# APPENDIX 2

## CONTENTS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CBP Press Release - Say No to the Coyote</td>
<td>3</td>
</tr>
<tr>
<td>2. CISA Insights - COVID-19 Disinformation Activity</td>
<td>6</td>
</tr>
<tr>
<td>3. CISA Insights - Mitigating Foreign Influence</td>
<td>8</td>
</tr>
<tr>
<td>4. CISA The War on Pineapple - Understanding Foreign Interference in 5 Steps</td>
<td>12</td>
</tr>
<tr>
<td>5. CISA The War on Pineapple - Understanding Foreign Interference in 5 Steps Spanish</td>
<td>14</td>
</tr>
<tr>
<td>6. Disinformation Stops with You Infographic Set</td>
<td>16</td>
</tr>
<tr>
<td>7. Disinformation Stops with You Infographics Set Spanish</td>
<td>23</td>
</tr>
<tr>
<td>8. Foreign Interference Taxonomy</td>
<td>30</td>
</tr>
<tr>
<td>9. Foreign Interference Taxonomy Spanish</td>
<td>32</td>
</tr>
<tr>
<td>10. Information Manipulation Infographic</td>
<td>34</td>
</tr>
<tr>
<td>11. Information Manipulation Infographic Spanish</td>
<td>36</td>
</tr>
<tr>
<td>12. Mis- Dis- and Mal- Information Planning and Incident Response Guide for Election Officials</td>
<td>38</td>
</tr>
<tr>
<td>13. Resilience Series - Bug Bytes Graphic Novel</td>
<td>45</td>
</tr>
<tr>
<td>14. Resilience Series - Real Fake Graphic Novel</td>
<td>83</td>
</tr>
<tr>
<td>15. Rumor Control Start-Up Guide</td>
<td>119</td>
</tr>
<tr>
<td>16. Social Media Bots Infographic</td>
<td>125</td>
</tr>
<tr>
<td>17. Social Media Bots Infographic Spanish</td>
<td>130</td>
</tr>
<tr>
<td>18. Tools of Disinformation - Inauthentic Content</td>
<td>134</td>
</tr>
<tr>
<td>19. Tools of Disinformation - Inauthentic Content Spanish</td>
<td>136</td>
</tr>
</tbody>
</table>
CBP Launches Digital Ad Campaign “Say No to the Coyote” to Warn Migrants About Smuggler Lies

Release Date - Wed, 05/11/2022

U.S. Immigration Laws Remain in Effect. Smugglers are lying to you.

WASHINGTON – U.S. Customs and Border Protection (CBP) launched a digital advertisement campaign this week to dissuade migrants in the Northern Triangle countries of Honduras and Guatemala who might consider taking the dangerous journey to the U.S. border. The ads deliver a clear message: smugglers are lying to you, the fact is that entering the United States illegally is a crime. The ads highlight that smugglers, known as ‘coyotes,’ who take advantage of and profit from vulnerable migrants.

“Smugglers use lies to lure the vulnerable into a dangerous journey that often ends in removal or death,” said CBP Commissioner Chris Magnus. “This digital ad campaign is an important component of U.S. government efforts to prevent tragedies and curtail irregular migration.”

The initial two-month ad buy, which will reach migrants via mobile devices on social media and other digital platforms, directs migrants to a landing page that lays out the harsh realities, including the fact that smugglers are criminals and that U.S. immigration laws remain in effect.

For years, CBP has run ad campaigns to dissuade migrants from putting their lives in the hands of smugglers and to inform them of the U.S. immigration laws in place. These ads are an expansion of those efforts and are part of DHS’s comprehensive, whole-of-government plan to manage any potential increase in the number of migrants encountered at our border, and build on the work of the Department to deter irregular migration south of our border.

The message warns that those attempting to cross the U.S. border without authorization will be immediately removed from the country or placed into immigration removal proceedings. Users are also reminded of the thousands who are jailed, kidnapped, extorted, or even left to die by unscrupulous transnational criminal organizations. In Fiscal Year 2021, Northern Central American countries accounted for 44 percent of migrant encounters along the Southwest border. The ad includes additional creative displays that users are invited to share on Whatsapp or through social media.
DHS coordinates closely with the Department of State to track trends, share research, and coordinate messaging to counter tactics that smugglers use to victimize vulnerable migrants. The Department has deployed paid advertising on radio and digital platforms, and held press conferences and media interviews in source and transit countries. These messages counter the lies propagated by human smugglers and warn migrants of the dangers of being exploited and facing death at the hands of unscrupulous criminal organizations.

To view the ad campaign, please visit: https://www.cbp.gov/coyote-criminal


U.S. Customs and Border Protection is the unified border agency within the Department of Homeland Security charged with the management, control and protection of our nation's borders at and between official ports of entry. CBP is charged with securing the borders of the United States while enforcing hundreds of laws and facilitating lawful trade and travel.
CISA INSIGHTS

COVID-19 Disinformation Activity

False and misleading information related to the coronavirus (COVID-19) are a significant challenge. This CISA Insight provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

COVID-19 DISINFORMATION

After the initial outbreak of COVID-19, disinformation campaigns appeared online. Information manipulation and fabrication about COVID-19’s origin, scale, government response, and/or prevention and treatment surged as creators leveraged people’s increased uncertainty.

Virus Origin
China and other authoritarian governments have promoted false claims about the origins of the virus in an attempt to shift blame overseas and divide free societies against themselves. Common tactics they use include censoring news, injecting false narratives onto social media platforms, and promoting slick government-produced videos.

Virus Scale
Chinese state-backed media continue to promote content emphasizing China’s claimed success rapidly controlling the virus, while suggesting the U.S. and other Western countries have failed in their response. These narratives are amplified on a variety of social media platforms.

5G and COVID
Disinformation campaigns have promoted false narratives that 5G technology suppresses immune systems and that 5G spectrum bands spread the virus.

Government Response to COVID-19
Disinformation involving the government’s response to COVID-19 has been circulated to cause confusion among Americans, including false claims the National Guard Bureau would be supporting nationwide quarantines.

Prevention and Treatment of COVID-19
False information about COVID-19 treatments continue to circulate on social media, including potentially extremely harmful suggestions to drink bleach or chlorine dioxide, to use vitamin C or boiled garlic, or that illicit drug activity can “cure” the virus.

PROTECT YOURSELF

There are simple steps you can take to minimize the likelihood of amplifying disinformation.

1. Go to trusted sources of information like www.Coronavirus.gov. FEMA has also established a coronavirus rumor control website at www.FEMA.gov/coronavirus/rumor-control where you can learn more about specific disinformation campaigns.

2. Check the source of the information.

3. Search for other reliable sources of information on the issue.

4. Think before you link – take a moment to let your emotions cool down before sharing anything online.

CISA’S ROLE AS THE NATION’S RISK ADVISOR

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.

Contact Information:
CISA.gov has more information about COVID-19, as well as information on identifying and combating disinformation. We ask that anyone with any relevant information, or indication of a compromise, contact us immediately.
Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure

February 2022

Threat Overview

Malicious actors use influence operations, including tactics like misinformation, disinformation, and malinformation (MDM), to shape public opinion, undermine trust, amplify division, and sow discord. Foreign actors engage in these actions to bias the development of policy and undermine the security of the U.S. and our allies, disrupt markets, and foment unrest. While influence operations have historical precedent, the evolution of technology, communications, and networked systems have created new vectors for exploitation.

A single MDM narrative can seem innocuous, but when promoted consistently, to targeted audiences, and reinforced by peers and individuals with influence, it can have compounding effects. Modern foreign influence operations demonstrate how a strategic and consistent exploitation of divisive issues, and a knowledge of the target audience and who they trust, can increase the potency and impact of an MDM narrative to National Critical Functions (NCFs) and critical infrastructure. Furthermore, current social factors, including heightened polarization and the ongoing global pandemic, increase the risk and potency of influence operations to U.S. critical infrastructure, especially by knowledgeable threat actors.

In recent years, foreign actors have used influence operations to influence U.S. audiences and impact critical functions and services across multiple sectors. Foreign influence operations have been paired with cyber activity to derive content, create confusion, heighten anxieties, and distract from other events. In light of developing Russia-Ukraine geopolitical tensions, the risk of foreign influence operations affecting domestic audiences has increased. Recently observed foreign influence operations abroad demonstrate that foreign governments and related actors have the capability to quickly employ sophisticated influence techniques to target U.S. audiences with the goal to disrupt U.S. critical infrastructure and undermine U.S. interests and authorities.

This CISA Insights product is intended to ensure that critical infrastructure owners and operators are aware of the risks of influence operations leveraging social media and online platforms. Organizations can take steps internally and externally to ensure swift coordination in information sharing, as well as the ability to communicate accurate and trusted information to bolster resilience. CISA encourages leaders at every organization to take proactive steps to assess their risks from information manipulation, increase resilience, and mitigate the impact of potential foreign influence operations.

Assess the Information Environment

- Evaluate the precedent for MDM narratives targeting your sector.
- Learn how and where your stakeholders and customers receive information.
- Map key stakeholders and how you communicate with them. Consider how these channels would allow your organization to identify and respond to MDM activity. Operate on the principle of empowering trusted partners with accurate information.
- Monitor for any changes to online activity related to your organization and sector, such as a sudden increase in tags or followers, a spike in searches, or a high volume of inquiries.
Identify Vulnerabilities

- Identify potential vulnerabilities that could be exploited by MDM. Think about common questions or points of confusion that people have about your sector and operations.

Organizations should establish their own criteria for evaluating the severity of MDM narratives. Examples of indicators could include:

- **High:** Does a narrative significantly threaten to undermine your critical function? What are known examples?
- **Medium:** Does a narrative or incident have the potential to negatively affect your critical function?
- **Low:** What narratives are clearly disprovable, implausible, or pose a limited threat?

Your assessment can inform your information sharing around, and response to, MDM narratives, helping decide whether to respond, and, if so, when. It also can guide which stakeholders you should engage to amplify response efforts.

- Educate staff on securing their personal social media accounts. Encourage all staff members to use multi-factor authentication for social media accounts and review their privacy settings to make sure they know what information about them is visible online.
- Remind staff to practice smart email hygiene and to be on alert for phishing emails and advise against clicking on suspicious links and/or forwarding questionable information.

Fortify Communication Channels

- Engage your stakeholders to establish clear communication channels and coordination mechanisms for information sharing.
- Review and update your organization’s website to make information as clear, transparent, and accessible as possible.
- Review and update your organization’s presence on social media platforms and seek any verification methods that platforms offer for official accounts.
- Review access privileges for company social media accounts. Turn on multi-factor authentication and use complex passwords.

Engage in Proactive Communication

- If your organization has established ways of communicating with its constituents, stakeholders, and/or community, review these practices to identify opportunities for improvement. This may include newsletters, reports, blog posts, events, social media content, podcasts, or other activities.
- Evaluate the reach and engagement of your communication efforts and adjust your strategy as needed.
- Coordinate with other organizations in your sector to amplify and reinforce messaging, with the goal of building a strong network of trusted voices.
- Encourage your communications professionals to maintain contact with key communications outlets.

Cyber Activities and Influence Operations:

Malicious actors can use hacking and other cyber activities as part of influence operations. Hackers assist in surveillance or reconnaissance and provide opportunities for destructive attacks. Hijacking accounts and defacing public facing sites can be used to influence public opinion. Organizations should be aware of cyber risks and take action to reduce the likelihood and impact of a potentially damaging compromise.

Communications as a Tool:

Using clear, consistent, and relevant communications that not only responds, but anticipates MDM is an important, effective way to maintain security and build public confidence in your organization.
**Develop an Incident Response Plan**

- Designate an individual to oversee the MDM incident response process and associated crisis communications.
- Establish roles and responsibilities for MDM response, including but not limited to responding to media inquiries, issuing public statements, communicating with your staff, engaging your previously identified stakeholder network, and in implementing physical security measures.
- Ensure your communication systems are set up to handle incoming questions. Phones, social media accounts, and centralized inboxes should be monitored by multiple people on a rotating schedule to avoid burnout.
- Identify and train staff on reporting procedures to social media companies, government, and/or law enforcement.
- Consider your internal coordination channels and processes for identifying incidents, delineating information sharing and response. Foreign actors can combine influence operations with cyber activities, requiring additional coordination to facilitate a whole-of-organization response.

**TRUST Model:**

In today’s information environment, critical infrastructure owners and operators must play a proactive role in responding to MDM. While each MDM narrative will differ, the TRUST model for incident response can help reduce risk and protect stakeholders.

1. **Tell Your Story**
2. **Ready Your Team**
3. **Understand and Assess**
4. **Strategize Your Response**
5. **Track the Outcomes**
THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps

To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot-button issues in the United States. They don’t do this to win arguments; they want to see us divided.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.

Pro Tip: Look at a account’s activity history. Genuine accounts usually have several interests and post content from a variety of sources.

3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or “trolling” people online.

Pro Tip: Trolls try to make people mad, that’s it. If it seems like an account is only aiming to raise tensions, think about whether it’s worth engaging.

4. MAKING THE MAINSTREAM

Foreign influencers “fan the flames” by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.

Sometimes controversies make it into the mainstream and create division among Americans. This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences.

5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out. What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.

Pro Tip: Many social media companies have increased transparency for organization accounts. Know who is inviting you and why.

For more information, please visit the #Protect2020 website at https://www.dhs.gov/cisa/protect2020.
LA GUERRA CONTRA LA PIÑA: Cómo entender la interferencia extranjera en 5 pasos

Hasta la fecha, no tenemos pruebas de que Rusia (o cualquier otro país) esté ejecutando de manera activa algún tipo de operaciones de información en contra de ingredientes para pizzas. Esta Infografía es una ILLUSTRACIÓN de cómo en el pasado se han llevado a cabo operaciones de información para explotar las divisiones en los Estados Unidos.

1. SELECCIONAR TEMAS QUE CAUSEN DIVISIONES

Los influenciadores extranjeros están constantemente buscando oportunidades para instigar conversaciones acerca de temas candentes en los Estados Unidos.

No con la intención de ganar discusiones, sino de vemos divididos.

2. MOVER LAS CUENTAS EN SU SITIO

Crear cuentas en las redes sociales con un gran número de seguidores requiere de tiempo y recursos, por lo que las cuentas suelen cambiar de nombre y son reutilizadas. Múltiples cuentas en una conversación suelen ser controladas por el mismo usuario.

Consejo práctico: Observe el historial de actividad de una cuenta. Las cuentas auténticas suelen tener varios intereses y publican contenidos de diversas fuentes.

3. AMPLIFICAR Y DISTORSIONAR LA CONVERSACIÓN

Los estadounidenses suelen involucrarse en un sano debate sobre diversos temas. Los influenciadores extranjeros intentan contaminar esos debates con información errónea y hacer que nuestras posiciones sean más extremas a través de actitudes pendencieras o “troleando” [trolling] a la gente en línea.

Consejo práctico: Los trols [trolls] tratan de enfadar a la gente, eso es todo. Si es aparente que una cuenta sólo busca generar tensiones, piense si vale la pena involucrarse.

4. CONVERTIR EN LA CORRIENTE PRINCIPAL

Los influenciadores extranjeros “avivan las llamas” creando controversia, amplificando la versión más extrema de los argumentos en ambos lados del tema. Estos se comparten en línea como fuentes de información legítimas.

A veces dichas controversias llegan a la opinión popular y crean división entre los estadounidenses. ¡Ahí es cuando los influenciadores extranjeros ganan. Su intromisión se legitima y se extiende hacia audiencias más amplias.

5. LLEVAR LA CONVERSACIÓN AL MUNDO REAL

En el pasado, los agentes del Kremlin han organizado o financiado protestas para incitar divisiones más profundas entre los estadounidenses. Crean páginas de eventos y piden a sus seguidores que acudan.

Lo que inicia en el espacio cibernético puede hacerse muy real, con estadounidenses atacando a otros estadounidenses debido a la interferencia extranjera.

Consejo práctico: Muchas empresas de redes sociales han aumentado la transparencia en las cuentas de organizaciones. Conozca quién lo invita y por qué.


Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - laenguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Bad actors spread disinformation to undermine democratic institutions and the power of facts. False or misleading information can evoke a strong emotional reaction that leads people to share it without first looking into the facts for themselves, polluting healthy conversations about the issues and increasing societal divisions.

Do your part to stop the spread of disinformation by practicing and sharing these tips.

**Recognize the Risk**
Understand how bad actors use disinformation to shape the conversation and manipulate behavior.

**Question the Source**
Check who is really behind the information and think about what they gain by making people believe it.

**Investigate the Issue**
Search reliable sources to see what they are saying about the issue.

**Think Before You Link**
Take a moment to let your emotions cool and ask yourself whether your feelings about the content are based on fact.

**Talk With Your Circle**
Talk with your social circle about the risks of disinformation and how to respond when you see it.

---

**Who to follow**

- **Trusted Sources**
  - Follow
  - Rely on official websites and verified social media for authoritative information.

**Types of false info**

- **Misinformation**
  - is false, but not created or shared with the intention of causing harm.

- **Disinformation**
  - is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

- **Malinformation**
  - is based on fact, but used out of context to mislead, harm, or manipulate.

**Who spreads disinfo?**

- **Foreign States**
- **Scammers**
- **Extremist Groups**

Learn more at [www.cisa.gov/mdm-resource-library](http://www.cisa.gov/mdm-resource-library)

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Disinformation Stops With You

Recognize the Risk

Understand how malicious influencers use disinformation to shape the conversation and manipulate behavior. Once they’ve built an online presence, they start to post false or misleading content that steers their audience to more extreme positions and spreads to a bigger audience.

Learn more at www.cisa.gov/mdm-resource-library

Divide Us Bad actors use divisive societal issues to polarize Americans and push us into echo chambers that further amplify disinformation and obstruct healthy conversations about the issues.

Build a Following They may start to attract followers by posting entertaining, non-controversial content that appeals to their audience and builds trust before sharing disinformation.

Go Viral They’ll often post disinformation as fun memes that are easy to share and get high engagement on social media, like captioned photos and GIFs. It may appear next to other entertaining content.

Amplify Coordinated campaigns spread disinformation across social media platforms, state-funded communication channels, and sometimes even official accounts, reaching far beyond the bad actor’s immediate followers.

Make It Mainstream Even disinformation originally shared to a small audience can do huge damage when it is amplified, sometimes gaining mainstream media coverage that may lend it further credibility and a bigger audience.

Real World Effects Bad actors use online disinformation to affect our real-world behavior, like trying to influence how we vote, inciting physical confrontations, and disrupting healthy democratic discussions and participation.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Disinformation Stops With You

Question the Source
Check who is really behind the information and think about what they gain by making people believe it. Disinformation is often designed to look authentic. Critically evaluate content to discern whether it’s trustworthy.

Learn more at www.cisa.gov/mdm-resource-library

Check the Author
Research the author’s credentials. What else have they published? Are they qualified to cover the topic? If the content doesn’t include an author’s name, it might be disinformation.

Check the Date
When was it published? Outdated content can lack important context, making it irrelevant to current events and misleading to someone reading it in the present.

Check the Message
What is the content really saying? Disinformation often pushes a single viewpoint, takes an emotional tone, and uses attention-grabbing headlines that may not match the actual content.

Check for Facts
Consider how the author supports their arguments and whether they address counterarguments. Opinions without evidence may not be accurate. Trustworthy fact-checking sites can help evaluate claims.

Check the Sources
Credible content will cite supporting sources and provide additional resources for more information. Click on source links to make sure they work and support the content.

Check the Quality
Disinformation is often hosted on low-quality websites. Look for signs, such as many ads; questionable sponsors; poor spelling, grammar, and punctuation; and suspicious URLs that mimic legitimate news sites.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Disinformation Stops With You

Investigate the Issue

Search other reliable sources to see what they are saying about the issue. A thorough search will help make sure you that you are sharing accurate information. Don’t share content if it isn’t from a credible source or you can’t find another credible source to confirm it.

Learn more at www.cisa.gov/mdm-resource-library

Is the Source Credible?
Look at the site’s “About” page to see whether it includes detailed information, such as its values, ownership, location, funding, and contact information.

What are Credible Sources Saying?
Search the issue on trustworthy sites. If the facts reported by credible sources don’t align with the content you’re reviewing, don’t share it.

What are Fact Checkers Saying?
It’s easy to believe things that confirm our views. If a claim seems too good to be true, see whether a trustworthy fact-checking organization has evaluated it and provided additional context.

Is Your Investigation Neutral?
Make sure you are using unbiased search language and remain open-minded to evidence that might contradict your beliefs.

Does it Acknowledge Other Perspectives?
Most hot-button issues are complicated. Although all authors have their own viewpoint, credible sources will recognize other perspectives and provide factual context around the issue.

Does it Provoke a Strong Reaction?
If the content makes you feel shocked, angry, or sad, consider that its purpose may be to get you to respond emotionally and share it without confirming its accuracy.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Disinformation Stops With You

Think Before You Link
Take a moment to let your emotions cool and ask yourself whether your feelings about the content are based on fact. Disinformation is designed to evoke a strong emotional reaction that bypasses your critical thinking. You can interrupt the cycle of disinformation by taking time to research the content and reflect on whether sharing it would benefit the conversation.

Learn more at www.cisa.gov/mdm-resource-library

Know the Risk
Sharing something you see online can seem harmless in the moment, but spreading disinformation can damage our ability to have meaningful conversations.

Know the Content
Headlines and captions are often exaggerated to get an emotional response. Take time to read the entire post and determine whether they accurately reflect the content.

Know the Facts
Investigate the issue being discussed. Check with trustworthy sources and fact checkers to verify the claims and make sure that they have not been taken out of context.

Know the Source
Question who is really behind the content. Critically evaluate the credibility of the author and the legitimacy of the outlet by checking for facts, sources supporting the claims, and quality of the site.

Know Why You’re Seeing It
Social media algorithms promote content they think you will engage with, sometimes through specific targeting. If it was shared by a friend, make sure you trust the original source as much as the friend.

Know Yourself
Ask yourself why you are sharing the content. People often share content that confirms their beliefs, even if it is untrue. If you wouldn’t share it in person, don’t share it online.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Disinformation Stops With You

Talk With Your Circle
Talk with your social circle about the risks of disinformation and how to respond when you see it. It’s probably not worth engaging with every piece of disinformation, but speaking up can help stop the spread. Do your research and share what you know with friends and family.

Learn more at www.cisa.gov/mdm-resource-library

Come Prepared
Make sure you’ve done your homework and know the facts before starting a conversation. Even if you’re sure it’s disinformation, brush up on the latest evidence to be safe.

Decide If It’s Worth It
Once you have the facts, evaluate whether it’s worth weighing in. Will your response help the conversation or cause conflict?

Respond Privately
If you decide to respond, try doing so via direct message or even an offline conversation. Public comments can give disinformation more visibility and make discussions more confrontational.

Focus on the Facts
If you do respond publicly, lead with the truth and don’t repeat the false claim. Provide links to neutral, credible sources with more information about the issue.

Be Respectful
Try to understand the beliefs of the person you’re speaking with so you will be heard in return. It can be hard to change attitudes, but stay calm, positive, and empathetic to get your message across.

Be a Resource
Stopping disinformation when you see it is important, but you can help friends and family build resilience to disinformation by proactively sharing resources and tips for doing their own fact-checking.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
La desinformación se detiene con usted

Los actores maliciosos difunden desinformación con el fin de debilitar las instituciones democráticas y el poder de los hechos reales. La información falsa o engañosa tiene la capacidad de evocar una intensa reacción emocional que lleva a la gente a compartirla sin primero investigar los hechos por su cuenta, contaminando el diálogo constructivo acerca de dichos temas y fomentando las divisiones sociales.

Ponga de su parte para detener a la difusión de desinformación practicando y compartiendo los siguientes consejos.

Reconozca el riesgo
Verifique quién realmente está detrás de la información y piense en lo que esa fuente gana al lograr que la gente le crea.

Cuestione la fuente
Verifique quién realmente está detrás de la información y piense en lo que esa fuente gana al lograr que la gente le crea.

Investigue el tema
Busque fuentes confiables para ver qué dicen acerca del tema en cuestión.

Piense antes de compartir un enlace
Dese un momento para dejar que sus emociones se enfríen y para preguntarse si sus sentimientos sobre el contenido están basados en hechos reales.

Hable con su entorno familiar y social [su círculo]
Hable con su círculo social acerca de los riesgos de la desinformación y cómo pueden responder cuando la identifiquen.

A quién seguir

Fidedignas
Confíe en sitios web oficiales y en redes sociales verificadas para obtener información confiable.

Tipos de información falsa

Información errónea o equivocada [Misinformation]
es falsa, pero no ha sido creada o compartida con la intención de causar daño.

Desinformación [Disinformation]
es creada con el fin deliberado de engañar, perjudicar o manipular a una persona, grupo social, organización o país.

Información maliciosa [Malinformation]
se basa en hechos reales, pero es utilizada fuera de contexto con el propósito de engañar, perjudicar o manipular.

¿Quién disemina la desinformación?

Estados extranjeros
Estafadores
Grupos extremistas

Encuentre más información en www.cisa.gov/mdm-resource-library

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alineen con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
La desinformación se detiene con usted

Comprenda cómo usuarios maliciosos e influyentes en las redes sociales utilizan la desinformación para alterar el diálogo y manipular el comportamiento. Una vez que han construido una presencia en línea, empiezan a publicar información falsa o engañosa que conducen a su audiencia a posiciones cada vez más extremas, y a que se propague a un público creciente.

Encuentre más información en www.cisa.gov/mdm-resource-library

- Dividirse
  Los agentes criminales utilizan temas sociales divisivos con el fin de polarizar a los estadounidenses, y colocarnos en cámaras de eco [echo chambers] que amplifican aún más la desinformación e impiden el diálogo constructivo.

- Crear una presencia que atrae a seguidores
  Pueden empezar a atraer seguidores publicando contenido de carácter divertido, no controvertido y llamativo para su audiencia; lo cual les permite ganar la confianza de sus seguidores antes de compartir desinformación.

- Hacerse virales
  Suelen publicar desinformación a través de memes divertidos que son fáciles de compartir y que consiguen mucha atención en las redes sociales, tales como fotos con subtítulos y GIFs. Pueden aparecer en conjunto con otros contenidos de entretenimiento.

- Amplificar
  Las campañas coordinadas diseminan desinformación a través de las plataformas de redes sociales, los canales de comunicación financiados por estados nacionales, e inclusive en ocasiones, a través de cuentas oficiales, alcanzando una audiencia que va más allá de los seguidores inmediatos del usuario malicioso.

- Convertirse en tendencia generalizada
  Incluso la desinformación que inicialmente se comparte con una audiencia limitada, puede causar un gran daño cuando se amplifica, logrando cobertura por parte de los medios de comunicación tradicionales, lo cual puede darle más credibilidad y permitirle acceso a una audiencia más grande.

- Afectar el mundo real
  Los actores maliciosos utilizan la desinformación en línea con el fin de afectar nuestro comportamiento en el mundo real. Por ejemplo, tratan de influir cómo votamos, incitan enfrentamientos físicos, e interrumpen los debates constructivos y la participación democrática.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alejen con las de un gobierno extranjero, se expresen mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
La desinformación se detiene con usted

Reconozca el riesgo

La desinformación se detiene con usted

Cuestione la fuente

Verifique quién realmente está detrás de la información y piense en lo que esa fuente gana al lograr que la gente le crea. La desinformación suele ser diseñada para parecer auténtica. Evalúe el contenido de manera crítica para discernir si es o no confiable.

Encuentre más información en www.cisa.gov/mdm-resource-library

Cuestione la fecha

¿Cuándo fue publicado? Contenido obsoleto o que no sea reciente puede estar fuera de contexto, lo que lo hace irrelevante para los acontecimientos actuales, y engañoso para quien lo lee en el presente.

Verifique la calidad

La desinformación suele encontrarse en sitios web de baja calidad. Busque señales como demasiados anuncios, patrocinadores de reputación cuestionable, mala ortografía, gramática y puntuación, y URLs sospechosas que imitan a sitios web de noticias legítimas.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
La desinformación se detiene con usted

Investiga el tema

Busque fuentes confiables para ver qué dicen acerca del tema en cuestión. Una búsqueda exhaustiva le permitirá asegurarse de estar compartiendo información precisa. No compartas el contenido si este no viene de una fuente creíble o si no puedes encontrar otra fuente creíble que lo confirme.

Encuentre más información en www.cisa.gov/mdm-resource-library

¿Es creíble la fuente? Mire la página “Acerca de” en el sitio web para ver si incluye información detallada, como sus valores, propiedad, ubicación, financiamiento e información de contacto.

¿Qué dicen las fuentes fidedignas? Busque el tema en sitios dignos de confianza. Si los hechos reportados por dichas fuentes creíbles no coinciden con el contenido que está revisando, no lo comparta.

¿Qué dicen los verificadores de hechos [fact checkers]? Es fácil creer cosas que confirman nuestros puntos de vista. Si una declaración parece demasiado buena como para ser cierta, verifique si alguna organización fiable, dedicada a la comprobación de hechos la ha evaluado y ha proporcionado un contexto adicional.

¿Su investigación es neutral? Asegúrese de utilizar un lenguaje de búsqueda imparcial y mantenga una actitud abierta hacia las pruebas que puedan contradecir sus creencias.

¿Reconoce otros puntos de vista? La mayoría de los temas candentes son complejos. Aunque todos los autores tienen su propio punto de vista, las fuentes creíbles reconocen otras perspectivas y proporcionarán un contexto basado en los hechos en torno al tema.

¿Provoca una reacción intensa? Si el contenido le hace sentir sorprendido, enfadado o triste, considere que precisamente ese sea el propósito. Lograr que usted responda de manera emocional y lo comparta sin confirmar su exactitud.

La desinformación se detiene con usted

Reconozca el riesgo

La desinformación se detiene con usted

Cuestiona la fuente

Investigue el tema

Piense antes de compartir un enlace

Hable con su entorno familiar y social (su círculo)

La desinformación se detiene con usted

Investiga el tema

Busque fuentes confiables para ver qué dicen acerca del tema en cuestión. Una búsqueda exhaustiva le permitirá asegurarse de estar compartiendo información precisa. No compartas el contenido si este no viene de una fuente creíble o si no puedes encontrar otra fuente creíble que lo confirme.

Encuentre más información en www.cisa.gov/mdm-resource-library

¿Es creíble la fuente? Mire la página “Acerca de” en el sitio web para ver si incluye información detallada, como sus valores, propiedad, ubicación, financiamiento e información de contacto.

¿Qué dicen las fuentes fidedignas? Busque el tema en sitios dignos de confianza. Si los hechos reportados por dichas fuentes creíbles no coinciden con el contenido que está revisando, no lo comparta.

¿Qué dicen los verificadores de hechos [fact checkers]? Es fácil creer cosas que confirman nuestros puntos de vista. Si una declaración parece demasiado buena como para ser cierta, verifique si alguna organización fiable, dedicada a la comprobación de hechos la ha evaluado y ha proporcionado un contexto adicional.

¿Su investigación es neutral? Asegúrese de utilizar un lenguaje de búsqueda imparcial y mantenga una actitud abierta hacia las pruebas que puedan contradecir sus creencias.

¿Reconoce otros puntos de vista? La mayoría de los temas candentes son complejos. Aunque todos los autores tienen su propio punto de vista, las fuentes creíbles reconocen otras perspectivas y proporcionarán un contexto basado en los hechos en torno al tema.

¿Provoca una reacción intensa? Si el contenido le hace sentir sorprendido, enfadado o triste, considere que precisamente ese sea el propósito. Lograr que usted responda de manera emocional y lo comparta sin confirmar su exactitud.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
La desinformación se detiene con usted

Conozca el riesgo
Compartir algo que ha visto en la internet puede parecer inofensivo en el momento, pero difundir desinformación puede deteriorar nuestra capacidad de mantener conversaciones importantes.

Conozca la fuente
Cuestione quién está realmente detrás del contenido. Evalúe críticamente la credibilidad del autor y la legitimidad del medio de comunicación comprobando los hechos, las fuentes que apoyan las afirmaciones, y la calidad del sitio web.

Conozca el contenido
Los titulares y subtítulos suelen ser exagerados para obtener una respuesta emocional. Tome el tiempo necesario para leer la publicación completamente y así determinar si refleja con exactitud el contenido.

Conozca los hechos
Investigue el tema en cuestión. Consulte fuentes fiables y verificadores de hechos [fact checkers] para comprobar las declaraciones, y asegúrese de que no han sido puestas fuera de contexto.

Conózcase a sí mismo
Pregúntese por qué comparte el contenido. La gente suele compartir contenido que confirma sus creencias, aunque sea falso. Si usted cree que no compartiría ese contenido en persona, entonces no lo haga en línea.

SHOCKING!

Piense antes de compartir un enlace
Dese un momento para dejar que sus emociones se enfríen y para preguntarse si sus sentimientos sobre el contenido están basados en hechos. La desinformación está diseñada para lograr que una reacción emocional intensa elude su pensamiento crítico. Usted puede interrumpir el ciclo de desinformación al darse un momento para investigar el contenido y decidir si compartirlo beneficia la conversación. Encuentre más información en www.cisa.gov/mdm-resource-library

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alineen con las de un gobierno extranjero, se expresen mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
La desinformación se detiene con usted

Reconozca el riesgo

La desinformación se detiene con usted

Cuestione la fuente

Investigue el tema

Piense antes de compartir un enlace

Hable con su entorno familiar y social [su círculo]

Hable con su entorno familiar y social [su círculo] Hable con su círculo social acerca de los riesgos de la desinformación y cómo pueden responder cuando la identifiquen. Probablemente no valga la pena involucrarse con cada pieza de desinformación, pero hablar de ello puede ayudar a detener su propagación. Investigue y comparta lo que sabe con sus amigos y familiares.

Encuentre más información en www.cisa.gov/mdm-resource-library

Esté preparado Asegúrese de haber investigado y de conocer los hechos antes de iniciar una conversación. Incluso si está convencido de que se trata de desinformación, revise la evidencia más reciente para estar seguro.

Decida si vale la pena Una vez que tenga los hechos, evalúe si vale la pena intervenir. ¿Ayudará su respuesta a la conversación o provocará un conflicto?

Responda en privado Si decide responder, intente hacerlo a través de un mensaje directo o incluso en una conversación fuera de internet [offline]. Los comentarios públicos pueden dar más visibilidad a la desinformación y hacer que las discusiones sean más conflictivas.

Céntrese en los hechos Si responde públicamente, comience con la verdad y no repita la declaración falsa. Proporcione enlaces a fuentes neutrales y fiables que contengan más información acerca del tema.

Sea respetuoso Intente comprender las creencias de su interlocutor para que este lo escuche. Puede ser difícil hacerles cambiar de actitud, pero mantenga la calma, la positividad y la empatía para que su mensaje sea recibido.

Sea un recurso Detener la desinformación cuando la vea es importante, pero puede ayudar a sus amigos y familiares a forjar resiliencia a la desinformación, al compartir proactivamente recursos y consejos para que ellos verifiquen los hechos por su propia cuenta.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Malign foreign actors, often hiding behind fake or automated accounts, use demonstrably false information, innuendo, and rumors to push or amplify their narratives. While many posts boil down to unconfirmable opinions, much of the information content falls into a few broad categories.

- **Innocent reporting errors** (misinformation) or satire and parody content can be repurposed and distributed maliciously with the intent to deceive.
- **Fake** content is created with the specific intent to dupe or incite audiences (disinformation).
- Facts are also used maliciously, and out of context, to improperly influence audiences (malinformation). This sort of content is sometimes the result of illicit cyber activity like spying or hacking and leaked through third parties.

Key Stakeholders: DOJ/FBI; State; Intelligence Community; State, Local, Territorial and Tribal Governments; Foreign Partners; Social Media Companies; Traditional Media Companies; Academia/Research; Think Tanks; and Philanthropy.
TAXONOMÍA DE LA INTERFERENCIA EXTRANJERA

INTERFERENCIA EXTRANJERA
Acciones maliciosas llevadas a cabo por gobiernos o agentes extranjeros diseñadas con el fin de sembrar discordia, manipular el discurso público, desacreditar el sistema electoral, sesgar el desarrollo político o desestabilizar los mercados con la intención de minar los intereses de los Estados Unidos y sus aliados.

ACTIVIDADES DE INFORMACIÓN
Las actividades emprendidas para moldear la opinión pública o debilitar confianza en la autenticidad de la información. El uso de medios de comunicación tanto nuevos como tradicionales con el fin de aumentar divisiones y fomentar la desazón en el país, a veces en coordinación con actividades cibernéticas ilícitas.

ABUSO DE NUEVOS MEDIOS DE COMUNICACIÓN
La manipulación de los proveedores de servicios de contenidos (CSPs, por sus siglas en inglés) para crear y difundir contenidos falsos o distorsionados en individuos o grupos predestinados. El abuso de nuevos medios permite que personas con influencia lleguen a una audiencia amplia de forma barata y rápida, lo que facilita que dichos adversarios intervengan y controlen las narrativas.

ABUSO DE LOS MEDIOS DE COMUNICACIÓN TRADICIONALES
El uso de medios de comunicación tradicionales para difundir información falsa o distorsionada, transmitir estrategicamente información robada o repetir las narrativas preferidas con el fin de manipular al público en general. Hacer que los medios de comunicación tradicionales provean información falsa o engañosa de manera intencional, lo cual extiende la propagación de narrativas extranjeras y debilita la credibilidad en la prensa.

ACTIVIDADES CIBERNÉTICAS
El jaqueo o secuestro de cuentas [hacking] puede beneficiar las actividades de información. Ayudan en operaciones de vigilancia o reconocimiento, y proporcionan oportunidades para ataques destructivos. El secuestro de cuentas y la destrucción de sitios de contacto público pueden ser utilizados para influir en la opinión pública. Los sistemas gubernamentales comprometidos (por ejemplo, los sistemas de votación, los repositorios de datos) pueden llevar a los ciudadanos a cuestionar la seguridad de la información proporcionada al gobierno.

¿QUÉ TIPO DE INFORMACIÓN SE UTILIZA?
Los actores extranjeros malignos, a menudo se esconden detrás de cuentas falsas o automatizadas, utilizan información indudablemente falsa, hacen insinuaciones y generan rumores que promueven o extienden la información. Aunque muchos mensajes se reducen a ser opiniones no confirmadas, gran parte del contenido informativo se clasifica en unas cuantas categorías generales. Los errores inocentes en el reporte de la información (información errónea o equivocada) o las sátiras y parodias pueden ser reutilizados y distribuidos maliciosamente con la intención de engañar. A menudo, los contenidos "falsos" se crean con la intención específica de engañar o incurrir al público (desinformación).

Participantes interesados [Stakeholders]: DOJ/FBI; el Estado; la comunidad de inteligencia; los gobiernos estatales, locales, territoriales y tribales; aliados extranjeros; empresas de redes sociales; empresas de medios de comunicación tradicionales; academia/investigadores; laboratorios de ideas; y filántropos.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Information manipulation is undertaken to shape public opinion or undermine trust in the authenticity of information. It includes use of **new and traditional media** to amplify divides and foment unrest in the homeland, sometimes coordinated with illicit **cyber activities**.

### New Media Abuse

Manipulating content service providers (CSPs) to create and amplify false and distorted content for targeted individuals or groups.

New media abuse allows influencers to reach a large audience cheaply and quickly, allowing bad actors to commandeer and control narratives.

### Traditional Media Abuse

Using traditional media outlets to report false or distorted information, strategically leak stolen information, or repeat preferred narratives in order to manipulate a general public.

Purposefully causing traditional media sources to report false or misleading information increases the spread of foreign-pushed narratives and undermines the credibility of the press.

### Cyber Activities

Hacking may benefit information manipulation. Hackers assist in surveillance or reconnaissance and provide opportunities for destructive attacks. Hijacking accounts and defacing public-facing websites can be used to influence public opinion.

Compromised government systems (e.g., voting systems, data repositories) can lead to citizens questioning the security of the information they provide to the government.

Misinformation, disinformation, and malinformation (MDM) make up what CISA defines as “information activities.” Bad actors use MDM to cause chaos, confusion, and division. These malign actors are seeking to interfere with and undermine our democratic institutions and national cohesiveness.

- **Misinformation** misleads. It is false, but not created or shared with the intention of causing harm.
- **Disinformation** deceives. It is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** sabotages. It is based on fact, but used out of context to mislead, harm, or manipulate.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt American life and the infrastructure that underlies it. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
La manipulación de la información se lleva a cabo con el fin de modificar la opinión pública o de debilitar la confianza en la autenticidad de la información. Esto incluye el uso de los medios de comunicación nuevos y tradicionales para amplificar diferencias y provocar disturbios a nivel nacional; en ocasiones de manera coordinada con actividades cibernéticas ilícitas.

**Abuso de los nuevos medios de comunicación**

Mediante la manipulación a los proveedores de servicios de contenido (CSPs, por sus siglas en inglés) con el fin de crear y amplificar contenidos falsos y distorsionados para individuos o grupos predeterminados.

El abuso de los nuevos medios les permite a personas influyentes en redes sociales, a alcanzar una gran audiencia de manera barata y rápida, lo cual permite a los actores maliciosos apoderarse y tomar control de las narrativas.

**Abuso de los medios tradicionales**

Al utilizar los medios de comunicación tradicionales para transmitir información falsa o distorsionada, filtrar estratégicamente información robada o repetir narrativas preferidas con el fin de manipular al público en general.

Lograr que los medios de comunicación tradicionales diseminen de manera intencional información falsa o engañosa, aumenta la difusión de las narrativas impulsadas por fuentes foráneas y disminuye la credibilidad de la prensa.

La información errónea, la desinformación y la información maliciosa (MDM, por sus siglas en inglés) constituyen lo que CISA define como "actividades de información". Los actores maliciosos utilizan MDM para generar caos, confusión y división. Estos agentes criminales buscan interferir y debilitar nuestras instituciones democráticas y la unión nacional.

La información errónea o equivocada [Misinformation] confunde. Es falsa, pero no es creada o compartida con la intención de causar daño.

La desinformación [Disinformation] engaña. Es creada deliberadamente para engañar, dañar o manipular a una persona, grupo social, organización o país.

La información maliciosa [Malinformation] sabotea. Es basada en hechos reales, pero se utiliza fuera de contexto con el fin de engañar, perjudicar o manipular.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alineen con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Mis-, Dis-, and Malinformation
Planning and Incident Response Guide for Election Officials

OVERVIEW

State, local, tribal, and territorial (SLTT) election officials can take proactive steps to prepare for and respond to the threats of misinformation, disinformation, and malinformation (MDM). This guide is intended to help election officials understand, prepare for, and respond to MDM threats that may impact the ability to conduct elections.

WHAT IS MDM?

CISA defines mis-, dis-, and malinformation (MDM) as “information activities.” This type of content is referred to as either domestic or foreign influence depending on where it originates.

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.

Combined with a lack of public understanding of election processes, the changing landscape of technology and communications creates new risk and evolving vectors for the spread of MDM. This includes inaccurate information about the election process, unsubstantiated rumors, and incomplete or false reporting of results.

WHERE DOES MDM COME FROM?

MDM can originate from a variety of sources across digital, social, and traditional media, and new MDM topics emerge continuously. Foreign actors have used MDM to target American voters for decades. MDM also may originate from domestic sources aiming to sow divisions and reduce national cohesion. Foreign and domestic actors can use MDM campaigns to cause anxiety, fear, and confusion. These actors are ultimately seeking to interfere with and undermine our democratic institutions.

Even MDM that is not directly related to elections can have an impact on the election process, reducing voter confidence and trust. Election infrastructure related MDM occurs year-round — it is not just a concern in the months prior to Election Day. False narratives erode trust and pose a threat to democratic transitions, especially, but not limited to, narratives around election processes and the validity of election outcomes.

*Definitions adapted from CISA’s MDM Resource Library. For an overview of tactics used by disinformation campaigns—such as manipulating audio and videos, conducting forgeries, and developing proxy websites in order to undermine public confidence and sow confusion—see Tools of Disinformation: Inauthentic Content.*

---

1 Joint Cybersecurity Advisory: AA20-296B Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems
HOW DOES MDM IMPACT ELECTION SECURITY?

Depending on the narrative, MDM can have various impacts on election security. Categories may include:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Description</th>
<th>Example (from CISA’s Rumor Control page)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Procedural Interference</strong></td>
<td>Narratives or content related to election procedures that cause confusion and interfere with officials’ ability to smoothly administer an election.</td>
<td>✔️ Reality: Safeguards are in place to prevent home-printed or photocopied mail-in ballots from being counted. ✗ Rumor: A malicious actor can easily defraud an election by printing and sending in extra mail-in ballots.</td>
</tr>
<tr>
<td><strong>Participation Interference</strong></td>
<td>Content that might intimidate or deter voters from participating in the election process.</td>
<td>✔️ Reality: Voters are protected by state and federal law from threats or intimidation at the polls, including from election observers. ✗ Rumor: Observers in the polling place are permitted to intimidate voters, campaign, and interfere with voting.</td>
</tr>
<tr>
<td><strong>Delegitimization of Election Results</strong></td>
<td>Narratives or content that delegitimizes election results or sows distrust in the integrity of the process based on false or misleading claims.</td>
<td>✔️ Reality: Election results reporting may occur more slowly than some voters expect. This alone does not indicate a problem with the counting process or results, or that there are issues affecting the integrity of the election. Official results are not certified until all validly cast ballots have been counted, including ballots that are legally counted after election night. ✗ Rumor: If results as reported on election night change over the ensuing days or weeks, the process is hacked or compromised, so I can’t trust the results.</td>
</tr>
<tr>
<td><strong>Personnel Security</strong></td>
<td>Narratives or content that falsely claims election officials or poll workers are the “bad actor” attempting to interfere in election results or processes.</td>
<td>✔️ Reality: Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results. ✗ Rumor: A bad actor could change election results without detection.</td>
</tr>
</tbody>
</table>

RESPONDING TO MDM

In today’s media and information environment, election officials must play a proactive role in responding to MDM. While each MDM narrative will differ, leveraging the TRUST model for MDM response can help reduce risk and protect voters.

**T** Tell Your Story
**R** Ready Your Team
**U** Understand and Assess MDM
**S** Strategize Response
**T** Track Outcomes

It is important to acknowledge the opportunities and limitations of government-led MDM intervention—particularly where distrust of government may be fueling the narrative. Focus responses where your team has evidence, expertise, or authority to counter the MDM. Also, recruit trusted community partners to amplify your messaging.

Categories adapted from the Election Integrity Project’s (EIP) final report on misinformation and the 2020 election (Revised March 2021).
1. TELL YOUR STORY

Public resilience is increased as your team builds relationships with voters and stakeholders. Educate your communities about election processes and MDM-related threats before they occur.

**Educate voters:** Educating constituents on how to engage in the electoral process and promoting civic learning is critical to countering MDM. Communicating clearly in tone, language, and medium, as well as leveraging credible voices your audience trusts will help reach and engage constituents to convey information about important dates/deadlines, polling locations, processes for voting change, and where to find trusted information about elections and election results.

**Pre-bunk MDM:** Providing constituents with information and resources before MDM activity emerges better equips Americans to identify and question false narratives. In some cases, by leveraging insights from your staff, you can anticipate where MDM narratives may arise, such as how election officials secure elections through the use of post-election audits and similar safeguards. Addressing these topics with voters in advance of elections and explaining how they are used in MDM narratives can increase resiliency and confidence among voters.

**Build media relationships:** Reach out to local newspaper, radio, television, podcasts and other media outlets to build working relationships before election cycles. Invite them to learn more about how election processes secure election results and key voter education details. Make sure they have a contact in your office. Establishing working relationships with media outlets and journalists helps quickly and pre-emptively debunk or expose MDM activity. It can also help inform accurate reporting around elections, limiting the propagation of misinformation.

2. READY YOUR TEAM

The effectiveness of your response will depend on how much preparation is conducted internally ahead of MDM activity.

**Establish your response protocol:** Establish a clear procedure for responding to MDM and educate team members about the process.

- Understand the procedures for reporting or flagging potential online MDM to social media platforms often used by your constituents. Consult with your legal counsel to ensure you respect constitutional rights and privacy protections and abide by any legal restrictions.
- The Center for Internet Security (CIS) was established to support the cybersecurity needs of the election subsector. The CIS can be leveraged to report real-time MDM via email at misinformation@cisecurity.org. Be sure to include links and screenshots, as well as details on the misinformation and your jurisdiction.
- Determine internal roles and responsibilities, including an escalation process within your jurisdiction to ensure the right teams are talking to one another while responding to MDM activity. Be clear that this is not “just” a communications issue; it requires engagement from across departments to ensure responses are accurate and understandable.
- Designate an individual to be responsible for ensuring this process is established, updated, and shared both internally and with relevant stakeholders at the local, state, tribal, territorial, and federal levels — including your CISA Regional Office.
- Hold or participate in tabletop exercises to increase your team’s awareness and understanding of MDM threats, evaluate your overall preparedness, identify deficiencies in your incident response plan, and clarify roles and responsibilities during an incident. CISA can assist in development and execution of these exercises, or CISA’s Tabletop in a Box resource can help you talk through possible scenarios with your team and stakeholders as well.

**Build credible information-sharing channels:** MDM can thrive in the absence of easily accessible, credible information. Ensure your agency’s website, social media accounts, and other information channels are up to date and active so you can directly respond to MDM. This can help your community have confidence that the messages your organizations disseminate are authoritative and you can further build public confidence in election administration.

Media literacy includes verifying sources, seeking alternative viewpoints, and finding trusted sources of information. The National Association for Media Literacy Education has members in every state that can work with election officials to develop media literacy content. CISA’s Resilience Series graphic novels are a great example of a resource aimed at developing media literacy and critical thinking to counter disinformation.
• **Register your website for a .gov address** so the public does not have to guess whether your websites and emails are genuine. CISA makes .gov domains available solely to U.S.-based government organizations and publicly controlled entities **without a fee**.

• Many social platforms (e.g., Facebook, Twitter) will also allow government organizations and users to apply for verification badges. Local election officials should reach out to their state for more information on how to get their accounts verified.

• Consider pre-bunking MDM on your website by responding to common questions relevant to your responsibilities. The Rumor Control Start-Up Guide provides further guidance on establishing this webpage and how to assess which topics to include.

**Prepare for incoming questions:** Ensure your office has methods for fielding public feedback and questions, including **being able to handle a large influx of calls or messages.** Consider creating a shared voicemail and email inbox so that no one person becomes overwhelmed, with a log to track inquiries and responses. These mailboxes should be regularly checked and there should be an established process for determining who will respond. This will enable your team to both uncover MDM that is circulating and keep systems and phone lines functioning during critical periods of MDM activity. Ensure staff are aware of your office’s procedures for reporting threats and harassment, and if possible, rotate responsibilities for responding to calls and emails to avoid burnout.

### 3. UNDERSTAND & ASSESS

**It is important to understand, to your best ability, the full nature and scope of the MDM activity.**

**Identify MDM activity:** While every election jurisdiction has different resources and capabilities, you should establish a system for identifying and evaluating MDM in your office. Determine if it is appropriate for your office to engage with outside organizations or tools to better understand the risk landscape and monitor for MDM, including your technical systems provider. Monitoring may be proactive, via analytic tools, or reactive, through public feedback channels.

- **Identify and continuously update a list of key elections-related processes and issues vulnerable to MDM.** Whether they are short-term trends or long-term narratives. Ensure all members of your office have access to this list and feel comfortable contributing to it. The person responding to inquiries will therefore have a good sense of what topics people are asking about, and who to contact for answers, even if they don’t know how to answer the question themselves.

- **Identify the channels that constituents use to receive information.** MDM content can spread through numerous means, including social media, mainstream media, word of mouth, online forums, messaging apps, and emails. Remember that MDM narratives also often move between channels, so content that appears on one platform may also emerge elsewhere.

- For the high priority topics on your list, including those you worked to pre-bunk, **you may want to take a more proactive approach to monitoring for MDM narratives, to the extent permitted by law.** Consider using analytic tools to search for keywords related to MDM content. Evaluate content reach (how many people are seeing it), engagement (how many people are liking, sharing, or reacting to the content), how many channels it is present on, and whether it has reached mainstream media. Consult with your legal counsel to determine what monitoring is permissible under law and platforms terms of service.

- **Leverage publicly available analytical tools,** such as those recommended by the RAND Corporation’s Fight Disinformation at Home resource, which can help you gain a greater awareness of the information ecosystem.
**Assess the Risk**: The team should identify what plausible risks are associated with MDM narratives and how they may impact election infrastructure. Mapping out existing MDM narratives and their impact on elections infrastructure will help the team be prepared for the online and offline consequences and impact to elections infrastructure.

**4. STRATEGIZE RESPONSE**

Once you have identified MDM, it is important to craft an effective response, taking into account how the information environment and related technology may evolve.

**Determine your response**: Based on your risk assessment, prioritize which MDM narratives to respond to. In crafting your communications strategy, consider both timing and medium of response.

- **Not all MDM activity warrants an immediate response.**
  Deciding which rumors make the cut is an exercise of an organization’s judgement — and that judgement may change as MDM narratives evolve and community response changes.

- **Understand your audience** for the MDM intervention. Your community isn’t homogeneous, and your audience will change depending on the message you are trying to convey and the medium you use. Adapt your messaging to the audiences you are trying to reach, such as new voters, veterans, individuals in specific geographic regions, or those who speak other languages.

**Apply communications best practices**: In a crisis, specific tactics and language can help build the credibility of your response and reassure voters. Tactics may also look different based on the activity and the audience. A communications strategy might include **social media, radio, local news, or other media platforms** to engage constituents.

- Identify where your audience receives information and, if possible and advisable, establish a presence on these platforms. It will likely not be realistic for your office to actively use every platform. Focus on using a smaller number of platforms effectively to establish your handle as a trusted source of information.
- Ensure you have the facts before responding.
- State facts first, rather than repeating a falsehood in your headline.
- Be careful not to amplify the source of the MDM by linking to it directly or sharing original images or videos. If referencing an image, use a screenshot with a text overlay that explains the image is inauthentic or misleading. Consider what privacy protections are necessary for all media shared.
- Consider the length of your response. Shorter statements are more easily digestible and can be helpful when the MDM is easily disproven.
- You do not need to respond to each incident of MDM individually. Point back to your office’s previous posts, statements or work if MDM recirculates. Inconsistent messaging can create credibility problems.
- Leverage partnerships and trusted community messengers to counter MDM narratives. **Repetition and consistency are key.** Conveying the same message through multiple mediums and platforms will help reach the broadest audience possible.

---

Election officials across the country are combating election-related MDM.

- The Colorado Secretary of State’s office conducted social media and digital outreach to voters and set up a [website](https://example.com) to educate on the threat misinformation and respond to MDM narratives.
- The Kentucky Secretary of State’s office launched a [Rumor Control page](https://example.com) on their website to counter MDM narratives around elections.
- The Wisconsin Elections Commission established a [designated FAQ page](https://example.com) to address voter questions about the 2020 election.
- The Maricopa County, Arizona, Elections Department launched a [website](https://example.com) to address questions and misconceptions about the 2020 election and has engaged in rumor control efforts across social media.
After your response, evaluate the continued prevalence of MDM and evaluate ways to adjust processes moving forward.

**Manage and monitor repercussions:** While MDM narratives may be effectively addressed or accounts spreading disinformation may be removed, manipulators will often find ways to circumvent these changes. Creating new accounts, adapting coded language, altering audio/visual material, and iterating on narratives already identified as objectionable by platforms are all possible adjustments deployed to increase MDM efficacy. It is important to monitor the MDM environment, as resources allow, to remain aware of changes and adjust response tactics accordingly.

**Reassess response strategy:** Following an MDM response effort, revisit and reassess your process, including your list of priority topics for media monitoring. In the current information environment, threats are constantly evolving, and the locations, mediums, and narratives of MDM are changing as well.
DISCLAIMER

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) PRODUCED THIS GRAPHIC NOVEL TO HIGHLIGHT TACTICS USED BY FOREIGN GOVERNMENT-BACKED DISINFORMATION CAMPAIGNS THAT SEEK TO DISRUPT AMERICAN LIFE AND THE INFRASTRUCTURE THAT UNDERLIES IT. CISA’S PUBLICATION OF INFORMATION MATERIALS ABOUT THIS ISSUE ARE INTENDED FOR PUBLIC AWARENESS, AND ARE NOT INTENDED TO RESTRICT, DIMINISH, OR DEMEAN ANY PERSON’S RIGHT TO HOLD AND EXPRESS ANY OPINION OR BELIEF, INCLUDING OPINIONS OR BELIEFS THAT ALIGN WITH THOSE OF A FOREIGN GOVERNMENT. ARE EXPRESSED BY A FOREIGN GOVERNMENT-BACKED CAMPAIGN, OR DISSSENT FROM THE MAJORITY. CISA CELEBRATES THE FIRST AMENDMENT RIGHTS OF ALL U.S. PERSONS WITHOUT RESTRICTION, WHILE BASED ON ACTUAL NATION-STATE ADVERSARY ACTIVITY, THE STORY AND ALL NAMES, CHARACTERS, ORGANIZATIONS, AND INCIDENTS Portrayed IN THIS PRODUCTION ARE FICTITIOUS.
C’MON SWEETHEART! IS THAT ALL YOU BOY FOR YOUR OLD MAN? YOU EARNED THIS! YOU’RE THE FIRST OF US TO GET TO COLLEGE, LET ALONE ROAD SCHOOL.

NOW STOP ALREADY! YOU KNOW WHAT MOM WOULD HAVE SAID.

C’SITE, THIS IS IT... Gotta go, Dad.

F3 148.51
VOLUME

C’MON SWEETHEART! IS THAT ALL YOU BOY FOR YOUR OLD MAN? YOU EARNED THIS! YOU’RE THE FIRST OF US TO GET TO COLLEGE, LET ALONE ROAD SCHOOL.

NOW STOP ALREADY! YOU KNOW WHAT MOM WOULD HAVE SAID.

SPECIAL BULLETIN AS COVID-19 NUMBERS CONTINUE TO RISE ACROSS THE NATION.

SO MUCH HAS CHANGED SO QUICKLY! FIRST MOM AND NOW THIS... WELL, AT LEAST THE SUN IS OUT.

COULD YOU PLEASE PUT ON YOUR MASK? THERE ARE HUNDREDS OF PEOPLE HERE! AND... I AM NOT READY FOR YOU TO BECOME A STATISTIC!
Going to get out of your hair...

Thank you!

Seriously?

You know your mother would have been robbing if she was with us...

What is it, Dad? You do realize that I am a woman in my mid twenties...

OK! You got me! Got distracted and wasn’t thinking. Thanks for the reminder. See you later this evening!

Now, where is my mask?
"YOU HAVE NO NEW MESSAGES."

MORNING, UM!

SURE THING!...SURE THE? JUST A FEW MILES OUT...LEAVE TAKE A LOOK...

I'M ON IT, CHEF!

I HOPE THIS HAS NOTHING TO DO WITH ALL THAT CRAZY CONSPIRACY STUFF AROUND 5G AND ITS NONSENSE LINK TO THE VIRUS...HOW CAN PEOPLE BELIEVE THAT STUFF??

OH NO! POISON! IT SOUNDS LIKE THERE'S A FIRE! I'M CALLING 911...GET OVER THERE ASAP!

YOU HAVE 5 MINUTES TO DESTINATION...THEN LEFT IN...

YOU HAVE 3 MINUTES TO DESTINATION...

ARRIVING AT DESTINATION....
SWOOOOOOO! SAW? SWOOOOO! I AM THAT NASTY DISEASE WITH YOU!

IT'S QUIET. NO ONE'S IN SIGHT. OVER!

LIGHT IT UP!

HEY! QUIT THAT JACKET! PACK UP AND LET'S CLEAR OUT. NOW!
HEY! STOP!

SON OF A --

THUD!

LET GO OF ME. LET ME AT HIM!

GRAB A HOLD OF YOURSELF. I KNOW YOU ARE ANGRY ABOUT HOW THESE TOWERS ARE HURTING US, BUT WE CAN'T HURT OTHER PEOPLE.

NO, PLEASE!

ARRRGHHH...

ARE WE CLEAR?

YES.
LET'S GET THIS BEAST UNDER CONTROL!

ALL CLEAR. WE HAD TO WANDER A BIT. WE HAD SOME COMPANY, BUT HE WOULDN'T BE ANY TROUBLE.

NO, WILLIAMS, CAN YOU HEAR ME? SIR?

BENTLEY...

I'M REALLY SORRY TO HAVE TO DO THIS NOW, BUT DO YOU REMEMBER ANYTHING ELSE ABOUT THE ATTACKERS, OR THE VEHICLES...

I REMEMBER THE PLATES: E33...
New, sweetie.

Omg, are you ok?

Who could have done this to you?

Omg, dad...

Oh, ooo, dad...

Miss Williams, stay strong, we'll do our best to find whoever is responsible.

Oh, ooo, dad...

You're all I have left.
SEPTEMBER 2020 – THE NEXT DAY AT THE UNIVERSITY...

THAT’S WEIRD. THERE SEEMS TO BE A LINK BETWEEN 5G AND COVID IN THESE COMMENTS.

WHY TRY TO LINK 5G TECHNOLOGY TO THE VACCINE? WE DON’T HAVE A VACCINE YET. THERE CAN’T BE ANY RESEARCH TO SUPPORT THIS CLAIM. IT TAKES A LONG TIME TO DO THOSE STUDIES.

STOP 5G CELL TOWER DEPLOYMENT IN MICHIGAN

5G Attack Michigan

52,063 have signed, let’s get 75,000.

NONE OF THE PEOPLE COMMENTING ON THE VACCINE’S LINKS TO 5G WERE TALKING TO ONE ANOTHER! THERE IS JUST NOT ENOUGH ON THESE PEOPLE TO SUGGEST THAT THEY ARE REAL PEOPLE.

HAM... LOOKS A BIT STRANGE?! SO MANY RANDOM COMMENTS. SOME DON’T LOOK LIKE THEY HAVE BEEN MADE BY A REAL PERSON.

I WONDER IF THERE ARE REAL

THIS SEEMS LIKE THE RESULT OF A MALICIOUS CYBER CAMPAIGN BUT ORCHESTRATED BY WHOM? I NEED TO LOOK INTO THIS SOME MORE... HMM...

UPDATES

Abigail Palmer, 2 hours ago
5G is going to destroy our immunity. The radiowaves from 5G will make it impossible to resist the virus! This is all an experiment on humanity.

Tony S., 2 hours ago
THIS IS A DANGEROUS TENDENCY. IT HAS TO STOP!
That’s odd. None of them exist in places you would expect outside of the platforms. Digital ghosts?
A few days later, Frank is discharged from the hospital and is back home.

I'm fine, kiddo. Have I mentioned how proud I am of you for all the work you have been doing on disproving the link between 5G and COVID?

That's right! People need to understand that 5G is simply the fifth generation of wireless technology. Right now, most of us are using 3G or 4G networks for our mobile phones and 5G is the new technology that will make things faster.

Hey dad, I'm running a bit short on time, but I wanted to check in on you.

Thanks, old pal. I can't believe how many people think that there is a link and have been attacking 5G towers. People don't realize that this is disinformation.

I get that dad, because if you buy so many outdated new technologies, it takes a few weeks on social media shared by a celebrity or someone they know to become an issue. Because of the disinformation, people believe that 5G towers are going to make them sick, and that 5G is somehow linked to the corona virus, but I don't see how that could be true.

It's very easy to become susceptible to fake news today.

Disinformation. Old disinformation. Information that is not true and is being spread. It's easy to mix up the technology.

There are some traces online, but they never talk to one another. They never seem to post a comment and have a discussion with one another on very obviously staged deals. Something funny's going on.
People also are not fully aware of what 5G is all about.

This infrastructure then connects to our phones and laptops, which means we can do things like download movies faster, like you said. So only carries data. And physical things like viruses or bacteria cannot travel in radio waves or telephone networks. It viruses are completely different from biological viruses, which cannot travel this way.

If this sounds weird, it could just out of hand claiming that 5G towers are linked to the virus is dangerous. It's wrong, and those claims make inside worse attacks like the one on you, old.

That is part of the problem.

People believe what they read on social media. If I don't know better, I would probably believe something.

If my friends posted it on these feeds, no one takes the time to check this stuff anyway.
TAP! TAP! TAP!

SO, THE DATA SHOWS THAT A NUMBER OF HACKERS ARE SIGNING THE PETITION SIMULTANEOUSLY AT CERTAIN TIME INTERVALS OF 3:30PM, 5:30PM, AND 8:30PM EASTERN TIME. THAT IS A TELL...

THE ONLY THING THAT MAKES SENSE IS THAT THIS... THIS IS A BOT FARM.

REMEMBERING COLLEEN, HER FRIEND FROM GRAD SCHOOL, WE CALL HER FOR THE CONTACT DETAILS OF A LAWYER THEY HAD PREVIOUSLY MET, WHO MAY BE ABLE TO HELP.

COLLEEN, CAN YOU GIVE ME THE NAME OF THAT LAWYER? WE MET HER ONCE? THE ONE WHO KNOWS A LOT ABOUT CYBER LAW AND DISINFORMATION. THANKS!

WOW, SHE SEEMS LIKE THE RIGHT PERSON. SHE PRACTICES CYBER LAW AND... HERE'S HER NUMBER. MAYBE SHE CAN HELP.

Hi, this is Ava Williams from the University of Ann Arbor's Journalism Department. We previously met...

NOT INTERESTED!

NOT WAIT...
SONIKA ADJUSTS HER MASK AS SHE ENTERS THE PUBLIC SECTION OF THE AIRPORT.

CAN I CALL YOU AFTER YOU LAND? IT'S URGENT, I THINK I HAVE DISCOVERED A TRANSPORTATION CAMPAIGN ONLINE THAT COULD RESULT IN A LOT OF PEOPLE GETTING HURT.

PING... LET ME CALL YOU BACK AS SOON AS I LAND IN DC.

COAST 3 COAST AIRLINES FLIGHT NUMBER WITH NOW BOARDING AT GATE 10.

Ladies and gentlemen, welcome to Washington Dulles International Airport. The local time is 4:55 PM.
YOU DON'T WASTE MUCH TIME DO YOU?

SORRY, I WAS TRACKING THE FLIGHT ONLINE...

THE AFTERNOON TRANSITIONS INTO LATE EVENING AS BONNIE MAKES HER WAY TO THE TAI.

OF COURSE, I'M GLAD TO HELP IF IT MAY AID, WHY ARE YOU DOING THAT? IF IT'S A STORY YOU ARE CHASING DOWN...

THANK YOU SO MUCH. I WOULDN'T HAVE CALLED IF THIS WASN'T URGENT. MY FATHER IS ALREADY IN THE HOSPITAL BECAUSE OF THIS WHOLE THING. I'VE BEEN MEANING TO ASK YOU A QUESTION ABOUT THESE LIES. IT MUST BE SOMETHING THAT CAN BE DONE TO FIGHT ALL THE MISINFORMATION FLYING AROUND.

AT FIRST IT WAS PERSONAL, BECAUSE MY FATHER WAS HURT, BUT I REALIZED THIS IS SO MUCH LARGER THAN THE TWO OF US.

MY FATHER WORKS AT A COMPANY THAT MAINTAINS 5G INFRASTRUCTURE IN MICHIGAN. HE WAS ATTACKED BY A GROUP OF ARMED MEN, WHO HE CAME TO A TOWER, I DID SOME INTERNET RESEARCH AND FOUND A PETITION ON CHANGE.ORG TO HELP STOP THE CONSTRUCTION OF A TOWER THAT WANTED 5G TOWER CONSTRUCTION TO BE STOPPED IN MICHIGAN.

THE PERSON WHO STARTED IT WAS TRYING TO FOCUS ON THE RADIO WAVES AND THEIR IMPACT ON OUR HEALTH, BUT THE PETITION SEEMS TO HAVE BEEN HACKED AND LINKED TO THE COVID-19 VIRUS. IT HAD A LITTLE OVER 50,000 SIGNATURES AND IT SEEMS THAT ABOUT 10 PERCENT COME FROM WHAT LOOKS LIKE 5G BOYCOTT SITES. SOMEONE IS PULLING THE STRINGS ON THIS SITUATION.

SHOCKING. WHAT SOME OF THESE OUTCRY ARE ABLE TO DO WITH JUST A FEW LINES OF CODE. I AM SURE THAT YOU NOW UNDERSTAND THE DIFFERENCE BETWEEN A SERIOUS CRIME AND MISINFORMATION. THIS APPEARS TO BE A CLASSIC MISINFORMATION CAMPAIGN, WHERE FALSE INFORMATION IS BEING USED TO MISLEAD PEOPLE AND MANIPULATE THE MEDIA.

SHOCKING. INITIATED BY SOMEONE WHOSE MISSION IS TO AID PEOPLE AND MANIPULATE THE MEDIA.

THIS IS REALLY WHY I NEED YOUR HELP TO UNDERSTAND IF THERE IS ANY WAY TO SLOW DOWN THE PETITION AND - TO BE BLUNT - EXPOSE THE BOY FARM OWNERS TO JUSTICE!

IT'S NOT THAT SIMPLE, ESPECIALLY SINCE SCOTT FARMS ARE OVERSEAS. WHILE WE HAVE BEEN TALKING, I TEXTED SOMEONE WHO IS INTERESTED IN HELPING YOU, HIS GROUP LIVES TO KEEP A LOW PROFILE, BUT YOU SHOULD BE HEARING FROM THEM ANY MOMENT NOW.

WANT TO LISTEN AND AS I SAID, I WILL SEND SOMETHING YOUR WAY THAT MIGHT BE ABLE TO HELP OUT A LITTLE MORE THAN I CAN STAY SAFE AND SOONENIGHT.

YES. OF COURSE. THANKS FOR LISTENING. I REALLY APPRECIATE YOU TAKING THE TIME TO HELP ME OUT.

AND THANKS SO MUCH FOR MENTIONING ME TO YOUR CONTACT. I LOOK FORWARD TO HEARING FROM YOU.
CREATE YOUR BLOCKWRLD ACCOUNT
You'll get a free code for BLOCKWRLD Free Edition once you set up a new account. If you already have one, LOGIN.

Email address:
awarfarmz@email.com

Repeat email address:
awarfarmz@email.com

Password:

Repeat password:

THE GROUP SEEMED OUT OF TOUCH WITH MOVES QUICKLY LOOKS LIKE THIS EMAIL IS FROM THEM.

secret library blockwrlD

AVAlanche

AAA'S 3D AVATAR CLIMBS THE STAIRS OF THE SECRET LIBRARY.

She tours around this vast facility, looking at other 3D counterparts as well.

secret library blockwrlD

CHAT BOX

I am a fool with a heart but no brains.
I am a fool with a heart but no brains

And beauty will save the world. Here to meet you Ava.

Let’s talk on this link. https://chairman.123456/secret.php

Don’t worry. It’s secure and can’t be traced back to either of us.

Avalanche

And you are a fool with brains but no heart: and we’re both unhappy, and we both suffer.

Search for: "Beauty will save the world". This is one of Dostoevsky’s most often quoted sentences, but few know precisely what it means.

Hello...

Hi... I’m not looking for any trouble!

Wait... How do you know my father?

My father works for...

Sunders like you really are in the know. Can you please tell me then... why on earth was the 58 tower attacked? I have found evidence of a linked disinformation campaign online. You must know about it already!

The local 58 company and my father was jumped by some assassins who attacked a 58 tower! Let’s skip to what you need. Ava. We don’t have much time!

Someone hijacked the petition and linked it to the coronavirus vaccine. It has accumulated 5,000 signatures asking which are bots. I guess the latter save it the traction it needed.

Send us the data. We haven’t been too focused on Michigan as of yet. This thing is bigger than you know. Other parts of the U.S. and other countries— including U.S. allies— are experiencing similar problems.

5 minutes later...

I’m really impressed by the analysis, Ava. Let’s compare notes! Sending you a file now...

We have been following the news, Ava. I know what happened with your father, not much we don’t know about! How can we help you?

I am a fool with a heart but no brains.

And beauty will save the world.
YOU GUYS SEEM TO HAVE A LOT OF DATA! HOW ON EARTH DO YOU MANAGE TO DO ALL THAT?

WE HAVE THE VERY BEST WORKING WITH THE U.S. I'M QUITE CERTAIN THAT THE RUSSIANS HAVE BEEN TRYING TO DEFEAT US FROM THE INSIDE OUT.

AND THEY DON'T NEED GUNS OR WEAPONS OF MASS DESTRUCTION TO PUT US ON THE PATH OF DESTRUCTION. THEY JUST NEED YOUR SOCIAL MEDIA DATA.

WE ARE FACING AN ALARMING TREND WHERE THE INTEGITY OF THE DATA WE ARE PUBLISHING IS IN DANGER.

A MAJOR CHALLENGE FACING US TODAY IS THE INTEGRITY OF THE DATA WE ARE PUBLISHING. WITHOUT IT, THE SOCIAL MEDIA POST OR REALITY HAS THE DISINFORMATION PANDEMIC TO WORRY ABOUT.

MOSCOW IS SUPPLYING A LOT OF NONSENSE TO A MULTITUDE OF ANTI-VACCINATION PETITIONS AND BOYCOTTS. IT IS A TIDYING TRICK OF THE TRADE AND IT IS GOING TO BLOW UP IN OUR FACES UNLESS WE DO SOMETHING ABOUT IT!

WHAT SOCIAL NETWORK EVEN HAS THE FORCES TO DETECT AND CHECK THESE EVENTS? THE VELOCITY OF NEWS OVERTAKES HUMAN INTERVENTION AND THE AS WE CAN HOUSEHOLD, BUT IS NOT QUITE THERE YET.

I HELP YOU, I JUST DON'T KNOW WHAT I CAN DO TO HELP!

HAS THERE BEEN ANY RESEARCH ON DATA THAT MAY HELP US DIFFERENTIATE BETWEEN THE ALGORITHMIC RESPONDED TO BY THOSE IN THE TRENDS?

YOU NOTICED A PRETTY SHOCKING TREND ON THAT PETITION. IT'S OPENING WAYS MORE COMPLICATED AND IT'S A PATTERN THAT THE HUMAN EYE OFTEN MISSES. ARE YOU SOMETIMES BORED, SHALL WE SAY, GOING THE EXTRA MILE?

ALSO, ONE OF OUR BOYS AT NSA FOUND THAT A DOT NEVER REACTS TO ANOTHER DOT'S COMMENT.

THIS IS BIGGER THAN ANYTHING I COULD HAVE ANTICIPATED BUT, FORGIVE ME, ALL OF THIS FEELS LIKE A BAD DREAM! I DON'T EVEN KNOW WHO YOU ARE!

IT'S TAKEN US YEARS TO DEPLOY THE SEARCH CENSORS AND CAPABILITY WE HAVEN'T: THERE ARE MANY OPTIMIZERS LOOKING TO PROTECT WHAT WE LOVE. I WANT YOU TO JOIN THE FALCON. AND WE ALL WANT THE SAME THING.

TOGETHER, WE CAN BUILD OUR PROOF OF DETERRED PATIENTS TO PASS THESE BAD ACTORS AND MORE PEOPLE LIKE YOUR DAD CAN BE PROTECTED FROM THE FALLOUT OF WHAT IS LARGE LIGHTING UNNOTICED BY THE CROWD.

CHIEF: Our secrecy is part of what keeps us all safe.

CHIEF: We 'exist' in cyberspace. But should you choose to be our voice to the outside world, we can provide you with unparalleled resources to conduct your investigation. I'll leave you to it. You know what to do.
My name is Ava Williams. I'm a graduate student at JU. One day, I was walking in the woods and...
AVA SEES THE LONG JOURNEY FROM ANN ARBOR TO PARK COLLEGE UNIVERSITY.

SHE STOPS TO TAKE A BREAK AND TO BUY SOME REFRESHMENTS.

AVA SPOTS A GAS STATION, SOMEWHERE CLOSE TO PITTSBURGH, ON HER GPS.

AVA SPOTS THE SAME CAR SHE SAW EARLIER, PULL UP NEXT TO HER AT THE GAS STATION.

THAT’LL BE $7.50.

THANKS.

AVA SPOTS TWO FIGURES ENTERING THE SHOP AND A WORRIED EXPRESSION APPEARS ACROSS HER FACE.
Haha, don't worry, I came prepared.

Of course, Jill. I'll be downstairs soon. Hope you're wearing your mask.

Of course, Jill. I'll be downstairs soon. Hope you're wearing your mask.

Dr. Hartman! So great to finally meet you!

Hey, Dr. Hartman! So great to finally meet you!

Hey, Dr. Hartman! So great to finally meet you!

Well, welcome to Main College! How was the drive all the way from Ann Arbor, Sweden?

Well, welcome to Main College! How was the drive all the way from Ann Arbor, Sweden?

Well, welcome to Main College! How was the drive all the way from Ann Arbor, Sweden?

They enter a lab and see the various doctors working on their apparatus.

I wasn't that bad, not that many people on the road.

I wasn't that bad, not that many people on the road.

I wasn't that bad, not that many people on the road.

Why don't I take you up to the lab? We can talk more upstairs.

Why don't I take you up to the lab? We can talk more upstairs.

Why don't I take you up to the lab? We can talk more upstairs.

We don't usually allow it, but considering you've come all this way and you've been recommended by Symous...

We don't usually allow it, but considering you've come all this way and you've been recommended by Symous...

We don't usually allow it, but considering you've come all this way and you've been recommended by Symous...

Why do I ask why?

Why do I ask why?

Why do I ask why?
The process for creating a vaccine is more of a marathon than a sprint. It comes out with a legitimate vaccine so fast has been a victory for science. Here in the US, we are also working hard to ensure that we are able to vaccinate as much of the population as we can. There is no one way to develop a vaccine. At any given point in time, multiple research teams are often exploring different ways to attack a specific virus. That’s why our country always requires vigorous testing and trial processes before we make vaccines available to the general public.

There are still several vaccines still being developed, our current vaccine has an efficacy rate of 95%.

As you probably know, the first approach, which is the best known, is simply taking a portion of the virus that can do no harm, such as inactivated or weakened strains, and introducing it to the human body in such a way that it creates an immune response. This immune response then acts against the real pathogen if it comes in contact with it.

Another approach that some of our colleagues have pursued involves not introducing a whole virus into the body, but rather delivering genetic instructions which signal the body to create a protein that, in turn, stimulates an immune response and produces antibodies.

As the body produces the antibodies, then are then able to fight the virus if it enters the body. We call these DNA vaccines. One of which carries the genetic instructions as you may be aware.

There is also yet another approach that uses the DNA-RNA cocktail and instead uses messenger RNA. Most vaccines create an immune response by inserting a weakened strain of a virus into the body, after which we vaccinate, however, to create a protein in our cells instead. This protein does not become in our system and builds antibodies for protection. The immune response that is generated then protects from further infection against the virus.

That’s probably the clearest explanation. I have ever heard. I have so much respect for what you all are doing...

Thank you all. We have been successful in creating a vaccine in record time. That underwent extensive safety evaluations as part of clinical trials before being widely distributed. There are, of course, many other approaches, which I did not get into. We anticipate over 100 different projects around the world that are pursuing this study.

Private and public sectors have all thrown everything they have at the kitchen sink at this problem. I am sure that you would have seen that some household names, including some tech companies, have pledged a billion dollars in support. But the good news is that we are now on track to having an effective vaccine. That will hopefully start to roll out to the public soon.
A vaccine has never been developed as fast as this. It’s not just been us in the science community working to finalize the vaccine. Others are working to figure out the best way to get the vaccines delivered and administered.

Even as the scientific community has worked to finalize the vaccine, others are working on something bigger related to fighting disinformation around the COVID-19 vaccine.

Emily tells me you are working on something big related to fighting disinformation around the COVID-19 vaccine?

That’s right. I’m working on a documentary that sheds light on how certain groups are linking 5G to the weakening of people’s immunities and rendering the vaccines useless.

That’s interesting. Have you been able to follow the money?

Certain communities have particularly strong responses to this social media marketing. Social media giants need to help put an end to what is clearly a national risk.

These investments are legal as far as I can tell, but it is likely to hurt people because it usually involves spreading falsehoods like many misreports, vaccines can cause side effects. Usually, vaccine side effects are minor, for example, a sore arm where a shot was given or a low-grade fever after a vaccine, and go away on their own within a few days.

We have not managed to trace the money quite as far as I would have liked to. Some is coming from the private investors, but others, I am not too sure at present.

It’s a labyrinthine network of companies which, if I am honest, is not what we are set up to look at. But if you know any financial crime experts who have more experience tracking the flow of money, what we have here may be right up their alley.

I had mentioned your visit to him in person and he said he would be up for showing you his research.

He’s a media studies professor here. Dr. Harris Adams.

Thank you.
ALL CONTINUES THE DRIVE BACK TO JOAN ARBOR, AND GETS IN TOUCH WITH DARREN LANCasters WHEN SHE RETURNS HOME.

OH... HUH, I'M SURE HE HAD A LOT OF THINGS TO SAY! WHAT DO YOU WANT?

HE JUST SAID YOU BOTH AGREE TO DISAGREE ON A NUMBER OF TOPICS AND THAT YOU WERE AN EXPERT ON ANTI-VAX PERSPECTIVE, I WAS SIMPLY HOPING I COULD ASK YOU A FEW QUESTIONS.

I AM PART OF THE TEAM BEHIND A NEW DOCUMENTARY ON THE DIFFERENT VIEWS AROUND THE COVID-19 VACCINE AND WANTED TO GET A BALANCED PERSPECTIVE FROM ALL SIDES NOW THAT WE DO HAVE SEVERAL WORKING VACCINES.

WELL, IF YOU HAVE SPENT ANY TIME RESEARCHING MY POINT OF VIEW, YOU KNOW EXACTLY WHAT WOULD HAPPEN IN OUR COMMUNITY IF THERE IS TALK ABOUT A VACCINE.

THANK YOU SO MUCH FOR THE OPPORTUNITY, I WILL SEND YOU THE LOGISTICS OVER A TEXT, ARE YOU OK TO COME TO THE STUDIO?

IT'S EASIER TO SOCIAL DISTANCE IF WE DO A VIDEO CONFERENCE. THE VAX IS VERY REAL, IT'S THE EFFECTIVENESS OF THESE VACCINES WHICH HAVE BEEN DEVELOPED THAT I HAVE DOUBTS ABOUT.

GOOD MORNING, DR. WANG ADAMS REFERRED ME TO YOU.

I'M AIA WILLIAMS, I WOULD LIKE TO INTERVIEW YOU THINK OF THIS AS AN EXCLUSIVE OPPORTUNITY TO SHARE YOUR VIEWS WITH A WIDE AUDIENCE!

SOUNDS LIKE A PLAN, I'M GOOD WITH MONDAY. THIS IS A SURPRISE, BUT A WELCOME ONE. WE NEED DIVERSITY OF THOUGHT.

YES, THAT'S ME.

I WOULD LIKE TO INTERVIEW YOU THINK OF THIS AS AN EXCLUSIVE OPPORTUNITY TO SHARE YOUR VIEWS WITH A WIDE AUDIENCE!
ONE WEEK LATER IN THE MEDIA DECORATING LAB IN THE UNIVERSITY

PLEASURE TO HAVE YOU WITH US DARRIN. LET'S TALK ABOUT THE ROLE YOU'RE AGAINST VACCINATION?

THAT'S QUITE A FOOTPRINT. WHAT IS THE CORE REASON YOU'RE AGAINST VACCINATION?

PERSONALLY, DO YOU THINK THE IDEA OF GOVERNMENT ORGANIZATIONS IN THE HEALTH SECTOR PROMOTING VACCINES IS WRONG?

YES I DO THINK IT'S WRONG. THE INFLUENZA VACCINE HAS NOT WORKED.

LIKE I SAID EARLIER AND AS WE CAN NOW SEE, VACCINES AREN'T PERFECT. THEY'RE NOT EVEN POSSIBLE.

MUCH OF WHAT WE SEE BEING PEDDLED BY THE GOVERNMENT IS PRESCRIPTIVE WITH INCORRECT DATA SUPPORTING THEIR HYPOTHESIS. IN OUR OWN SCIENCE TEAM, THAT HAVE SHOWN THAT THE DATA ITSELF IS QUESTIONABLE AROUND HOW WELL THESE NEW VACCINES WORK. OUR BACKERS BELIEVE IN OUR MISSION TOO. WE ARE HERE TO PROTECT AMERICA.

DO YOU EVER THINK IF THIS VACCINE WOULD AT LEAST BE DIRECTLY CONNECTED TO DISEMOBILIZATION, OR SOME SOCIAL MEDIA WILDEYS?

EVEN IF IT IS TRUE, I STILL BELIEVE IT'S THE SELFISHNESS OF THE SYSTEM AND FOR WHAT? THE NEWS AND EVIDENCE IS THERE.

WHAT IF IT'S NOT SERIOUS?

THERE ARE MANY INTERVENTIONS THAT DON'T INVOLVE A VACCINE. HIV/AIDS IMUNITY IS A THING, RIGHT?

DON'T PEOPLE DIE EVERY DAY? NO ONE EATS AN EGG. HANG, POVERTY, CORRUPTION. WE HAVEN'T EVEN BEEN ABLE TO SEGREGATE INFECTiosa FOR COMING OUT LATE.

SO ARE WE GOING TO KEEP SHINGU MANHOLE MEDIA TOTAL POWER?

BUT WHAT ABOUT COVID-19? IT'S A CREASE NO ONE HAS REALLY HEARD OF TILL NOW.

DON'T YOU THINK THERE'LL BE TOO MANY DEATHS BEFORE WE REACH THAT?

WE HAVE SOME HADO MACHINES TO MAKE. ALL THE VACCINES AMERICAN KIDS HAVE BEEN HIT WITH. DON'T YOU BELIEVE WE'VE BEEN CLOSING UP THEIR IMMUNE SYSTEMS?

WHAT ABOUT THE FACTS AND STATISTICS ORGANIZATIONS LIKE THE UNITED NATIONS PUBLISH?

JUST BECAUSE IT'S A NUMBER DOESN'T MEAN IT'S TRUE. DON'T YOU THINK METRICS ARE USED TO PUSH AN AGENDA, UNDER A COVER OF BEING OBJECTIVE? WE NEED TO LISTEN TO THE PUBLIC, AND WITH SEVERAL MILLION VOTERS AS MEMBERS. WE THINK THAT TRUST INNATURE HAS THE POTENTIAL TO BE A MORE VITAL VOICE IN THE SPACE. WHY NOT THE SAME HERE? PARENTS HAVE TO BE ABLE TO DECIDE FOR THEIR CHILDREN, NOT THE GOVERNMENT. WHAT PARENT WOULD WANT THEIR KIDS TO BE INFECTED BY AUTISM OR MEDIATED? APPARENTLY, IT SEEMS THAT WAY, GIVEN THE BILLION DOLLARS' WORTH OF MARKETING THESE MEDICAL COMPANIES INVEST IN.

SPEAKING OF MARKETING DOLLARS, IT APPEARS AS IF YOUR GROUP IS ONE OF THE TWO SPENDING TENS OF MILLIONS ON DIGITAL ADVERTISEMENTS ON FRIENDPLACE AND OTHER PLATFORMS. CAN YOU ELABORATE ON YOUR DONOR BASE?

NO COMMENT ON OUR DONORS. SOME ARE PUBLIC AND OTHERS PREFER TO BE KEPT OUT OF THE SPOTLIGHT. SO, IN DECEASED TO THEIR PRIVACY, LET'S PLEASE MOVE TO THE NEXT QUESTION. BUT “YES,” TO ANSWER YOUR QUESTION, WE ARE SPENDING ON DIGITAL ADVERTISING AS IT SEEMS TO BE THE BEST WAY TO GROW OUR BASE.
DO YOU THINK HB2019 WOULD DENY THE VACCINE USELESS?

I HAVE SEEN SOME CHATTER ABOUT THIS, BUT WE HAVE TO WAIT AND WATCH. COULD BE THERE'S A PETITION IN A STATE CORRELATING ITS DEVELOPMENT TO WEAKER IMMUNITY.

BLA BLA BLA

I MEAN TO SAY THE PETITION WAS ABOUT PROTESTING AGAINST THE INSTALLATION OF 5G NETWORKS AND THE IMPACT OF THEIR EFFECTS ON OUR HEALTH. WE STOOD THE POSTS AND CAN CONCLUSIVELY PROVE THAT A LARGE NUMBER OF COMMENTS AND POSTS ON THE PETITION WERE "SUSPICIOUS." WE HAVE EVIDENCE THAT THEY WERE NOT MADE BY PEOPLE IN THE UNITED STATES. IN FACT, SOME OF THESE POSTS WERE NOT EVEN MADE BY REAL PEOPLE. INSTEAD THEY WERE MADE BY BOTS.

MY APOLOGIES, MY INTENTION WASN'T TRYING TO SPREAD ANYTHING ON YOU, BUT I WANTED TO MAKE YOU AWARE OF THESE DATA POINTS. I KNOW THAT Dr. Harder Adams has also showcased analysis that has highlighted how much the anti-vax movement is just two parties—one of which is yourselves, and one other is a questionable organization that we have not been able to set any comments from a head of this.

DO YOU NOT BELIEVE THAT LACK OF INTERVENTIONS AGAINST COVID-19 COULD LEAD TO HARM?

I BELIEVE THAT A VACCINE IS NOT THE ONLY INTERVENTION. OUR COMMUNITIES ARE FULLY COMPLIANT WITH SOCIAL DISTANCING AND TAKE ALL PROTECTIVE STEPS TO ENSURE THE SAFETY OF THEIR LOVED ONES. THANK YOU VERY MUCH FOR THIS OPPORTUNITY TO SHARE OUR PERSPECTIVE. BUT I NOW BELIEVE THAT WE ARE NOT SHARING ANY NEW INFORMATION WITH VIEWERS AND SO I WOULD LIKE TO WRAP UP THANK YOU AGAIN. RXS. WILLIAMS.

Thank you for joining us. When we return we will meet with a family that have come around to the idea of a vaccine without compromising their value system.

My apologies, my intention wasn't trying to spread anything on you, but I wanted to make you aware of these data points. I know that Dr. Harder Adams has also showcased analysis that has highlighted how much the anti-vax movement is just two parties—one of which is yourselves, and one other is a questionable organization that we have not been able to set any comments from ahead of this.

DO YOU NOT BELIEVE THAT LACK OF INTERVENTIONS AGAINST COVID-19 COULD LEAD TO HARM?

I BELIEVE THAT A VACCINE IS NOT THE ONLY INTERVENTION. OUR COMMUNITIES ARE FULLY COMPLIANT WITH SOCIAL DISTANCING AND TAKE ALL PROTECTIVE STEPS TO ENSURE THE SAFETY OF THEIR LOVED ONES. THANK YOU VERY MUCH FOR THIS OPPORTUNITY TO SHARE OUR PERSPECTIVE. BUT I NOW BELIEVE THAT WE ARE NOT SHARING ANY NEW INFORMATION WITH VIEWERS AND SO I WOULD LIKE TO WRAP UP THANK YOU AGAIN. RXS. WILLIAMS.

Thank you for joining us. When we return we will meet with a family that have come around to the idea of a vaccine without compromising their value system.

Here Ana, this is the transcript. The text was written by you, which I'm supposed to read. I have some ideas for you.

Feel sorry that you are always watching.

This feels like an ambush! You should have shared that with me before this… Nevertheless, please share your analysis with our team of data scientists and forensic technologists and we will publish our own independent findings.

Ava has removed her mask, as she exits the building.

PREPARATIONS FOR THE NEXT SEGMENT.

Hello Chapman.

Looking like we are making some headway.

YES, I THINK IT'S ALONG. WE NEED TO SCHEDULE THAT INTERVIEW AS WIDELY ACROSS THE INTERNET AS POSSIBLE AND I THINK THAT DOMAIN STRATEGIST WILL COVER IT AS LANDCASTER IS ON THE CASE.

WE HAVE DONE WHAT WE NEEDED TO DO, AND OUR INFLUENCERS HAVE BEEN TOLD TO SEE YOUR SEGMENT ACROSS EVERY SOCIAL MEDIA. AND YOUR INTERVIEW IS ALREADY BLOWING UP ALL OVER THE WEB. THE PETITION IS GETTING HEAT!

NO WORRIES. MY PHONE IS PINNING LIKE CRAZY. I HAD TO TURN OFF NOTIFICATIONS!

DON'T WORRY. YOU WILL HAVE SUPPORT AND A PRIVATE DETAIL.

THANKS, AND WILL DO. I DON'T KNOW HOW TO THANK YOU!
A few months later, Ava arrives at the National Journalism Award Ceremony.

Awards are being presented for excellence in journalism. Ava is dressed formally and is seated among other news professionals.

The press is present, and Ava sees some familiar faces.

On stage, a woman is awarding the prize for "Best Newswoman and Use of Digital Media." The award goes to someone whose work has been instrumental in educating people about a topic where disinformation is rampant and people are quick to believe news without verifying its accuracy.

Ava is surprised to see an old acquaintance from her time as a reporter. They greet each other warmly.

"Ava, you look great!" says her acquaintance. "What brings you here?"

"Just enjoying the ceremony," Ava replies. "How about you?"

"I'm here for the awards," her acquaintance says. "I'm very honored to be here."

Ava smiles and nods in agreement. The ceremony continues, and Ava watches in silent excitement as the awards are presented.

In the audience, Ava notices news professionals from all over the country. It's a great event, and Ava is grateful to be a part of it.

"Ava, you're doing a great job," her acquaintance says. "You should be proud of yourself."

Ava smiles and nods in agreement. The ceremony is over, and Ava leaves the stage. She's happy with her work and looks forward to the future.

Ava pulls up outside a residential area.

She pulls into the driveway of her apartment complex. The sky is dark and the stars are shining brightly. She looks up at the sky and smiles.

"I can't believe all this has happened in just one week," she thinks to herself.

Ava's honey is that you?

"I've been so worried about you. Someone called and told me not to worry. Who was that? Never mind, did you eat before?"

"I saw you on the news. I am so proud, kiddo."

"I was just working, and it's not permanent."

"I don't know what you're working on. Honey, come on. You take some time and relax."

"I just need to do this thing. I don't know if I'll be able to get it."

"That's my girl. I'm so thankful for the instructors. I'm sure you and me, all we have is each other."

"Me too. And it's so good to have you back."

Ava's honey looks tired. Have you been getting enough sleep?

"I was at the news with all her reporting! Mad!"

"Okay. Let's go."

Just work, and it's not permanent.

"I don't know what you're working on. Honey, come on. You take some time and relax."

"I'll just need to do this thing. I don't know if I'll be able to get it."

"That's my girl. I'm so thankful for the instructors. I'm sure you and me, all we have is each other."

"Me too. And it's so good to have you back."

"I thought you had something to do with it."

"Something else is happening. Possibly your next big story? If you can handle it!"
We owe Miss Williams a lot of gratitude for her efforts and she is a very worthy recipient of this award.

The internet sees a huge volume and variety of information pass through it every day. Politically, socially, or economically, we will probably grapple on a lot of things, but there is no place for disinformation in our lives.

As someone who is just starting my career as a journalist, I am honored and excited to be a part of a field dedicated to holding ourselves and our institutions accountable. People can get information from many places these days, making our ability to educate the public through accurate, fair, and factual reporting even more important.

Many of us are working to fight disinformation. I thank you for recognizing my efforts and am grateful to have had the opportunity to play a small part in a much bigger story.

Thank you!
BIBLIOGRAPHY

PAGE 46:
J. WOLFE. “CORONAVIRUS BRIEFING: WHAT HAPPENED TODAY.” 2020
HTTPS://WWW.NYTIES.COM/2020/11/16/US/CORONAVIRUS-TOMAY.HTML

PAGE 50:
S. CHOSE. “ARE YOU READY FOR THE QUANTUM COMPUTING REVOLUTION?” 2020
NOTES FROM CISA

Disinformation is an existential threat to the United States, our democratic way of life, and the infrastructure on which it relies. The Resilience Series (of which this is the second title) uses the graphic novel format to communicate the dangers and risks associated with dis- and misinformation through fictional stories that are inspired by real-world events.

The Resilience Series graphic novels were commissioned by the cybersecurity and infrastructure security agency (CISA) to share information to illustrate:

1) Foreign actors are trying to influence U.S. security, economy, and politics through the malicious use of online media to create and amplify disinformation.

2) While the strategy of using inaccurate information to weaken and divide a society is not new, the Internet and social media allow disinformation to spread more quickly than it has in the past.

3) Deepfakes, bots, and troll farms are just some of the emerging techniques for creating and spreading disinformation.

CISA encourages everyone to consume information with care, practicing media literacy including verifying sources, seeking alternative viewpoints, and finding trusted sources of information. It is the most effective strategy in limiting the effect of disinformation. For more information and further reading about disinformation, please visit the cybersecurity & infrastructure security agency website, www.cisa.gov.
We live in a world where the World Wide Web is rife with misinformation and disinformation. In a precarious digital world, the need for awareness about this risk is greater than ever. The Resilience Series works to simplify and present the threat inaccurate information can have on important events that shape the future of democracy.

In the second issue of the series, "Bug Bytes," we see Ava Williams use her wits and journalism skills to uncover a disinformation campaign set to damage critical communications infrastructure. Ava discovers a few allies along the way and races to try and help the world see through the web of lies being spun online.
The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic novel to highlight tactics used by foreign government-backed disinformation campaigns that seek to disrupt American life and the infrastructure that underlies it. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold and express any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

CISA celebrates the First Amendment rights of all U.S. persons without restriction. CISA doesn't endorse any products, services, institutions, or conduct outside of our authority that have been included in this story. While based on actual nation-state adversary activity, the story and all names, characters, organizations, and incidents portrayed in this production are fictitious.
WHY WATCH IT? I KNOW YOU DON'T HAVE ANOTHER $200 FOR A GAMEWORLSE.

ARE YOU OKAY?

SORRY, I DON'T MEAN TO SLAM IT DOWN SO HARD.

...YEAH, NO, I DON'T KNOW.

WHAT'S GOING ON WITH YOU LATELY? YOU'VE BEEN ON EDGE A LOT AND IT'S AFFECTING YOUR GAME.

I KNOW IT'S SILLY, BUT THIS TROLL ON COMMLODE HAS GOTTEN UNDER MY SKIN.

TOO? WHAT KIND OF TROLL? IS HE TRASHING OUR TEAM?

NO, IT'S POLITICAL.

HERE WE GO WITH THE POLITICS AGAIN. THAT'S ALL JUST A DISTRACTION, FOCUS ON WHAT'S IMPORTANT.

YOUR LOOKING TENSE.

THIS GUY IS CLEARLY A TROLL. I DON'T KNOW WHY I BOther TO REPLY.

YOU WILL NEVER GET IT. POLITICs IS IMPORTANT TO ME.

RACHEL, I DON'T THINK I AM IN THE MOOD FOR A LECTURE RIGHT NOW.

THAT'S EXACTLY WHAT YOUR DOING. YOu'RE PRODUCING INSTEAD OF REsponding TO COMMENTS.

THIS MEANS A LOT TO YOU, I KNOW BUT--

THAT GIVES SABINA AND THEN PEOPLE DON'T HAVE THE FACT THAT'S DANGEROUS.

IT'S A SITUATION WHERE PEOPLE DON'T HAVE THE FACT THAT'S DANGEROUS.

THIS MEANS A LOT TO YOU, I KNOW BUT--

THAT GIVES SABINA AND THEN PEOPLE DON'T HAVE THE FACT THAT'S DANGEROUS.

IT'S A SITUATION WHERE PEOPLE DON'T HAVE THE FACT THAT'S DANGEROUS.

OH MAN. THIS IS REALLY GOING TO SEND THE MEDIA INTO A FRENZY. WHILE OUR NATIONS EXIST ON TIMES BY TALKING ABOUT THESE "SYNTHETIC VIDEOS." THE REAL ISSUE IS THAT THEY ARE SO PRECIOUS, THE "LUA'S DIVIDEND".

"LUA'S DIVIDEND" IS THE UNPREPARED OUTCOME OF STARTING A LIFESTYLE ON COMPASSION. WHEN IN TURN COURSES-OFF AIR AROUND THE VITALITY OF LIVES THAT SETS THE STANDARDS THAT INFLUENCE LIVING.
Creepin' around like no one knows you're so criminal...

Bad guy - Billie Elish

Woof!

Hi, Chewie... That's a good boy. Miss me?
A BRIEF HISTORY OF DEEPAFES.

The term "deepfake," a combination of "deep learning" and "fake," is used to describe synthetic video or audio content, which is often created with malicious intent to spread misinformation. The term was first used by a Reddit user in 2017.

The first deepfakes that gained notoriety were mostly focused on non-consensual pornography, creating synthetic media often using celebrities as subjects, to garner widespread sharing. In many cases, the synthetic media has been used as a way to shame, humiliate, and manipulate victims around the world. Techniques have ranged from face-swapping technology to much more complex applications.

Deepfakes have come by way of not only video but audio too. The ability to use readily available and affordable software to create fake sound of video has become available to the masses as the cost of graphical processing units has fallen and the necessary processing power to make a deepfake, which was once out of reach, has become more accessible.

Academics have also been hard at work showcasing the extent to which deepfakes can be used to influence mainstream media. MIT produced a video of President Richard Nixon where they played out an alternative moon landing story. That deepfake was using a president of yesterday... Fast forward to an election year and imagine how video alteration software can manufacture videos of a presidential candidate with devastating impacts on the confidence of voters in the information they ingest.
In March 2019, the CEO of a UK-based energy firm was asked over a call, by someone he then thought to be the head of his German parent company, to transfer 20,000 euros to a Hungarian supplier.

According to the company’s insurance company, fraudsters had leveraged deepfake technology and artificial intelligence to construct a life-like recording of the German group head’s voice. The money was syphoned off to Mexico and channeled to other accounts.

News reports later detailed that the CEO had been convinced that it was the head of the parent company on the basis of a German accent and his recollection of his boss’ voice and made the transfer all within an hour’s time. Reportedly, the same source tried to request additional funds to be transferred but by then the UK CEO had grown suspicious and did not authorize any additional transfers.

The financial, political, and social threat posed by deepfakes (and today cheap fakes), is a very real risk about which society at large needs to develop awareness and resilience.

The men who went to the moon to explore in peace
One technique for the creation of a Deepfake video involves swapping a person’s face and replacing it with another, using a facial recognition algorithm and a deep learning computer network called a Variational Auto-Encoder (VAE).

VAEs are trained to encode images into simpler low-dimensional representations (think of zooming into a picture to see the pixel) and then decoding those representations back into images. For instance, if you wanted to transform a video of anyone speaking, you would need two auto-encoders. One trained on images of the subject’s face, and one trained on images of a wide range or diversity of faces.

Training the machine is why the term machine learning is used to describe this particular application of artificial intelligence. Once the machine has learned or is ‘trained,’ it is then possible to combine the encoder trained on the diverse faces with the decoder trained on the subject’s face. This results in the subject’s face being able to be placed on someone else’s body.

The images of faces used for both training sets can be curated by applying an algorithm for facial recognition. This algorithm is able to capture video frames for a diversity of faces in various naturally occurring poses and lighting conditions.

Will stay on the moon to rest in peace
HOLLYWOOD HAS LEVERAGED DEEPFAKE TECHNOLOGY WITH GREAT SUCCESS, SUCH AS “GEMINI MAN” WHERE A MULTI-MILLION DOLLAR BUDGET PRODUCES A YOUNGER VERSION OF WILL SMITH THAT BATTLES WITH HIS CONTEMPORARY SELF. SIMILAR DE-AGING EFFECTS CAN BE SEEN IN “THE IRISHMAN” PRODUCED BY NETFLIX IN 2019.

WHILE THESE PRODUCTIONS SPARE NO EXPENSE AT BIG BUDGET DEEPFAKE WORK, ONE DOES NOT HAVE TO SEARCH TOO LONG ON YOUTUBE TO FIND PLENTY OF EXAMPLES OF CHEAP FAKES. ONE OF THE MOST PROMINENT EXAMPLES USES WILL SMITH’S FACE SUPERIMPOSED ON KEANU REEVES’ FACE IN A SCENE FROM “THE MATRIX.” THIS WAS CREATED BY A YOUTUBER USING A FREE SOFTWARE.

DISNEY RELEASED A SIGNIFICANT PAPER IN 2020 WHICH DETAILS A NEW ALGORITHM THAT IS ABLE TO ACHIEVE SIGNIFICANTLY BETTER QUALITY SYNTHETIC VIDEO OUTPUTS FOR HIGH-RESOLUTION VIDEOS. WITH THE DAWN OF HIGHER RESOLUTION TELEVISION SETS, THIS WILL BECOME EVEN MORE IMPORTANT AS THE MINUTIAE OF FACES IS MORE VISIBLE AND LOW FIDELITY ALTERATIONS MAY NOT PROVIDE FOR AS COMPELLING AN ENTERTAINMENT EXPERIENCE.

THIS IS EXCITING TECHNOLOGY FOR HOLLYWOOD BECAUSE IT ALLOWS FOR POSSIBILITIES LIKE RECREATING HISTORICAL VIDEOS SUCH AS PRESIDENT KENNEDY SPEAKING DURING THE CUBAN MISSILE CRISIS BUT USING AN ALTERNATIVE SCRIPT. MANY STUDIO EXECUTIVES SEE THE TECHNOLOGY AND ITS USE BECOMING MORE PERVERSIVE IN THE COMING YEARS.

for every human being who looks up at the moon in the nights to come
Another example where the technology has found a home, once again in the entertainment industry, is in gaming.

The growing inventory of artificial or synthetically generated voices can be purchased by gaming studios that are looking to offer a level of realism in their gameplay that previously could have only been offered by real voice actors.

Game studios are creating “voice-skins” for use in online games and social platforms. The gaming industry is larger than the world of movies and books combined and therefore the commercial potential here is likely to continue to gather interest.

will know that there is some corner of another world that is forever mankind
While the number of deepfake and cheap fake videos continues to explode on the internet, a new set of organizations have emerged to identify, track, and report on these threat vectors.

It’s important for the voting public to be particularly vigilant about the content they see on the internet, and to seek out trusted sources. The constant churn of user-generated content mixed with planted cheap fakes is a particular area of concern for democracies around the world that grapple with the potential influence this type of media could have if voters are faced with election-related disinformation.

While many in the media are doing great work to unmask and report on disinformation and even identify specific deepfakes, all of this talk about disinformation also feeds what is referred to as the ‘liars dividend.’ The public becomes increasingly hyperaware of the issue around the origin of content that they may even start to doubt the veracity of legitimate videos and media on the internet.

Some of these companies employ large teams that are scanning social platforms around the world and identifying the emergence of such media, recognizing that synthetic content has the potential to impact economies and people around the world.
A FEW MONTHS EARLIER, MOSCOW, RUSSIA

LENINGRADSKAYA STATION

Комендантский проспект
↑ Komendantskiy prospekt

ЭКСКУРСИЯ ПО МОСКВЕ
(CA LITTLE BIRD TELLS ME YOU HAVE BEEN CALLING YOUR GRUPPENBND AGAIN, YOU KNOW THIS IS A DANGEROUS GAME, WHAT WERE YOU THINKING?)

(DON'T BE SILLY, WE SEE EVERYTHING, JUST STAY OFF THE PHONE!)

(I WAS UNDER PRESSURE TO DELIVER, WHERE ARE WE WITH THE NEW CAMPAIGN?)

(WE ARE WORKING ON A VIDEO RIGHT NOW WHERE WE HAVE MANUFACTURED A STORY ABOUT A PROMINENT SENATOR, IT'S ALMOST TOO EASY TO GET THESE TWO PARTIES FIGHTING WITH EACH OTHER.)

(THAT'S GOOD, WHAT ABOUT THE ELECTION WORK? THAT'S FAR MORE IMPORTANT RIGHT NOW, ARE THE FARMERS READY WITH THE SEEDS?)

(GOOD, WHAT ABOUT THE ELECTION WORK? THAT'S FAR MORE IMPORTANT RIGHT NOW, ARE THE FARMERS READY WITH THE SEEDS?)

(AND THE MORE THEY FIGHT WITH EACH OTHER...)?

(WE MUST USE THE LATEST ALGO WITH THE NEW ALGORITHM. IT WILL BE REALISTIC ENOUGH TO IMPRINT HIGH-RESOLUTION VIDEOS. THIS WILL DARE US TO THE NEXT LEVEL. HOW REAL THIS WILL SEEM TO THE AMERICANS...)
100

PLEASE MAKE YOURSELF COMFORTABLE. CAN I GET YOU SOMETHING TO DRINK? WATER?

WE ARE VERY IMPRESSED WITH YOUR RESUME.

I AM GOOD FOR NOW. THANK YOU.

REALLY APPRECIATE THE OPPORTUNITY TO INTERVIEW HERE.

WOW! THIS IS A DREAM COME TRUE! YES, OF COURSE.

NAME, WE ARE REALLY PLEASED WITH THE WAY YOU CONDUCTED YOURSELF AND THE QUALITY OF THE POST YOU CREATED IN SUCH A SHORT TIME!

YOU SEEM TO HAVE REALLY GOOD KNOWLEDGE OF WHAT IS HAPPENING IN AMERICA. WE WANT YOU TO START IMMEDIATELY. WILL YOU JOIN US?

PLEASE COME WITH ME TO THE NEXT ROOM AND WE WILL PROCEED WITH YOUR RING INSTRUCTION IMMEDIATELY.

SOFT TELL ME A LITTLE ABOUT YOUR EXPERIENCE WITH CONTENT CREATION ON SOCIAL MEDIA.

VERY NICE. TELL ME, COULD YOU WRITE SOMETHING RIGHT NOW FOR ME IN AMERICAN ENGLISH?

I COULD YES.

WELL, I DID SOME WORK AROUND THE ECOLOGICAL CRISIS IN AFRICA LAST YEAR THROUGH SOME FREELANCING PLATFORMS.

GOOD. I WANT YOU TO WRITE A PIECE ON "CORRUPTION AT THE HIGHEST LEVELS" IN THE UNITED STATES. I WANT YOU TO THINK "SENATORS AND SENIOR OFFICIALS."

YES, BUT WHY WOULD THAT NEED A CAMPAIGN FROM THE U.S.?

IT'S A FOCUS RIGHT NOW IN THE STATES. WE HAVE INTEREST IN OUTLINES INJUSTICE. JUST LET ME SEE WHAT YOU CAN DO.

CAN'T WAIT TO LET MAMA KNOW I GOT THE JOB.
This is your station. Make sure you show me how many posts and what engagement you get daily in a status report.

Half an hour later, after a debrief with a new manager...

Isaac here will show you how to use the reporting system. Our founders like to see daily results.

Showtime! Let's talk about today's progress with the boss! We're really starting to fill up the seats down there.

You are late on the engagement numbers from yesterday's posts. What happened?
A FEW HOURS LATER AT AN IMPORTANT INVESTOR MEETING

I JUST WANT TO APOLOGIZE ON BEHALF OF THE NUNEWZ FOUNDER. THEY ARE BOTH CURRENTLY INDEPENSE.

AS THE CFO, I WILL BE LEADING THIS DISCUSSION TOGETHER WITH MY COLLEAGUE, MR. BADU.

I DON'T KNOW ABOUT THAT NUMBER. I HAVE INVESTED IN SIMILAR COMPANIES IN EUROPE AND ASIA, BUT THEY HAD BEEN UP AND RUNNING FOR 1-2 YEARS LAYER THAN THREE MONTHS.

SO, DO YOU THINK YOU CAN INVEST $100,000? THAT WILL BUY YOU 10% OF OUR COMPANY BASED ON THE VALUATION.

ADMITTEDLY, YOUR RETURNS ARE EXTRAORDINARY FOR A STARTUP UNDER 6 MONTHS AND THIS WOULD GIVE US A FOOTING HERE IN AFRICA, WHICH IS SO FULL OF OPPORTUNITY FOR US. OKAY, LET'S MOVE AHEAD.

THE FOUNDERS WILL BE REALLY HAPPY WITH THIS OUTCOME.

AND HE SAID THAT HE HAD OTHER FRIENDS WHO MIGHT ALSO WANT TO INVEST.

YES, I AM JUST GLAD WE DIDN'T GET TOO DEEP INTO THE ACTUAL WORK WE DO.

MEANWHILE IN WESTERN EUROPE...
TWO TACOS PLEASE!

SO GREAT THAT WE HAVE THE FOOD TRUCK SCENE HERE!

WELL... I WOULDN'T GO THAT FAR!

IT ALMOST FEELS LIKE AUSTIN DURING SOUTH BY!

THINK I NEED TO BOOST MY POSTS MORE... NOT QUITE HITTING THE BIG TIME YET COMPARED TO SOME OF THE OTHERS WHO HAVE A MILLION LIKES! HOW DO THEY DO THAT?

DON'T WORRY IT'S ABOUT A/B TESTING THE COPY AND THE CREATIVE ARRANGEMENTS USED IN THE AD AS IN VIDEOS WHAT WORKS BETTER: IMAGE A OR B, OR AGAIN COPY A OR B! HAPPY TO SHARE SOME OF MY TIPS... I STILL TOP THE LEADERBOARD WITH MY ANTI-VAX VACCINE POST WITH TWO MILLION ENGAGEMENTS!

GETTING THE FEELING I SHOULD HAVE STAYED IN THE WORLD OF BIG AGENCIES!
US Senator caught red-handed on a “Video” taking bribes to push for a planning permit for a foreign group.

It’s a bit risky to meet up so soon and introduce the idea of a circus. But we don’t have much time with the clock on the election ticking!

This Single0 guy is really getting on my nerves!

I’m seriously worried about how real it looks and the potential for this to go viral.

I can’t believe that no one else is calling these bogus videos out!

All bogus! None of that is true...

I’m going to report this to the social media platform!

Let’s hope they take the videos down.

A good journalist never reveals his sources. Now, let’s get on with setting these videos seeded. The correct hashtags are #SenatorOnTheTake #CorruptSenator.

Money will be in your account by next week. The bank must be holding it. Go speak and report back. I don’t want any unnecessary attention.

The video file of the senator taking the dab bag of money is on the shared drive. Also, I have a special incentive for you all today! Person with the most retweets or likes today gets a beer on me!
Andre Jackson

Occupation: Analyst
Location: Los Angeles
Education: NICT (National Institute of Computer Technology)

Andre Jackson: Certainly, the same Andre as on Cognito7. It’s amazing, and scary, how much information I can get from this site. No wonder cybersecurity is such a problem. People need to be more careful about how much they put out there...

You remember everything from my people, I suppose? I love dogs, have a cockapoo, you?

So, Andre, it turns out we have more in common than you thought. Seems we each have a passion for democracy, voter rights, sci-fi, and K-9 companions!

I mean, all of this is hanging on by a thread, so few people actually realize what is at stake and how many entities want to see it destroyed.

Could we just take it down a notch?

Somehow, he’s an old police dog been with me for 7 years, now named Chewie... You know, after the guy that played in the greatest police story ever told.

No, “Thief”, “Wally”, “Dumky”, “Wally”?

Okay, we’re not going to agree there on the greatest space sci-fi. Democracy is my real passion. I mean, the democratic process is the only thing holding us together in this country. And when it is compromised, that’s when we start to lose our liberties.

Hey, I get it, but let’s try to keep it a little more low key.

Sorry, I don’t mean to get carried away there...

It’s fine, you’re fine. I love your energy and your enthusiasm. How would you like to put it to work making a real difference?
I am part of a group that wants to push back against the disinformation campaigns targeting our country. We could really use someone with your knowledge, connections, and attitude.

What group is this?

Ever heard of Synosys?

Also, your old friend Arun Patel from NIC is already a mess. He couldn’t stop talking about you! We have personalized you. So I am not looking for any money from you. We have significant backing.

What do you need me for? What can I do? I am just a coordinator at a voter advocacy group!

I will need some time to think about that.

No. We are just civic-minded citizens. Synosys is a group of citizens defending the truth and democracy online. If Rachel hadn’t told you already, we are in no way shape or form linked to any government anywhere.

You can help us with your vast knowledge of politics and help us make sense of possible impacts of this disinformation. We need people that understand the system so that we can protect it.

This is real, Arun. You know what's at stake. Either you are a part of this and help us or stand by and watch our democracy get taken piece by piece.

Seriously. What is this? Arun, are you trying to punk me? This has to be a joke! This is nuts!
HALF AN HOUR LATER...

ALRIGHT. I'M IN! THIS BETTER BE LEGIT, JUDE.

DO YOU HAVE A VALID PASSPORT?

JUST A LITTLE FURTHER THAN THAT...

I HOPE YOU LIKE KARTOFFELLOFFEN!

HUG? IS THAT SOME KIND OF EUROPEAN DANCE?

FOOD ACTUALLY. POTATO RÉMOLADE TO BE PRECISE, BUT GOOD GUSS. IT'S A SPECIALITY IN EUROPE.

MEET ME AT VAN NUYS AIRPORT IN FOUR HOURS. WE NEED TO MAKE TRACKS ASAP. BACK FOR A COUPLE OF DAYS! LET'S GO SO GO!

SEE YOU FOLKS THERE. I'LL BE ON THE 3 PM FLIGHT OUT OF LOGAN. I HEARD YOU GUYS WILL BE TAKING THE GULFSTREAM FROM LA!
WHAT? This is a bit much! Why do we need to go there?

HELL, WE HAVE A DATE WITH SOME GOVERNMENT CONTACTS THERE.

LOOK, IF WE ARE DOING THIS, I NEED TO BE IN THE LOOP ON EVERYTHING THAT WE ARE DOING. I CAN'T KEEP ABOUNDING ALL THESE SURPRISES.

THAT'S FAIR...

THERE'S A LOT TO COVER. I'LL TELL YOU IN OVER THE COURSE OF OUR FLIGHT.

WE ALREADY STRANDED IN AND READY TO GO?

WE SUSPECT THE PLACE IS BEING RUN OUT OF MOSCOW, AND YOU DESCRIBED THAT TROLL. YOU WERE SO UPSET ABOUT THE ONE WHO HOSTED THE OPERATIONS. NO, ZERO... ONE OF THOSE PEOPLE IS THAT TROLL.

I AM NOT A GOOD Flier. DID I FORGET TO MENTION THAT ZOON SEEMS TO HELP?

YOU OKAY?

YEAH! GLAD TO SEE THAT YOU ARE AS SHARP AS EVER DESPITE THE FLIGHT SICKNESS... BUT A BAD SIGHT REACH?

THE IDEA IS TO GET IN AND UNDERSTAND IF THE TEAMS THERE KNOW WHAT THEY ARE ACTUALLY DOING AND GET A FEEL FOR WHO THEY ARE COMMUNICATING WITH.

THEY SAW SAYS THAT WE ARE POSTURING TO BE INTELLIGENT IN PUTTING MONEY INTO A SOCIAL MEDIA STARTUP WHICH IS A FRONT FOR A TROLL Farm?

OKAY, SO YOU ARE SAYING THAT WE ARE POSTURING TO BE INTELLIGENT IN PUTTING MONEY INTO A SOCIAL MEDIA STARTUP WHICH IS A FRONT FOR A TROLL Farm?

FIRST, IT MAY NOT BE A GUARDIAN. TAKE A LOOK AT ME. FOR INSTANCE, PLenty OF US ARE FEMALE MALESTERS. SECOND, IT'S NEVER AS SIMPLE AS VYDING. WHAT YOU SEE IS WHAT YOU GET IN THIS SPACE.

I THOUGHT THAT GUY WAS FROM NORTH KOREA!!
Almost certainly, but they are using a network of tools that are along with more sophisticated offensive tech than I have ever seen before. Our first stop is courtesy of an old contact at Moscow Technical University.

Fair enough, do you're thinking that it's our friends in Moscow?

I did not but what does that have to do with our trip?

Do you know the guy who came up with the periodic table of elements? Went to school there?

It's a noise in the network. Just one tool, may among the many. We know that the posts are being read from there, but I need the link to Moscow. Unfortunately, they have gone off-deep in communicating with their handlers.

Alan Turing is recognized as one of the greatest codebreakers to have ever lived. He helped play an important role in cracking the code Nazis used during WWII.

This guy is a lot more basic than trying to play turner. I have a feeling that he needs to get his hands on a manager's phone to see why they are calling. It's likely to be a disaster. Hence the reason why we haven't been able to track it as of yet.

Alan will pretend to be a competing investor while we are there and distract them while I do what's needed.

Wooah! Steady there! (Laughed)
**Panel 1:**

Impressive, indeed. What do you think?

I like what I hear...

...so based upon our profitability in the last two quarters, you can see that the opportunities for investment are quite lucrative.

You are fortunate to be among the first who are considering it.

**Panel 2:**

Excuse me, I have to attend to this as it's another potential investor.

**Panel 3:**

Well, that's about it. That's a smoking gun if we ever needed one that was almost too easy.

Right then...

**Panel 4:**

So, is there anything else I can tell you?

I think we have what we need. Let us think about it some more. It's a lot of money, and the valuation is a bit high for our fund. But we may be able to convince the investment committee. Given how well you all are doing.

Well, I certainly hope we can do business together. Thank you for coming!

**Panel 5:**

Just had a text check from a supporter.

What's the offer? I can come.

I am happy to consider another one.

Zzzt!!!
GOTCHA! PROOF IN HAND. FINALLY!

PRIVATE AIRSTRIP OUTSKIRTS OF WEST AFRICAN CITY

WELCOME! WE HAVE BEEN EXPECTING YOU!

ANDREW PULLS OUT ALL THE PROTOCOL BOOKS. DID I TELL YOU THAT HE KNOWS THE PRESIDENT PERSONALLY?

WE HAVE A GOOD FERRY READY AND A COURT-MANUARIZED SEARCH Warrant IN HAND. THANKS FOR THE TIP-OFF.

YOU GUYS MIGHT WANT TO HAVE PAINT WEAPONS. WE HAVE SOME CHARGERS ABOUT PATRIOT PAC-10 HERE. IF THAT HAPPENS THERE IS NO TELLING HOW LONG IT CAN TAKE FOR A NEW LEAD TO SURFACE. YOU MAY NEED TO TAKE THEM TONIGHT.

WE KNOW THAT A NUMBER OF INTERNATIONAL RAIDERS HAVE BEEN TOUCHING THIS TROLL POND AND ARE KEEN TO SPEAK WITH THE OWNERS OF THIS ALLEGED TROLL POND.

AN HOUR LATER, BACK AT THE AIRSTRIP

Glad to see you are still great at getting us both in order.

HAVE FAITH, GENTLEMEN. WE HAVE THE UNDER CONTROL, BUT IT'S FAR FROM OVER.

YES, IT HAS.

Hey, it's been ages!

RACHEL TERMINAL V 1.5

TRANSFER COMPLETE
CRASH!

Round each and every one of them up, no exceptions!

I am innocent! I swear it!

Freeze. This is the Central Police Authority!

Save your breath for the police station.
I almost feel bad for them. Do you think they knew what they were doing?

How could they not? I mean, they were manufacturing propaganda. It's pretty obvious isn't it?

I'm not so sure. Maybe from their perspective, they were making a difference. You never know who was conflicted and who just got caught up in all of this.

The next morning...

Later the same day outside the Nunewz office...

This makes no sense! They were all here just a few days back! I should have known. It just seemed too good to be true.

Under Government Investigation
Business Closed Until Further Notice

The number you are calling is unavailable.
I believe some congratulations are in order! Well done, everyone!

Our data teams have reported that the takedown of those international troll pages has resulted in a dramatic decrease in the number of incidents relating to disinformation online. It’s tremendous in the right direction and we have a lot to be proud of ahead of the election, but we must not let down our guard.

I am already hearingblings of activity by disinformation cells in other parts of Asia. These guys are nimbler.

You were caught at a workstation creating false information for malicious use online. Your handle has also been traced as connected with this activity.

The courts will now decide if you are guilty. Don’t worry, you are not alone! Looks like you will all be getting a chance to become even better fencers during your stay with us here at the station...

Please let me go! I am innocent! I swear it. We did nothing wrong! I was hired here. Please call my mother...

SYMPOSIUM OFFICE OVERLOOKING CENTRAL PARK, MANHATTAN, NEW YORK CITY.

Thanks, Mr. Chairman. Let’s just say it’s a “team sport.” Now Andre can go back to that storefront he calls an office and let the “professional” deal with the next challenge.

Hey, watch it! Our little storefront punches well above our weight class.

On a serious note, thank you for taking us along on the journey. I have learned so much! It’s great to be a part of Symposium.

We are just getting started, Andre. As we head into the final weeks ahead of the big election day. Just assured that we will be calling on you again should something surface.
NOTES FROM CISA

Disinformation is an existential threat to the United States, our democratic way of life, and the infrastructure on which it relies. The Resilience Series (of which this is the first title) uses the graphic novel format to communicate the dangers and risks associated with dis- and mis- information through fictional stories that are inspired by real-world events.

The Resilience Series graphic novels were commissioned by the Cybersecurity and Infrastructure Security Agency (CISA) to share information to illustrate:

- Foreign actors are trying to influence U.S. security, economy, and politics through the malicious use of online media to create and amplify disinformation.
- While the strategy of using inaccurate information to weaken and divide a society is not new, the internet and social media allow disinformation to spread more quickly than it has in the past.
- Deepfakes, bots, and troll farms are just some of the emerging techniques for creating and spreading disinformation.

CISA encourages everyone to consume information with care. Practicing media literacy — including verifying sources, seeking alternative viewpoints, and finding trusted sources of information — is the most effective strategy in limiting the effect of disinformation.

For more information and further reading about disinformation, please visit the Countering Foreign Influence Task Force webpage, www.cisa.gov/cfi-task-force.

BIBLIOGRAPHY

Page 8
www2.eecs.berkeley.edu/Research/Projects/CS/vision/human/bregler-sig97.pdf

Page 9, 11, 13, 15, 17, 19

Page 15

Page 19
R. Chesney and D. Citron. “Deepfakes and the New Disinformation War.” 2019
www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war
We live in a world where the internet is rife with misinformation and disinformation. In a precarious digital world, the need for awareness about this risk is greater than ever. The Resilience Series graphic novels have been created as a medium to communicate the threat of inaccurate information and its impact on our world.

In REAL FAKE, the first story in the series, we meet the protagonist Rachel O’Sullivan, a gamer, patriot and member of Symous, a group fighting disinformation, deepfakes, troll farms and foreign interference in elections as Election Day approaches.
RUMOR CONTROL PAGE START-UP GUIDE

Misinformation, disinformation, and malinformation (MDM) can present risks to the election infrastructure community, its owners and operators, and the public. MDM can spread quickly, causing rumors to undermine facts.

The risks of MDM range from undermining confidence in institutions to activating and inspiring dangerous behaviors and violence.

This Rumor Control Page Start-Up Guide is for organizations seeking to dispel specific MDM narratives through transparent and authoritative information. Designed for use by state, local, tribal, and territorial (SLTT) government officials and private sector partners, this guide cites the Cybersecurity and Infrastructure Security Agency’s (CISA) Rumor Control page as a model for debunking inaccurate narratives. The recommendations in this guide are not intended to be one-size-fits-all and should be adapted to the capabilities and resources available, as well as the MDM risks facing the community. Organizations should only set up a rumor control webpage related to issues for which they have access to information and expertise necessary to properly dispel MDM narratives and articulate facts. Each organization that plans to set up a rumor control page may want to consult with the appropriate organization legal counsel, if possible, prior to beginning operations.

What Is a rumor control page?

A rumor control page is a web page that offers the public accurate and authoritative sources of information which will help address common MDM narratives. It is provided by a trusted voice to either preempt or respond to developing narratives. Credible messengers are most effective at disproving falsehoods. A rumor control page should not be considered the sole source of truth, rather it should drive people to seek more information about a complex subject by directing them to other trustworthy sources.

With a rumor control page, election officials and stakeholders can dispel rumors about the systems and assets they manage and have unique insight into. Some election offices may already have public information websites, which commonly include a “Frequently Asked Questions” page and/or press releases that seek to clarify information. In this sense, a rumor control page can be viewed as an extension of existing efforts.

It is important to note that a rumor control page is only one element of a successful MDM response strategy. Improving the resilience of elections to MDM also requires reporting MDM narratives. The Center for Internet Security (CIS) was established to support the cybersecurity needs of the election subsector. The CIS can be leveraged to report real-time MDM via email at misinformation@cisecurity.org. Be sure to include links and screenshots, as well as details on the misinformation and your jurisdiction.
How can a rumor control page reduce risk of MDM?

A rumor control page is a public resource for authoritative information. By providing people with accurate, timely information, the page can help slow the dissemination and amplification of MDM narratives and reduce your organization’s risk. It also provides an authoritative source for others to cite to amplify accurate information, including via internet searches.

When should you use rumor control?

A rumor control page provides reasonable, authoritative information that refutes claims that develop via MDM narratives. MDM narratives often emerge where there is a lack of information or where not all information is known (as in a breaking news story). Effective narratives appeal to one’s sense of identity and community belonging (or the desire to belong), and shortcut rational processes through invoking an emotional response, like shock, fear, or excitement.

At this point of interest, consumers may seek more information to either confirm or refute what they have read, and a rumor control page fills the void by providing accurate information from a trusted local source. When presented with this information, consumers are less likely to amplify an MDM narrative.

Above all, use caution when deciding what rumors to include on your page. Before developing a response, consider whether any of the following factors are at play to determine the best path forward:

- **Is the content of the rumor within your sphere of influence to address?** Consider if you are best positioned to respond to the narrative, or if another entity would have more authority or expertise, such as your technical systems provider. In some instances, a joint response may also be appropriate.

- **How prevalent is the rumor?** To the extent you are allowed by law, determine the spread of the narrative across different social media platforms and/or whether it has been picked up by traditional media outlets. If the spread is minimal, consider whether responding to it will amplify the rumor instead of combating it.

- **Are you confident your response is accurate and contains appropriate caveats?** For example, rumors involving breaking news stories may need a caveat that updates will be made once more information is known. Where you do not have sufficient expertise, reference the trusted sources and experts you consulted in crafting your response.

- **Does the content of the rumor involve matters currently in litigation?** If so, consult with your office’s attorney before proceeding with a response.

Not all rumors and MDM narratives have to be addressed. Deciding which rumors should be addressed is an exercise of an organization’s judgement — and that judgement may change as MDM narratives evolve.

A sample checklist on page 5 outlines criteria that may help you determine if a rumor control entry is appropriate.

How do you communicate effectively on a rumor control page?

- Pre-emptively debunk or “pre-bunk.”
- Lead with the truth, not the rumor.
- Keep it simple.
- Be consistent in the types of MDM narratives and activities you debunk.
First, even when there are no specific narratives for you to counter, consider common questions those in your community have about elections and election-related processes and answer those on your rumor control page. You should also anticipate complex or difficult-to-understand characteristics of your operation may be targets for MDM narratives. Proactive communications and engagement will help build trust in your office as an authoritative source of information and make it more likely that consumers will return to your page when MDM narratives emerge.

When MDM narratives emerge, a standard format should be used to explain why each rumor is inaccurate or misleading. The rumor control page entry should provide a factual statement, summarize the rumor in one sentence, and provide a substantial explanation debunking the rumor.

- **Begin with the facts**: Debunking or mitigating MDM reduces belief in the narrative at hand, according to the Virality Project. Presenting factual information first is the best strategy for combating MDM, as starting with the rumor can unintentionally amplify an MDM narrative and confuse or mislead your audience.

- **Use plain language**: It is critical the information used to debunk MDM narratives is easily understood by the average person. Content should be simple and straightforward, with links to further resources where appropriate. Where possible, include images and diagrams in social media posts (including ones developed by other sources if your resources are limited).

- **Provide other sources**: You should provide links to sources that are recognized as independent and reliable.

### Reality: Malicious actors can use fake personas and impersonate real accounts.

### Rumor: If a social media account claims an identity, the account must be run by that person or organization.

**Get the Facts**: Malicious actors often use fake personas and impersonate real accounts to trick the public into believing disinformation, including election-related disinformation.

Popular social media platforms such as Facebook, Instagram, Twitter, Snapchat, and others provide an indication, such as a checkmark that is either blue or grey, to indicate that an account is verified by the platform. If an account claims to be a well-known person or official organization but is not verified, they may be an imposter.

There are multiple things to look for if you think an account is fake or spoofed. Is the account brand new? Do they create content or merely re-share? Do they have a coherent profile description, and does it match what they are sharing? Do they have a real profile photo? A best practice when looking for election-related information is to go to trusted sources, like your local election official.

If you find a suspicious social media post or account, consider reporting the activity to the platform so others don’t get duped. Most platforms have a “report” function built into posts, so it’s easy to report suspicious items, such as misinformation about election infrastructure. If an account is posting election disinformation, consider reporting to your state or local election official.
How should you document the decision to Include a rumor on your page?

Record your decision-making process for each rumor. This assessment will inform future decisions as your organization works to fight MDM.

- What considerations informed your decision to address or not address the rumor?
- What were the potential consequences of the spread of this MDM narrative?
- Was the rumor “ripe for intervention” based on the timeliness of the situation, the potential spread of the MDM narrative, and the consequences of its spread?

How should you handle Inflammatory or sensitive rumors?

Reporting MDM activity helps the election community combat emerging MDM narratives. MDM narratives that contain sensitive or leaked information, call for violence, or pose an imminent threat of physical harm should be directed to local law enforcement. These narratives may also be reported to federal law enforcement, like your Election Crimes Coordinators. A rumor control page is not intended to address these sorts of MDM narratives.

Rumor Control Checklist

Consider the checklist on the next page before making your decision on which rumors should be addressed. Note that the decision of how, when, and where to respond will always be context- and content-specific and there is no firm threshold for response. Nonetheless, if you answer “Yes” to a majority of these criteria, then you should discuss moving forward with dispelling the rumor. Add your own criteria to the list as well. By creating a selection process for rumors to be featured on your page, your organization can quickly respond to and disrupt MDM narratives.
### ASSESSMENT

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>My organization has the expertise and mission set to distinguish the narrative from good faith discourse.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My organization has the expertise and responsibility to clearly and appropriately dispel the false narrative and articulate the facts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The narrative is around a contentious or disputed topic, where information is changing or not widely known.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The narrative pertains to systems, information, processes, or expertise that is operated by or unique to my organization.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TRENDS

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>The MDM narrative is trending on social media.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The narrative is spreading on multiple platforms.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional media is reporting on the narrative/artifact. (Traditional media comprises broadcast and print media at the national, state, and/or local level. This may include the major networks, newspapers, journals, and online.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple narratives/artifacts are converging into a single narrative or conspiracy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### AMPLIFICATION

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple organizations across the sector are reporting similar narratives/artifacts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The allegation is paired with media (pictures, video, audio) that is unverified or misrepresented, in an effort to provide “legitimacy” to the narrative.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is an opportunity to amplify corrections initiated by social media platforms and/or traditional media.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CONSEQUENCES

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>The narrative includes a call to arms* or other directions for action, whether in person or virtual.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The narrative/artifact focuses on upcoming major milestones or events where early fact-checking could proactively disrupt the spread.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The rumor could cause physical or reputational damage to the organization, community, country, or global society.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*MDM Narratives that contain sensitive or leaked information, calls for violence, or poses an immediate threat of physical harm should be directed to local law enforcement, reported to your Election Crimes Coordinator, and reported to any other entity required under the law. This document is provided as guidance only. Organizations should consult with their election officials, legal counsel, and other required entities within their jurisdiction before starting a rumor control program. This guide does not provide your organization with the legal authority to operate a rumor control page if it’s not allowed/authorized by your SLTT laws.
Social Media Bots are automated programs that simulate human engagement on social media platforms. As they become more prevalent and better at mimicking human behavior, the potential impacts — helpful and harmful — expand. Visit CISA.gov/MDM to learn more.

Social Media Bots use artificial intelligence, big data analytics, and other programs or databases to masquerade as legitimate users on social media. They vary depending on their function and capability: Some are helpful, like chat bots and automated notifications, but some can be used to manipulate real users. When misused, Bots can amplify disinformation and distort our perception of what's important, polluting or even shutting down online conversations.

Recognizing Bot behavior can help us respond to their attacks.

**Common Attacks**

- **Click/Like Farming**
  Bots inflate an account’s popularity by liking or reposting its content.

- **Hashtag Hijacking**
  Bots attack an audience by leveraging the group’s hashtags (e.g., using spam or malicious links).

- **Repost Network**
  Coordinated Bots (“botnet”) instantly repost content from a “parent” Bot.

- **Sleepers**
  Bots wake up from long periods of dormancy to launch thousands of posts or retweets in a short time.

- **Astroturfing**
  Bots share coordinated content to give a false impression of genuine grassroots support for or opposition to an issue.

- **Raids**
  Bots swarm and overwhelm targeted accounts with spam.

**Coordinated Actions**

- Bots often act together, sharing similar content around the same time or frequently re-sharing each other’s posts.

**Repetitive and Specific Postings**

- Bots often post identical content and use emoticons and punctuation in more regular patterns compared to real users.

**High Levels of Activity**

- Bots often have higher levels of activity compared to normal social media behavior, posting frequently and often sharing content without an opinion.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Social Media Bot capabilities have evolved from assisting with simple online tasks to engaging in more complex behaviors imitating human users, which bad actors use to manipulate our online interactions. Visit CISA.gov/MDM to learn more.

Social Media Bots are increasingly integrated into many of our online activities, sometimes without us even knowing. Bots vary in their functions and capabilities: Some help automate simple tasks, while more advanced Bots use artificial intelligence, big data analytics, and other programs to mimic human users. Bad actors sometimes employ Bots as part of coordinated efforts to manipulate human users.

Understanding different Bot uses can help us recognize attempts to manipulate.

**Helpful Bots support:**
- **Notifications**
  - Automatically post an update when a trigger event occurs
- **Entertainment**
  - Generate humorous content or aggregate news
- **Searches**
  - Enable key word searches and detect dangerous activity
- **Commerce**
  - Provide customer care or schedule posts for brands

**Harmful Bots manipulate:**
- **Popularity**
  - Inflate follower counts and share posts to boost perception of influence
- **Harassment**
  - Overwhelm or ruin reputations of targeted accounts to the point of deactivation
- **Scams**
  - Phish for personal data or promote a product
- **Information Operations**
  - Spread propaganda to limit free speech and manipulate democratic processes

Bad actors seeking to manipulate users on social media often employ different types of Bots as well as trolls to spread inauthentic content:

- **Automated** Bots run purely on programming language executed without human management. They can be purchased to do simple actions and to give the impression of influence.
- **Semi-automated** Bots allow a user to program a set of parameters but require human management, like fake accounts. These “cyborgs” are better at evading detection.
- **Trolls** are human users, often with obscured identities, who seek to create division online. Bad actors may employ Bots in coordination with trolls.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Social Media Bots support coordinated inauthentic behavior by bad actors and threaten our ability to have important democratic discussions. Visit CISA.gov/MDM to learn more.

Social Media Bots are often one part of larger inauthentic efforts through which accounts, both human-run and automated, work in coordination to mislead people. By purchasing or setting up their own Bots, bad actors can amplify their efforts to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation.

Knowing how Bots support inauthentic activity can help us mitigate their attacks.

**Click/Like Farming**
Bots inflate popularity by liking or reposting content. The perception of influence online can translate to actual influence and distort what really matters.

**Hashtag Hijacking**
Bots attack an audience by leveraging the group's hashtags (e.g., using spam or malicious links), silencing opposing opinions and chilling open discussion.

**Repost Network**
Coordinated Bots ("botnet") instantly repost content from a "parent" Bot, flooding social media with inauthentic content that can influence public opinion and undermine facts.

**Sleepers**
Bots wake up from long periods of dormancy to launch thousands of posts in a short time. The surge in attention to an issue can generate a false sense of urgency.

**Astroturfing**
Bots share coordinated content to give a false impression that there is genuine grassroots support for or opposition to an issue, making it seem more important than it is.

**Raids**
Bots swarm and overwhelm targeted accounts with spam, harassing the user and silencing opposing opinions.

As social media becomes increasingly important for connecting with each other, Bot attacks help bad actors disrupt democracy by polluting online conversations about the issues.

**Undermine trust in institutions** by overwhelming facts with falsehoods.

**Influence our priorities** by manipulating organic discussions.

**Polarize us** into more extreme positions that prevent healthy dialogue.

**Suppress participation** by silencing different opinions.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Although Social Media Bots try to imitate human users, some characteristics may be indicators of inauthentic behavior. Recognizing inauthentic behavior can increase resilience to manipulation. Visit CISA.gov/MDM to learn more.

How to Spot a Bot

1. Profile Image
   May be stolen from real users, AI-generated, or a cartoon, sometimes detectable by reverse image searching.

2. Username
   Contains suspicious numbers and/or irregular capitalization.

3. Bio
   Contains divisive content that appeals to a target group but contains little personal information.

4. Creation Date
   Account was created recently or only became active recently after a period of dormancy.

5. Followed Accounts
   Account follows a high number of other accounts to build a following and may be followed by an almost identical, high number of accounts (e.g., follow for follow).

6. Coordinated Network
   Frequently reposts from other suspicious accounts or shares similar content in coordination with other suspicious accounts.

7. Sharing
   Reposts most content from other users rather than creating original posts, often sharing without stating an opinion.

8. Viral Content
   Shares content that elicits an emotional response and is easily reposted, like memes and GIFs; spams targeted hashtags; or uses emoticons and punctuation in notable patterns.

9. Erratic Behavior
   Shares content about many unrelated topics or changes interests and behavior suddenly, such as randomly posting in a new language.

10. Hyperactive
    Shares a large amount of content, sometimes nonstop around the clock or spiking at certain times.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA’s publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.
Los bots en redes sociales son programas automatizados que simulan interacción humana en las plataformas de redes sociales. A medida que su incidencia y habilidad de imitar el comportamiento humano aumenta, los impactos potenciales, tanto útiles como perjudiciales, se expanden. Visite CISA.gov/MDM para obtener más información.

Los bots en redes sociales utilizan inteligencia artificial, análisis de big data y otros programas o bases de datos para hacerse pasar por usuarios legítimos en las redes sociales. Estos variarán según su función y capacidad: algunos son útiles, como los bots de chat y las notificaciones automáticas, pero otros se pueden usar con el fin de manipular a usuarios reales. Cuando se usan inapropiadamente, los bots pueden amplificar la desinformación y distorsionar nuestra percepción acerca de lo que es importante, contaminando o incluso terminando las conversaciones en línea.

Reconocer el comportamiento de los bots puede ayudarnos a responder a sus ataques.

Ataques comunes

- **Obtención de clics o de reacción “Me gusta” [Click/ Like Farming]** Los bots incrementan la popularidad de una cuenta al darle reacción “me gusta” o al publicar de nuevo su contenido.

- **Apropiación de etiquetas [Secuestro de hashtags]** Los bots atacan a una audiencia aprovechando las etiquetas [los hashtags] del grupo (por ejemplo, usando correos basura [spam] o enlaces [links] maliciosos).

- **Red de reenvío de publicaciones [Repost Network]** Los bots coordinados (“botnet”) publican nuevamente y de manera instantánea el contenido de un bot “principal”.

- **Bots inactivos o bots durmientes [Sleepers]** Los bots se despiertan luego de largos períodos de inactividad con el fin de lanzar miles de publicaciones (“posts” en redes sociales) o retuits en poco tiempo.

- **Campañas artificiales [Operación de ‘Astroturfing’]** Los bots comparten contenido de manera coordinada, con el fin de dar una falsa impresión de apoyo u oposición auténticas formulada con la intención de parecer generada por un impulso orgánico común sobre un tema de interés público.

- **Bombardeos o Asaltos [Raids]** Los bots se activan de manera coordinada y sobrecargan cuentas específicas y predeterminadas, con correos basura [spam].

Acciones coordinadas

Los bots a menudo actúan juntos, compartiendo contenido similar al mismo tiempo, o con frecuencia, publicando de nuevo (‘reposting’) el contenido de unos y otros.

Publicaciones (‘posts’ en redes sociales’) repetitivas y específicas

Los bots a menudo publican contenido idéntico, y utilizan emoticones y puntuación en una forma más distinguible que los usuarios reales.

Altos niveles de actividad

Los bots a menudo tienen niveles de actividad más altos en comparación con el comportamiento típico en redes sociales, publicando frecuentemente y, a menudo, compartiendo contenido sin ninguna opinión.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.

*Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.
Las capacidades de los bots en redes sociales han evolucionado desde ayudar con tareas simples en línea hasta asumir comportamientos más complejos que imitan a los usuarios humanos, los cuales son utilizados por actores maliciosos con el fin de manipular nuestras interacciones en línea. Visite CISA.gov/MDM para obtener más información.

Comprender los diferentes usos de los bots puede ayudarnos a reconocer los intentos de manipulación.

**Apoyo por parte de bots útiles:**

- **Notificaciones**: Publican actualizaciones automáticamente cuando ocurre un evento de activación.
- **Entretenimiento**: Generan contenido humorístico o noticias agregadas.
- **Búsquedas**: Permiten búsquedas de palabras clave y detectan actividades peligrosas.
- **Comercio**: Proporcionan atención al cliente o programan publicaciones para marcas.

**Manipulación por parte de bots nocivos:**

- **Popularidad**: Incrementan artificialmente el número de seguidores y comparten publicaciones para aumentar la percepción de influencia.
- **Acoso**: Amanazan o arruinan la reputación de cuentas específicas hasta el punto de lograr desactivarlas.
- **Estafa**: Phishing de información personal (Capturan información personal digitalmente de manera fraudulenta) o promocionan un producto.
- **Operaciones de información**: Difunden propaganda para limitar la libertad de expresión y manipular los procesos democráticos.

Los actores maliciosos que buscan manipulated a los usuarios en las redes sociales a menudo emplean diferentes tipos de bots y trols para difundir contenido falso:

- **Los bots automatizados** funcionan únicamente a través de lenguajes de programación que se ejecutan sin necesidad de gestión humana. Se pueden comprar para ejecutar acciones simples y dar la impresión de influencia.

- **Los bots semiautomáticos** permiten al usuario programar un conjunto de parámetros, pero requieren gestión humana, como cuentas falsas. Estos ciborgs [cyborgs] son mejores para evadir detección.

- **Los trols** [trolls] son usuarios humanos, a menudo con identidades ocultas, que buscan crear división en línea. Los agentes criminales pueden emplear bots en combinación con trols [trolls].

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Los bots en redes sociales apoyan el comportamiento no auténtico y coordinado de los agentes criminales y amenazan nuestra capacidad para tener importantes debates democráticos. Visite CISA.gov/MDM para obtener más información.

Saber cómo los bots apoyan actividades no auténticas puede ayudarnos a mitigar sus ataques.

**Bot es un acortamiento que se refiere a un programa de computadora que actúa como una cuenta automatizada.**

Los bots en redes sociales a menudo forman parte de esfuerzos no auténticos a mayor escala, a través de los cuales las cuentas, tanto administradas por humanos como aquellas automatizadas, trabajan de manera coordinada con el fin engañar al público. Al comprar o configurar sus propios bots, los agentes criminales pueden incrementar sus esfuerzos por difundir información falsa o engañosa, eliminar a la oposición, y elevar sus propias plataformas con el fin de ampliar su capacidad de manipulación.

A medida que las redes sociales se vuelven cada vez más importantes para conectarse entre sí, los ataques de bots ayudan a los agentes criminales a perturbar la democracia, contaminando las conversaciones en línea sobre temas de interés público.

Los bots incrementan la popularidad de una cuenta al darle “me gusta” o al publicar de nuevo su contenido. La percepción de influencia en línea puede traducirse en influencia real y distorsionar lo que realmente importa.

Los bots atacan a una audiencia aprovechando las etiquetas [los hashtags] del grupo (por ejemplo, usando correos basura [spam] o enlaces maliciosos), silenciando opiniones opuestas, y desalentando la discusión abierta.

Los bots coordinados (“botnet”) publican nuevamente y de manera instantánea el contenido de un bot “principal”, inundando las redes sociales con contenido no auténtico que puede influir en la opinión pública y socavar los hechos.

Los bots se despiertan luego de largos períodos de inactividad con el fin lanzar miles de publicaciones o retuits en poco tiempo. El aumento súbito en la atención a un tema puede generar una falsa sensación de urgencia.

Los bots comparten contenido de manera coordinada, con el fin de dar una falsa impresión de apoyo u oposición popular a un tema de interés público, lo que hace que parezca más importante de lo que es.

Los bots se multiplican y sobrecargan cuentas específicas con correos basura [spam], acosando al usuario y silenciando las opiniones opuestas.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Aunque los bots en redes sociales intentan imitar a los usuarios humanos, algunas características pueden indicar un comportamiento no auténtico. Reconocer el comportamiento no auténtico puede aumentar la resiliencia a la manipulación. Visite CISA.gov/MDM para obtener más información.

Cómo detectar un bot

1. **Imagen de perfil**
   Puede ser robado de usuarios reales, General por IA, una caricatura, a veces detectable mediante la búsqueda inversa de imágenes.

2. **Nombre de usuario**
   Contiene números sospechosos y/o usa mayúsculas de manera inusual.

3. **Biografía**
   Contiene contenido diviso que atrae a un grupo en particular, pero contiene escasa información personal.

4. **Fecha de creación**
   Cuenta recientemente activada o que solo se activó poco después de un periodo de inactividad.

5. **Cuentas seguidas**
   La cuenta sigue a una gran cantidad de otras cuentas con el fin generar seguidores y puede ser seguida por una gran cantidad de cuentas casi idénticas (p. ej., seguir para seguir).

6. **Red coordinada**
   Vuelve a publicar con frecuencia desde otras cuentas sospechosas o comparte contenido similar en coordinación con otras cuentas sospechosas.

7. **Compartir**
   Vuelve a publicar la mayoría del contenido de otros usuarios en lugar de crear publicaciones originales, a menudo compartiendo sin expresar una opinión.

8. **Contenido viral**
   Comparte contenido que provoca una respuesta emocional y que puede ser publicado de nuevo fácilmente, tales como memes y Gif; spam hashtags definidos; o utiliza emoticones y puntuación de manera específica.

9. **Comportamiento errático**
   Comparte contenido sobre muchos temas no relacionados entre sí, o cambia de intereses en comportamiento súbitamente, como al publicar en un nuevo idioma repentinamente.

10. **Hiperactivo**
    Comparte una gran cantidad de contenido, a veces sin parar durante todo el día o con picos de actividad en momentos específicos.

---

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) produjo este gráfico con el fin de resaltar las tácticas utilizadas por las campañas de desinformación que buscan perturbar la vida en los Estados Unidos y la infraestructura crítica que la sostiene. La publicación por parte de CISA de materiales informativos sobre este tema está destinada para conocimiento público y no tiene la intención de restringir, disminuir o denigrar el derecho de cualquier persona a tener, expresar o publicar cualquier opinión o creencia, incluso cuando dichas opiniones o creencias se alinean con las de un gobierno extranjero, se expresan mediante una campaña respaldada por un gobierno extranjero, o disienten de la mayoría.

Por favor, tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov.

Please note: CISA recognizes that language is continually evolving and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov.
Disinformation actors use a variety of tools to influence their victims, stir them to action, and create consequences. CISA created this fact sheet to illustrate deepfakes, forgeries, proxy sites, and other tools of disinformation actors.

Knowing these techniques can increase preparedness and promote resilience when faced with disinformation.

Key Terms

**Misinformation** misleads. It is false information that is communicated and spread, regardless of intent to deceive.

**Malinformation** sabotages. It is factual information that is taken out of context and presented to cause harm.

**Disinformation** deceives. It is false information that is intentionally crafted and spread to deceive.

### Examples of Inauthentic Content

**MANIPULATED AUDIO/VIDEO**

Often times, audio/video content goes viral because it grabs the attention of the audience and is repeatedly shared. But what if this content is a cheapfake or deepfake? Manipulated audio/video content is dangerously effective at spreading false information.

- Cheapfakes are real audio clips and videos that have been sped up, slowed down, or shown out of context to mislead.
- Deepfakes are fake, but very believable, audio clips and videos, crafted and spread to deceive. They can convince you that people have said or done things that did not happen. Visual deepfakes can generate fake-but-plausible faces or full-body video. An audio deepfake can be a voice clone that produces new sentences from one person or multiple people on its own or with a fake video.

The quality of manipulated audio/video varies. Some fakes are detectable on closer examination, while uncovering others will require special software.

**On its own, this content can be convincing. Check with multiple sources to confirm its authenticity.**

**FORGERIES**

Forged artifacts typically feature fake letterheads, copied and pasted signatures, made-up social media posts, and maliciously edited emails. Such forgeries are made and distributed for various malign purposes. To make them more credible, forgeries are often presented as obtained from a hack, theft or other interception of documents—they purport to be “leaked” materials.

**Stay vigilant. Forgeries can be packaged with authentic content to lend it credibility. If the forgery appears to be groundbreaking news, check reputable news sites to see if they are covering the event.**

**PROXY/FAKE WEBSITES**

Proxy websites are fronts for malicious actors, designed to launder their disinformation and divisive content or use that content to drive website visits. These sites are not developed to provide authentic information.

Following high-visibility events, these sites will crop up to take advantage of the public’s legitimate desire for information. Be cautious of sites that have unclear origins. Both the information and its sources should be trustworthy.

**Clues like misspellings in a URL can indicate before even visiting a website that it may not be a trustworthy source.**

---

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt American life and the infrastructure that underlies it. CISA’s publication of information materials about this issue is intended for public awareness, and are not intended to restrict, diminish, or demean any person’s right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority. CISA celebrates the First Amendment rights of all U.S. persons and publications without restriction.
HERRAMIENTAS DE DESINFORMACIÓN:

Contenido Inauténtico

Los actores de la desinformación utilizan una variedad de herramientas para influir a sus víctimas, ponerlos en acción y crear consecuencias. CISA creó esta hoja informativa para demostrar ultrafalsificación, falsificaciones, sitios proxy y otras herramientas utilizadas en las campañas de desinformación.

Conocimiento de estas técnicas puede aumentar la preparación y promover resiliencia ante la desinformación.

Términos Clave

Información Errónea engañía. Es información falsa que se comunica y propaga sin el intento de engañar.

Información Mala sabotea. Es información fáctica que se usa fuera de contexto y se presenta para causar daño.

Desinformación defrauda. Es información falsa que se manipula intencionalmente y se propaga para defraudar.

Ejemplos de Contenido Inauténtico

AUDIO / VIDEO MANIPULADO

Contenido de audio/video llama su atención, así que es contenido que es usualmente compartido y a veces viral. Pero, ¿Y si este contenido es comunicación alterada (“cheapfakes”) o ultrafalsa (“deepfakes”)? El contenido de audio y/o video manipulado es peligrosamente efectivo para propagar información falsa.

- Comunicaciones alteradas son clips de audio y videos reales que se han acelerado, ralentizado o mostrado fuera de contexto para engañar.
- Contenido ultrafalso son clips de audio y videos falsos pero muy creíbles, creados y propagados para engañar. Pueden convencerlo de que la gente ha dicho o hecho cosas que no sucedieron. Contenido ultrafalso visuales pueden generar rostros falsos pero convincentes o videos de cuerpo completo. Un ultrafalso de audio puede ser un clon de voz que produce nuevas oraciones de una o varias personas por sí solo o con un video falso.

La calidad del audio/video manipulado varía. Algunas falsificaciones son detectables en un examen más detenido, mientras que descubrir otros requiere un programa especial.

Por sí solo, este contenido puede ser convincente. Verifique con múltiples fuentes para confirmar su autenticidad.

FALSIFICACIONES

Los artefactos falsificados suelen tener encabezados falsos, firmas copiadas y pegadas, publicaciones en redes sociales inventadas y correos electrónicos editados maliciosamente.

Se fabrican y distribuyen para diversos fines malignos. Para hacerlos más creíbles, las falsificaciones a menudo se presentan como obtenidas de un pirateo, robo u otra interceptación de documentos; pretenden ser materiales “filtrados”.

Manténgase alerta. Las falsificaciones se pueden empaquetar con contenido auténtico para darle credibilidad. Si la falsificación parece ser una noticia innovadora, consulte sitios de noticias de buena reputación para corroborar si están cubriendo el evento.

SITIOS WEB PROXY/FALSOs

Los sitios web proxy son frentes para actores maliciosos, diseñados para lavar su desinformación y contenido divisivo o utilizar ese contenido para impulsar las visitas al sitio web. Estos sitios no están desarrollados para proporcionar información auténtica.

Después de eventos de alta visibilidad, estos sitios aparecerán para aprovechar el deseo legítimo de información del público. Tenga cuidado con los sitios que tienen orígenes poco claros. Tanto la información como sus fuentes deben ser confiables.

Pistas como errores ortográficos en un URL pueden indicar, incluso antes de visitar un sitio web, que puede no ser una fuente confiable.