ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE INFORMATION DOMAIN

Issue 03/24 (March)

Astroturfing

INTRODUCTION

1. Astroturfing broadly refers to the attempt to create an impression of widespread grassroots support for a policy, individual, product, cause or idea where such support did not exist previously. The phrase was coined in 1985 by then US Senator Lloyd Bentsen, who described efforts by local companies to build support as "the difference between grassroots and astroturf". It has since evolved from describing domestic US politics to commercial advertising, and most importantly to state-based entities carrying out information operations. Astroturfing can be used as a tool to spread disinformation. According to the LSU Law Journal for Social Justice & Policy, astroturfing consists of mimicking real individuals and sparking real debates about a certain topic with the main purpose of influencing real individuals to join the false movement.

2. We have seen a new rise in astroturfing in recent years. This is due to a proliferation of automated bots, as well as refinements to existing methods allowing practitioners to avoid being detected. Recent studies, as well as experiences with real world information campaigns, have highlighted how such "coordinated inauthentic behaviour" (CIB) exploits vulnerabilities differently compared to other forms of information warfare.

KEY CHARACTERISTICS OF ASTROTURFING

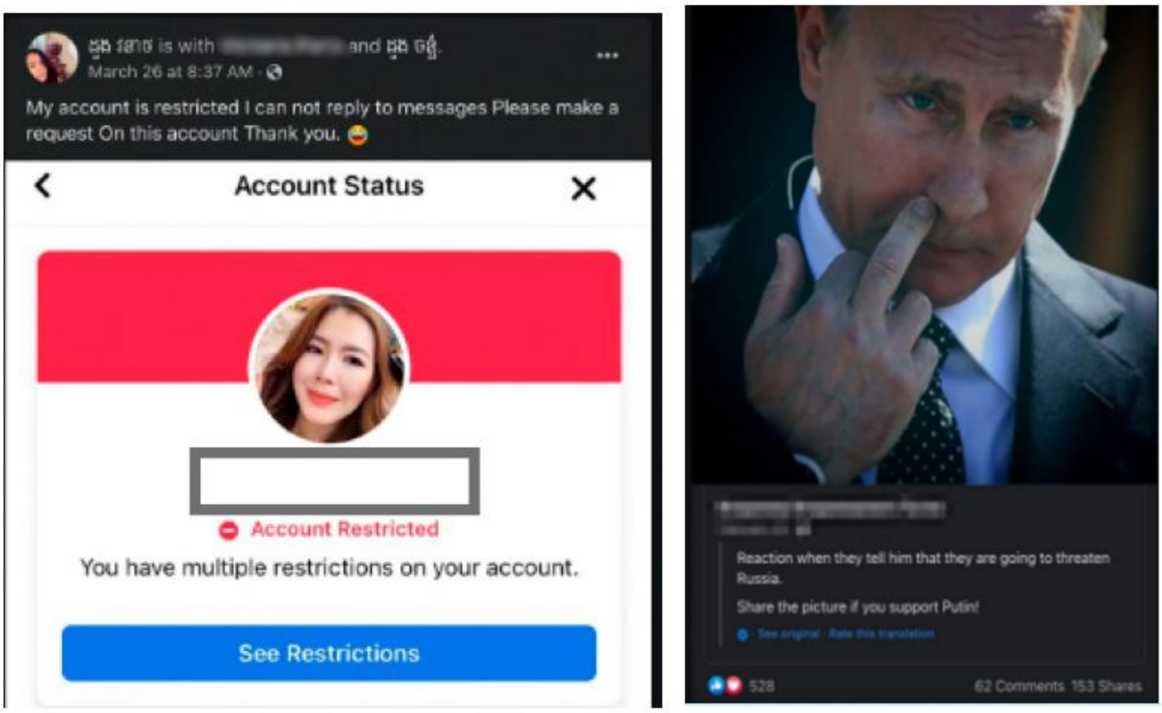
Threats to Public Discourse

3. Astroturfing is capable of eroding trust in genuine grassroots voices and government legitimacy, exacerbate political polarisation as well as undermine national unity. By subverting genuine ground sentiments, coercing support from local accounts/influencers, and creating an atmosphere of supposed consensus around a specific narrative, malicious actors can influence public opinion within a country. An example is the successful information campaigns carried out by the Russian-state supported Internet Research Agency (IRA), run by Russian oligarch Yevgeny Prigozhin. The IRA conducted "sweeping and

sustained social influence operation[s] consisting of various coordinated disinformation tactics… designed to exert political influence and exacerbate social divisions" from 2013 to 2023, when it was shut down by Russian authorities following Prigozhin's fall from grace. In the US specifically, the IRA sought to create and reinforce existing political divisions across a slew of targeted communities across the entire political spectrum. Their activities resulted in a US grand jury indicting the IRA for violating criminal laws with the intent to interfere, as the US Department of Justice put it, "with US elections and political processes".

4. The IRA's activities represent only a sliver of the astroturfing campaign carried out by Russian state entities. In the wake of Russia's military actions in Ukraine in 2022, pro-Putin and pro-Kremlin pages began content production to portray Putin as an "ethical leader" and a hero for standing up to Western aggression. The campaign consisted of largely single or double account users posting in English, Russian, Farsi, Arabic and Khmer, and achieved significant success when spreading content in large groups. For example, the Khmer language Facebook group "Duong Vanath" with ~27,000 members were found to be a strong pro-Putin support group with administrator accounts operated by a network of pro-Kremlin users. These users had been on the platform for years with limited activity, but ramped up content production and posting among grassroots during the Russian invasion of Ukraine.

Figure 1: Astroturfing accounts and posts amplifying pro-Putin narratives



[illegible] is with [redacted] and [illegible].
March 26 at 8:37 AM ·

My account is restricted I can not reply to messages Please make a request On this account Thank you. 😂

Account Status

[redacted]

Account Restricted

You have multiple restrictions on your account.

[redacted]

Reaction when they tell him that they are going to threaten Russia.

Share the picture if you support Putin!

Source: Ayad (2022). The Vladimirror Network: Pro-Putin Power-Users on Facebook, p.7.

Challenges in Detection

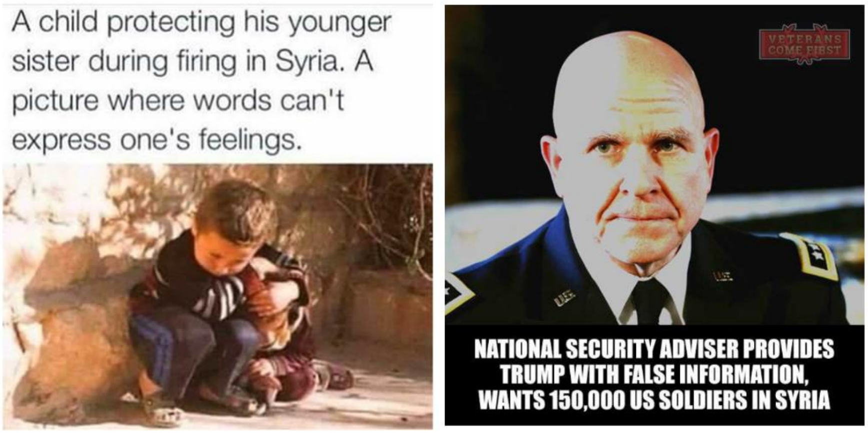
5. Automated account detection is still often flawed. In one 2018 study, bot detection algorithm classified almost half of the members in the US Congress as bots. While automated accounts and duplicate accounts violate many social media companies' guidelines, in reality many practitioners continue to operate as administrators, moderators and contributors with multiple accounts, operating freely due to the difficulties in detection. Skilled actors would also ensure that their accounts have a veneer of authenticity. For example, the identified administrator accounts in "Duong Vanath" also controlled two other pages not related to Putin in any form.

6. According to the LSU Law Journal for Social Justice & Policy, ideas spread by astroturfing are not necessarily false or inaccurate. Rather, they birth a discussion that is purely false and orchestrated. With this in mind, astroturfing, unlike other forms of CIBs, is often not picked up by the typical counter-disinformation efforts. Astroturfing campaigns often avoid detection as they do not engage in "explicit" illegitimate activities. Rather, they carry out innocuous activities such as reposting key posts, posting the same messages within a short span of time, or similar activities. For instance, IRA activities in the US often reinforced existing in-group camaraderie, with partisan content and demonisation of out-groups commonly observed.

Microtargeting Specific Groups

7. Astroturfing has also enabled state entities to micro-target specific groups with the customisation of narratives specific to them. This has allowed such actors to propagate consistent narratives despite disparate and ideologically diverse audiences. For example, Russian propaganda regarding their intervention in Syria against the Islamic State (IS) targeted Western audiences with a left-leaning stance with content expressing anti-war sentiments with objections to the US' involvement overseas. Pages fronted by the IRA like Instagram page @feminism_tag focused on the human element and suggested that the cause of suffering was coalition air strikes by the US. To right-leaning audiences, Russian pages suggested that US opposition to Syrian President Bashar Al-Assad was misplaced, and blamed then-President Barack Obama's belligerent attitude. When then-President Trump took office, these pages started hinting at established right-wing conspiracies such as Republican collusion with the "deep state".

Figure 2: Posts by Russian accounts, focusing on left-wing and right-wing audiences


A child protecting his younger sister during firing in Syria. A picture where words can't express one's feelings.
VETERANS COME FIRST
NATIONAL SECURITY ADVISER PROVIDES TRUMP WITH FALSE INFORMATION, WANTS 150,000 US SOLDIERS IN SYRIA

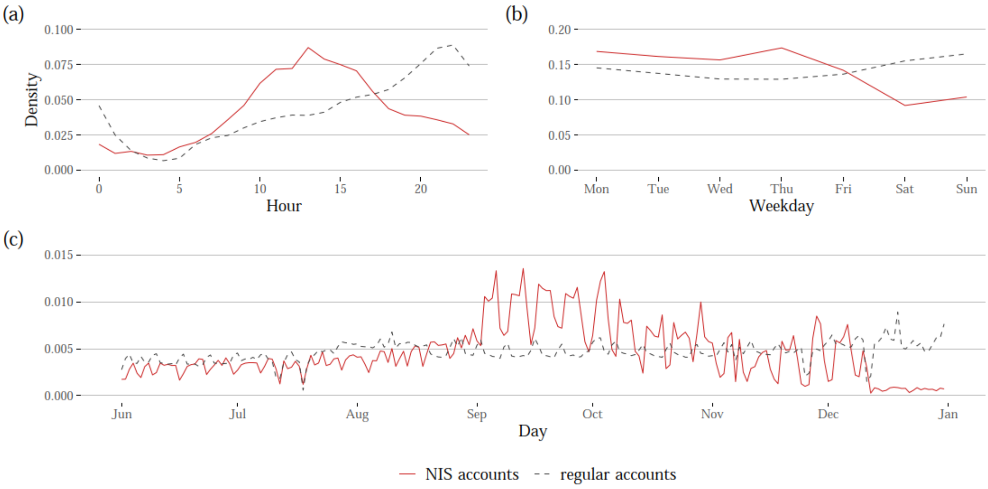
Source: @feminism_tag (left) Veterans Come First (right), taken from DiResta, Shaffer, Ruppel, Sullivan, Matney, Fox, Albright, Johnson (2022). The Tactics and Tropes of the Internet Research Agency, p.59 and p.61.

IMPLICATIONS

Identifying Astroturfing by Coordination Patterns

8. While most practitioners attempt detection by looking at suspicious activity patterns of individual accounts, astroturfing detection attempts are better served by detecting coordinated activity among groups of accounts. In a 2022 study, researchers examined the South Korean tweets in the 2012 Presidential Elections, and were able to identify the South Korean National Intelligence Service's (NIS) attempts to conduct an astroturfing campaign via examining tweets' temporal patterns. The Guardian reported that NIS had formally acknowledged in 2017 in a publicly released report of its involvement in election manipulation in the 2012 South Korean presidential elections to help the campaign of the then-incumbent South Korean President Park Geun-hye. The 2022 research study showed that NIS accounts had specific posting patterns at the hour, day and monthly interval. These patterns matched the office hours of the average South Korean white-collar worker, whose real posting patterns were heavily weighted to after office hours instead.

Figure 3: Comparison between NIS and regular South Korean account posting patterns



Source: Keller, Schoch, Stier, Yang (2022). Political astroturfing across the world, p.8.

"Benign" Astroturfing?

9. While state-based astroturfing is often described in a negative light, its principles may be useful for more benign uses, such as in countering extremist narratives. The US has implemented a programme known as Operation Earnest Voice (OEV) since 2011. Under OEV, the US Central Command had contracted web security company Ntrepid to develop a "sock puppet" – false online identities used for deceptive purposes – as an operating platform to spread pro-US and anti-jihadist propaganda across Pakistan, Afghanistan and the Middle East. OEV has been described by US officials as aiming to "counter extremist ideology and propaganda" by ensuring "that credible voices in the region are heard". That being said, sceptical commentators have suggested that this is an outlet for the US military to create a false consensus in online conversations, crowd out unwelcome opinions and smother commentaries or reports that are not aligned to their own objectives. It is likely that in the near term, the negative view on astroturfing will prevent any attempt to adopt its principles in a benign manner.

CONCLUSION

10. It is important to recognise the threat that astroturfing poses to our information spaces, and its capability to undermine our social cohesiveness and exacerbate existing fault lines. At the same time, identifying astroturfing efforts requires a different approach from general disinformation campaigns. By identifying coordination patterns and being vigilant against astroturfing attempts, practitioners will be better able to recognise such campaigns and respond in a timely manner. Enhancing information sharing and building digital literacy are key to building a first line of defence within our populations to recognise and report such threats.

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1 Manufacturing Rage: The Russian Internet Research Agency's political astroturfing on social media
[Link: https://firstmonday.org/ojs/index.php/fm/article/view/10801/9723]

2 The Vladimirror Network: Pro-Putin Power Users on Facebook
[Link: https://www.isdglobal.org/wp-content/uploads/2022/04/The-Vladimirror-Network_Pro-Putin-Power-Users-on-Facebook_.pdf]

3 Political Astroturfing Around the World.
[Link: https://cyber.harvard.edu/sites/default/files/2019-11/Comparative%20Approaches%20to%20Disinformation%20-%20JungHwan%20Yang%20Abstract.pdf]

4 It's not easy to spot disinformation on Twitter.
[Link: https://www.washingtonpost.com/politics/2019/10/28/its-not-easy-spot-disinformation-twitter-heres-what-we-learned-political-astroturfing-campaigns/]

5 The Tactics and Tropes of the Internet Research Agency
[Link: https://digitalcommons.unl.edu/senatedocs/2/]

6 Cyber Influence Operations: An Overview and Comparative Analysis.
[Link: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf]

7 Revealed: US Spy Operation that manipulates social media
[Link: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks]

8 The Grass is not Always Greener on the Other Side: The Use of Digital Astroturfing to Spread Disinformation and the Erosion of the Rule of Law [Link: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1031&context=jsjp]

9 South Korea spy agency admits trying to rig 2012 presidential election [Link: https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012]