir.
Hay chance de revertir esa tendencia?
No, mi presidente es matemáticamente imposible. Debemos dar.
Debemos pasar a la acción. Conmigo? Qué vaina!
Pues no queda de otra.
Me paraliza ya la totalización.
Que no le entreguen más actas a los testigos. Estás escuchando?
Pero, Presidente, ya muchos testigos han recibido sus actas ya en redes sociales.
Ya he visto varios videos y leyendo resultados.
Tranquilo que ya hablamos con el alto mando que hablamos con Vladimir.
Te voy a pasar los resultados que vas a leer.
Con el 80% de actas escrutadas.
Nicolás Maduro 5.150.092 votos.
Edmundo González 4.445.978 votos.
Esos son los que vas a leer el tendido presidente.
Ya Jorge Rodríguez me había indicado los mismos nombres.
Estamos en la.
En el mismo, mismo plano.
Estamos en contacto.
Ahora me tengo que ir AA1 encargo.
Es la responsabilidad máxima histórica.
La revolución está en tus manos.

English translation (machine-generated)

Hello.
How are you, Elvis? Good evening. How are you?
They tell me the updating is already underway.
Good evening, President.
Yes, we have received approximately 45% of the tally sheets at this hour.
That's good. But tell me,
what's the outlook, Mr. President? Huh?
It's negative. 30% down. Let's go.
But tell me, in what's still left to be transmitted—
is there a chance to reverse that trend?
No, Mr. President, it's mathematically impossible. We must act.
We must take action. With me? What a mess!
Well, there's no other choice.
Halt the totalization right now.
Don't give any more tally sheets to the witnesses. Are you listening?
But, President, many witnesses have already received their tally sheets—
they're already on social media.
I've already seen several videos and read results.
Don't worry, we've already spoken with the high command, we spoke with Vladimir.
I'm going to send you the results that you're going to read.
With 80% of tally sheets counted:
Nicolás Maduro – 5,150,092 votes.
Edmundo González – 4,445,978 votes.
Those are the results you're going to read aloud, Mr. President.
Jorge Rodríguez had already given me those same numbers.
We're on the—
on the same page.
We're in contact.
Now I have to go. I have something to take care of.
It's the highest historical responsibility.
The revolution is in your hands. Over and out.



vss@northwestern.edu

DEEPFAKES ARE ALREADY SHAPING OPINIONS AROUND CONFLICTS

foreignpolicy.com/2026/03/17/deepfakes-iran-trump-videos-war-tiktok/?utm_content=gifting&tpcc=gifti

FP Latest | Regions | Newsletters | FP Live

ANALYSIS

Deepfakes Are Already Shaping Opinions Around Conflicts

Governments and companies must do more to detect and debunk them.

By Daniel Byman, a professor in Georgetown University's School of Foreign Service, and V.S. Subrahmanian, the Walter P. Murphy professor of computer science and director of the Northwestern Security & AI Lab.

V.S. Subrahmanian

Walter P. Murphy Professor of Computer Science

Buffett Faculty Fellow – Buffett Institute of Global Affairs
Northwestern University

1800 Sherman Ave, Suite 3-000
Evanston, IL 60201

vss@northwestern.edu

https://vssubrah.github.io/
NSAIL Webpage: https://sites.northwestern.edu/nsail/