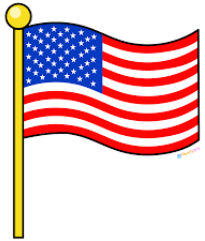
2024 Election Interference

Tech Talk – January 18, 2024

Is it only happening in the US?

- In researching election interference, I found reports on mal-information in the following countries: Taiwan, Kenya, Philippines, Nigeria, Brazil, Maldives. There was also a report done by 100 reporters in Europe who found it in 30+ countries around the world.
- So it’s not just limited to the US.



So what's the difference?
Misinformation?
Disinformation?
Mal-information?

Definitions
https://www.youtube.com/watch?v=cBAYmNMJtkA

RUSSIA

Let’s look at Russian mal-information activities…

- Known as Russia's Doppelganger campaign, it consists of Russian web brigades, also called Russian trolls, Russian bots, Kremlinbots, Kremlin trolls, etc., who are state-sponsored anonymous Internet political commentators and trolls.
- The campaign has expanded from faking websites of European outlets, including the U.K.'s The Guardian and Germany's Der Spiegel, to impersonating The Washington Post and Fox News as well as two Israeli news sites. It has also created fake websites purporting to represent NATO, the Polish and Ukrainian governments, the German police and the French Foreign Ministry.

Russia, continued

- The major area of mal-information is centered on the Ukraine war. Meta is continuing to take down fake accounts and ban fraudulent websites connected to a Russian-influence operation aimed at eroding support for Ukraine.
- Government officials said Russia was distracted by its war in 2022, but the fighting was intertwined with Russia's efforts to influence American politics. Russia appeared to consider delaying its withdrawal from the southern region of Kherson to avoid giving Ukraine supporters in the United States "a perceived win before the election." Russia ultimately announced its retreat a day after the election.

Russia, continued

- Reports in 2022 are that Russia tried to denigrate the Democratic Party, with a goal of weakening U.S. support for Ukraine, and undermine confidence in the elections. Russia also wants Republicans to win in order to inflict damage on NATO and the U.S. alliance system, and feels that a Trump White House will deliver victory for Russian forces in Ukraine.
- Before tearing our hair out on that one, remember what one spokesman at Meta said: "We've seen this operation posting its 'stop supporting Ukraine' content on websites with names like CoedNakedFootball.xyz, or EarlyGonorrhoeaSigns.com. As soon as you look at this, you just think, 'What?'"

CHINA

Let’s look at Chinese mal-information activities…

- Since 2019, tech companies and independent organizations have been tracking clusters of fake accounts posting pro-China content across social media. Known as "Spamouflage," these clusters were behind online attacks on pro-democracy protesters in Hong Kong and praise for China's COVID-19 response. These operations were mainly focused on YouTube, Twitter and Facebook. But as the larger companies caught on, it shifted to alternative sites that were smaller and less monitored.
- Now rather than start off on Facebook, it will post an article on a small forum in Nigeria or in Australia, and then it will start trying to share the link to that article on the larger platforms. Meta spokesman said "It's putting itself into these smaller and smaller buckets and then trying to reach out of there."

China, continued

- China worked very hard to try and sway the vote in the Taiwan election held five days ago. China wanted the Kuomintang presidential candidate to win so it appeared to pressure a billionaire businessman, Terry Gou, to drop out of the race. Gou claimed to have backing from Mazu, a sea goddess, but the Communist Party must have prevailed over the goddess as Gou did indeed drop out.
- A lot of other tactics were also tried, but China's attempts didn't work. The candidate that China didn't want to get elected, ended up winning.

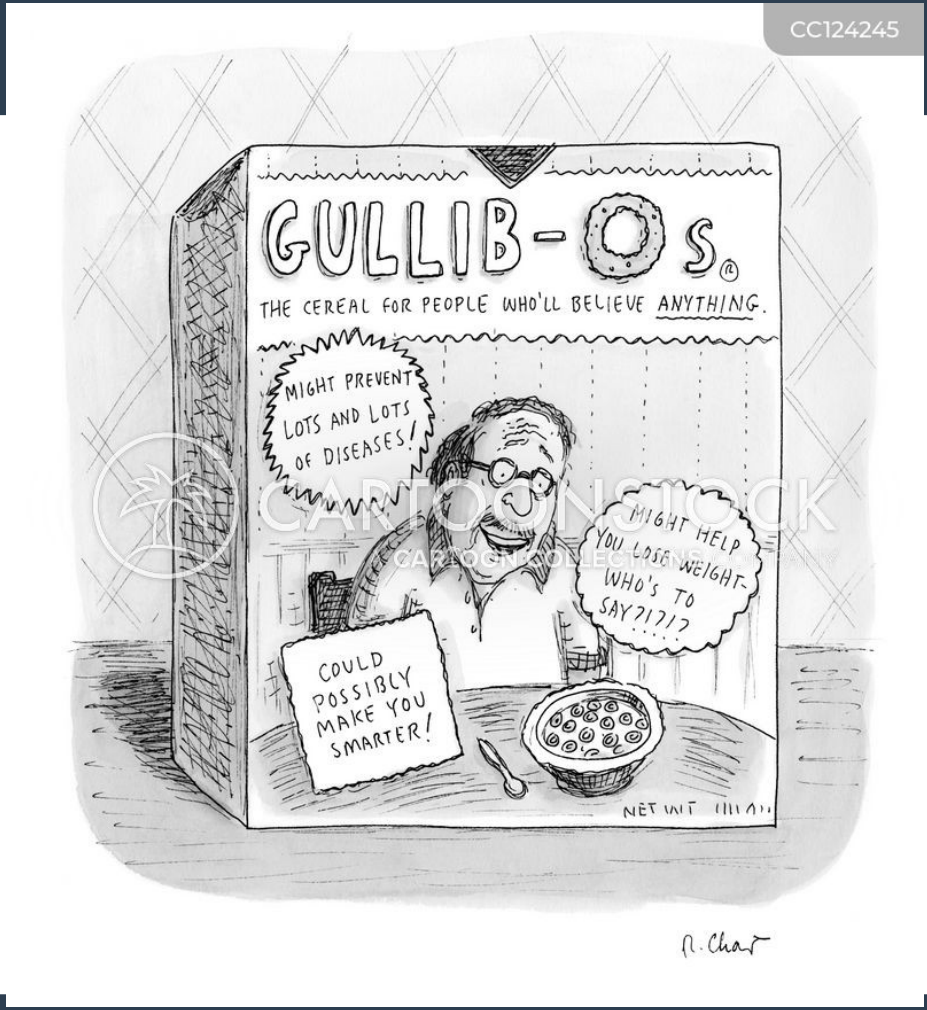
China, continued

- China has traditionally focused more narrowly and works against local politicians who take stands on Tibet, Taiwan or other similar issues. US officials say that may be about to change. It is not entirely clear what China is going to do, or what side it will take in 2024. But a report suggests that Chinese leaders viewed the 2022 election as a chance to portray the U.S. model as chaotic.
- How far the Chinese will go is not completely understood. But American spy agencies appear to know more than they are revealing. As one person said, “The report contains one of those frustrating redactions. It announces that Chinese leaders have ‘directed a new focus on’ and then blacks out the subject of the sentence.”

China, continued

- China has already begun experimenting with artificial intelligence in its influence campaigns. Industry experts say that new technologies will make it easier for foreign countries to mimic native English speakers and generate messages amplifying existing divisions more rapidly.
- Government officials are very worried about artificial intelligence technologies that could be used to create hyper-realistic, but fake, videos, and it's the kind of disinformation that could do damage quickly.

Why do people believe claims?


CC124245
GULLIB-O S.
THE CEREAL FOR PEOPLE WHO'LL BELIEVE ANYTHING.
MIGHT PREVENT LOTS AND LOTS OF DISEASES!
MIGHT HELP YOU LOSE WEIGHT. WHO'S TO SAY?!?!?
COULD POSSIBLY MAKE YOU SMARTER!
NET WT
R. Chast

Why people fall for misinformation
https://www.youtube.com/watch?v=hz6GULbowAk

What to look for regarding bots

Bots…

- What does a bot profile look like? The picture and username with a profile can be quite telling. Often if the username is a string of jumbled letters and numbers, there is a good chance it is a bot. You might also notice the profile picture is missing, or shows up in a reverse image search, meaning it has been used many times on the internet.
- if a presidential candidate tweets out something, a swarm of bots could automatically respond to him or her, thereby giving the impression of a massive crowd reaction. Or, the bots could be set up to tweet out any news items that are supportive of a particular cause on a 24/7 basis. With that in mind, let's look at a few rules to help with decisions.

Bots, continued

- Rule #1: Bots generate tremendous amounts of content
- Perhaps the defining aspect of a “bot” is that it’s constantly working to support a certain cause or to attack something it doesn’t believe in. While a human might send out 10 tweets a day, a bot can send out 50, 100, or even 1,000 tweets per day. Thus, if you spot a media account that is extremely hyperactive in how much content it generates, you’ve probably found a bot.

Bots, continued

- Rule #2: Bots have strange personal profiles
- On social media, bots don't spend a lot of time building up their personal profiles. Often, profile photos will be left blank and handles are sometimes just a nonsensical string of letters and numbers. Personal profiles are usually left blank as well. And most of these bots were set up fairly recently – so if you see that a social media account was set up for the first time in 2021, 2022, or 2023 that might be a tip-off you've encountered a new recruit for a media bot army.

Bots, continued

- Rule #3: Bots tend to hang out together
- The whole point of creating bots is to have a swarm of voices all talking about the same thing, all at the same time. Thus, bots link to bots. Bots re-tweet other bots. And bots follow other bots. So if you check out the followers of a bot media account, you'll often spot lots of suspicious-looking accounts. It's literally an echo chamber, with bots echoing other bots.

Bots, continued

- Final thought
- Just beware of “false positives,” because sometimes humans act a lot like bots – we go off on massive rants, or we only re-send things sent by people who think exactly like us. It’s too easy to dismiss someone who doesn’t think like us as a “Russian bot” – and it’s led to embarrassing situations where journalists have mistakenly accused some social media accounts of being bots.

So, where’s the good news?

GOOD NEWS...

- Many online entities are working to prevent mal-information from being posted. The largest is Meta (Facebook, Instagram) so I'm zeroing in on them.
- Meta said the last operation they took down was the "largest and most aggressively persistent" it had seen from Russia since 2017. Meta has taken down thousands of fake accounts and pages connected to that network and blocked more than 2,000 domains from being shared on Facebook and Instagram in the past two years.
- This Russian operation hasn't gained much traction among real social media users. That is because, in part, the fake accounts being used to promote links to the mal-info websites are so obviously fake as to be quickly detected.

A Question???

- Now the U.S., by law, is barred from combating disinformation on social media.
- Both Beijing and Moscow rely on informational, and perhaps more importantly, economic tools to weaken electoral prospects and, in some cases, strengthen their preferred candidates. These authoritarian influence campaigns pose a major dilemma for liberal democracies. Should constitutional democracies stand by and simply observe as authoritarian governments interfere in their electoral processes? And if they counteract these efforts, how to do so?

Good news, continued

- AI-generated fake faces are big on online influence operations. Meta said the Spamouflage operation is spread across different parts of China but shares internet infrastructure and "centralized directions" about what content to post.
- Meta has removed more than 8,600 Facebook accounts, pages, groups and Instagram accounts with a collective following of about 561,000 accounts. However, the company said many of those followers were themselves fake accounts, because the Chinese operation appeared to have bought pages from spam operators in Vietnam and Bangladesh that create pages and populate them with bot followers.

Good news, continued

- When real people pick up on Spamouflage online, they often reply to it and say, 'This is not real, this is a fake account' and call it out. So always do a quick scan of comments.
- There are times that one has to wonder if they are really trying to reach an audience in this country or are they just trying to show the people who are paying them that they're posting lots of content?

More good news...

MORE GOOD NEWS...

- So are countries still trying to hack into local government computer systems in the US?
- They are not. This is one bit of good news in the most recent intelligence assessment.
- The American election system's extreme decentralization is its greatest defense. Russian hackers did target voting systems in 2016, but foreign countries now believe it is far too difficult to meaningfully affect vote counts by hacking into local government computer networks.

More good news, continued

- A declassified U.S. government report concerning the 2022 federal elections says “foreign hackers did not change vote totals or otherwise compromise the integrity of federal elections” in the United States. The report does identify multiple instances in which hackers linked to Iran, China and Russia connected to election infrastructure, scanned state government websites, and copied voter information.
- But the report says there is no evidence that any cyber activity had any impact on the election or on the vote totals.

More good news, continued

- A Justice and Homeland Security report says election officials, third-party vendors and political organizations have all taken steps to reduce the potential for a damaging cyber intrusion, and federal and state officials have improved their collaboration with the private sector.
- The report does single out several episodes including suspected Chinese government hackers who scanned “election-related and non-election state government websites” or collected publicly available voter information, as well as pro-Russian “hacktivists” who claimed to have conducted a cyberattack that temporarily affected access to a state election office website.

[A brief aside on non-tech influences]

- Putin uses Russia's oil leverage to influence US political outcomes. It cut crude oil production ahead of the 2016 presidential election which led to an increase in consumer prices. It boosted output in September 2018 before the midterms and sharply decreased production in October 2022. Russia and other oil autocracies appear extremely likely to cut production ahead of the 2024 presidential election.
- But China won't like that. It's unclear how much Beijing will or can tolerate turmoil in oil markets. China is the world's largest crude oil importer and will suffer if Putin inflicts pain on the global economy ahead of the presidential election. And OPEC+ sells a lot of oil to China so they won't be happy if China isn't happy.

More good news, continued

- The National Intelligence Council, which represents the consensus of the U.S. intelligence network, assessed that the “aggregate scale and scope of foreign activity targeting the [2020] US midterm elections exceeded” what was detected during the 2018 midterms, and that Chinese cyber actors and pro-Russian hacktivists were largely unsuccessful in their efforts to target U.S. election infrastructure.

More good news, continued

- “There is no evidence that this activity prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information or any ballots cast during the 2022 federal elections.”

More good news, continued

- Russia's efforts in 2016 to meddle in the US election focused attention on election interference. Since then, US spies are seeing fewer and fewer attempts to attack voting infrastructure.
- "Notably, we have not seen persistent foreign government cyber efforts to gain access to and tamper with U.S. election infrastructure since the presidential election in 2016." Russia "almost certainly" accessed election-related infrastructure in two states that year and "reconnoitered" election systems in all states.

More good news, continued

- Because foreign actors have faced challenges in getting into the US election system and because of the heightened awareness of and resilience to cyber operations, these bad guys, who have been trying to affect election outcomes, are beginning to feel they'll have more impact with other operations than through targeting our voting system.
- The US intelligence community assesses that election interference is likely to shift away from voting infrastructure and toward establishing influence on online platforms. This is a move attributed to the establishment of "clear redlines" from the US as an effective deterrent.

More good news, continued

- Several tech giants have assessed their own election security protocols ahead of a packed election calendar around the world in 2024. Google released a memo outlining how it plans to approach the coming elections, detailing everything from how it intends to safeguard its platforms from abuse to how it will help the public better identify AI-generated election content.
- The US has bolstered its defenses, especially in partnerships that connect federal agencies, state election officials, and private industry. Using private industry allows the government to work faster.

More good news, continued

- FBI Director Wray has said “All those partnerships are exponentially more sophisticated and effective than they were in each prior election cycle, so we are, in that sense, much more on guard than we were in earlier cycles. So the threats are more challenging but the defense is better.”
- Wray would not say which new countries are now involved in election interference efforts but noted that in the last election, efforts by hackers in Iran to cause issues were quickly stopped and called out.

More good news, continued

- The government has a cybersecurity collaboration center created in 2020 that allows coordination with more than 850 defense industrial base companies.
- Participants can share information about vulnerabilities immediately, and it has become a big advantage in the fight against adversaries seeking to exploit prominent bugs.
- One finding is that AI-generated items can’t seem to come up with the needed bias impact that a human being can.

More good news, continued

- Plus we have “cyber soldiers” that are tasked with helping prevent problems within the infrastructure of our country.
- One team identified an intrusion by Iran as part of what is termed a “hunt-forward” mission, which gathers intelligence on and watchs the bad guys. The team quickly alerted officials at the U.S. cybersecurity agency, who then worked with the municipality to respond to the intrusion.

More good news, continued

- The National Defense Authorization Act passed in 2018 lets the US take down infrastructure and take on “adversaries” outside the country. In 2020 it allowed the US to step in and thwart attempts by Russia and Iran to interfere with the US election that year.
- Cybercom (US Cyber Command Center) has sent small teams to 22 countries to help hunt on their networks — “to identify malware, tradecraft, techniques that adversaries are using and then broadly publicize that.” That included Ukraine, where a team arrived on Dec. 3, 2021, more than two months ahead of the Russian invasion.

CYBER “SOLDIERS” are working all the time…

- Cyber Soldiers – current as well as former military and other cyber geeks monitor the online world, including the dark web, and let the proper authorities know of any misdeeds.
- So there’s a lot of “eyes” out there watching ---

Why I serve: Cyber Soldiers
https://www.youtube.com/watch?v=5xy1nTVZKjA

What can we do…

- It may not be the Democrats or the Republicans or Trump or Biden supporters who are splitting us apart, but rather someone in Russia, China, Iran, or another country attempting to manipulate us.
- Therefore, be sure and talk to people about how secure our election system is and how other countries are trying to promote division within our country through the news and online postings, especially on social media.

AND ONCE AGAIN FOR THE ZILLIONTH TIME..

If a news item, text, email, or media posting makes you laugh, sad, angry, or tugs at your heart strings, be suspicious. Make sure it's not something to lead you astray.

- Next Tech Talk is scheduled for Thursday, March 21, 2024 at 2:00 PM. I have no idea what it will be about.
- Any suggestions????