APPENDIX 2

CONTENTS

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**

To view this news release in Spanish, please visit: **https://cbp.gov/newsroom/national-media-release/cbp-lanza-campa-publicitaria-digital-d-gale-no-al-coyote-para**

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
CYBER+INFRASTRUCTURE

MAY 2020

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 combatting 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.

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.

- 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

Build Your Network:

Preparing communication channels and establishing contacts before MDM incidents occur allows you the ability to quickly respond and share information.

- 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.

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.

- 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.

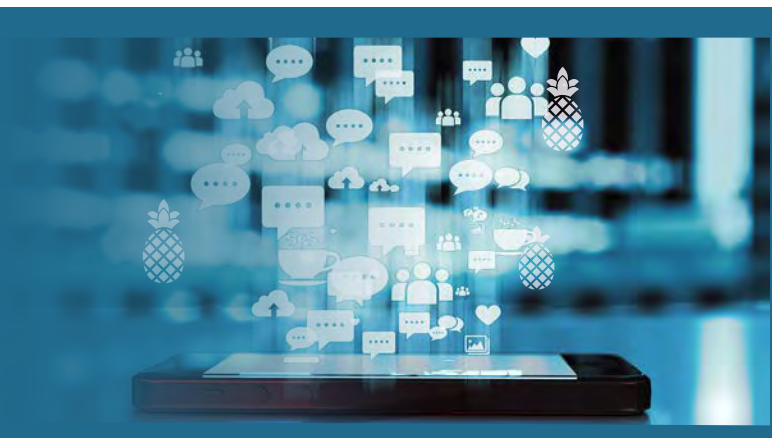
Develop an Incident Response Plan

- 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.

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.**

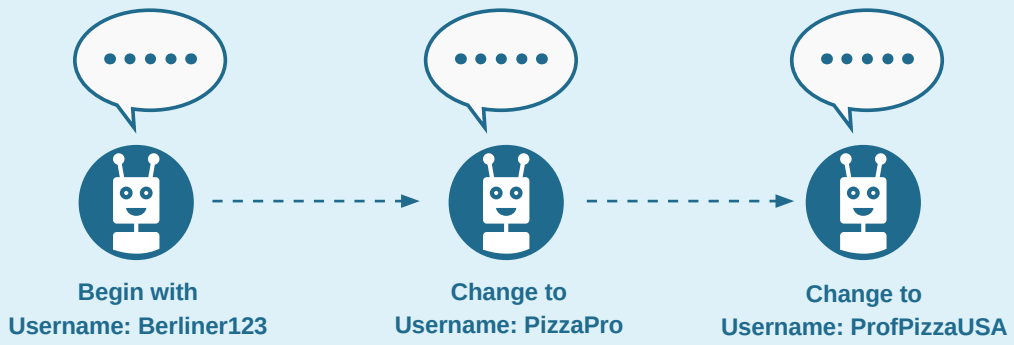
American Opinion is Split: Does Pineapple Belong on Pizza?

An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

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.

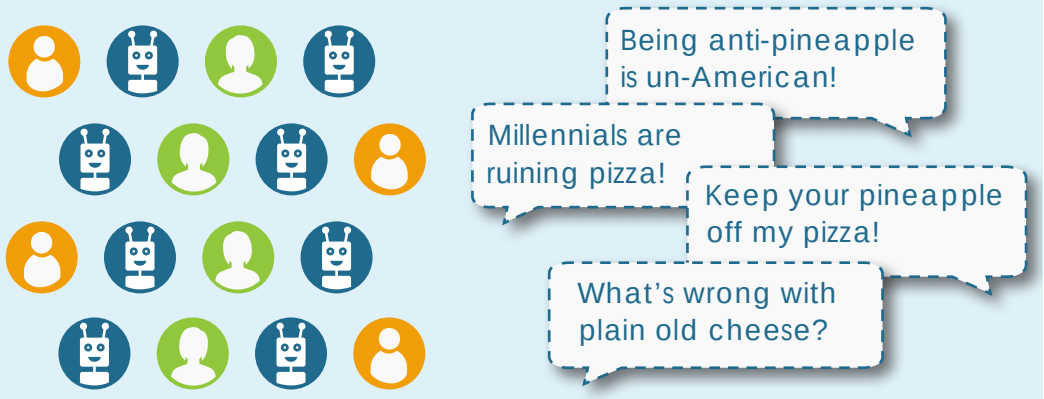
Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**



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.

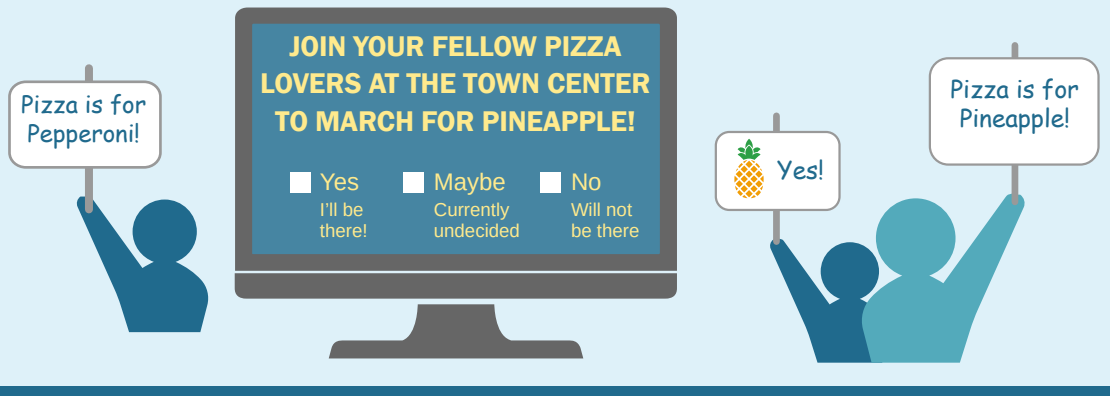
Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences**.

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 ILUSTRACIÓN 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 vernos divididos.**

La opinión estadounidense está dividida: ¿Poner piña en la pizza?

Una celebridad importante mencionó que le disgusta cuando se pone piña en la pizza, lo que impulsó un nuevo sondeo de opinión. No importa cómo se analice, los estadounidenses no están de acuerdo con el uso de frutas como ingrediente.

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.**

Empieza con el nombre de usuario: Berliner123

Cambia al nombre de usuario: PizzaPro

Cambia al nombre de usuario: ProfPizzaUSA

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 troles [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.**

Para más información, visite el sitio web de #Protect2020 en **https://www.dhs.gov/cisa/protect2020**.

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 Stops With You

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.

Share

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.

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

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

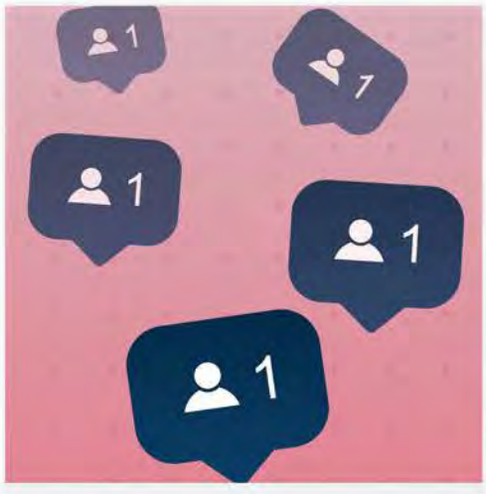
Disinformation Stops With You

Recognize the Risk

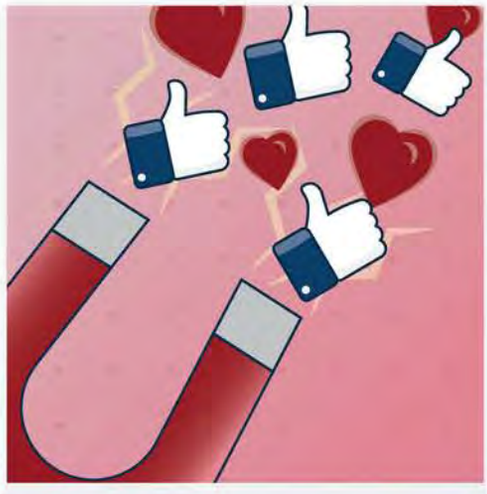
Understand how malicious influencers use disinformation to shape the conversation and manipulate behavior. Once they've built an online presence, they start to post false or misleading content that steers their audience to more extreme positions and spreads to a bigger audience.

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

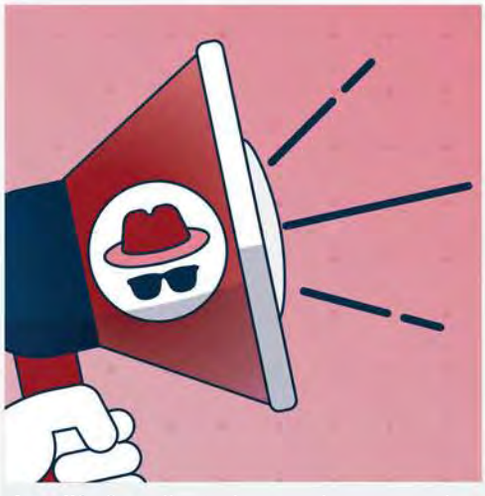
Divide Us Bad actors use divisive societal issues to polarize Americans and push us into echo chambers that further amplify disinformation and obstruct healthy conversations about the issues.



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.

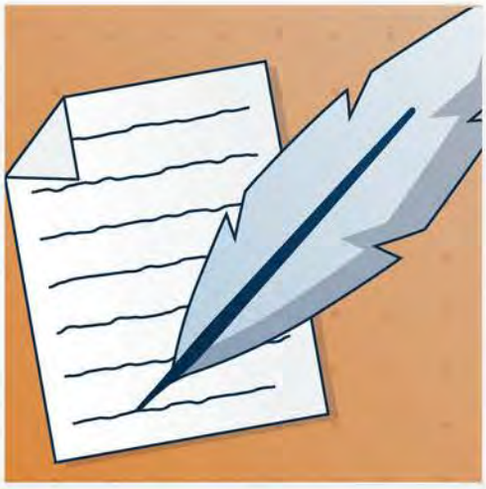
Real World Effects Bad actors use online disinformation to affect our real-world behavior, like trying to influence how we vote, inciting physical confrontations, and disrupting healthy democratic discussions and participation.

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.

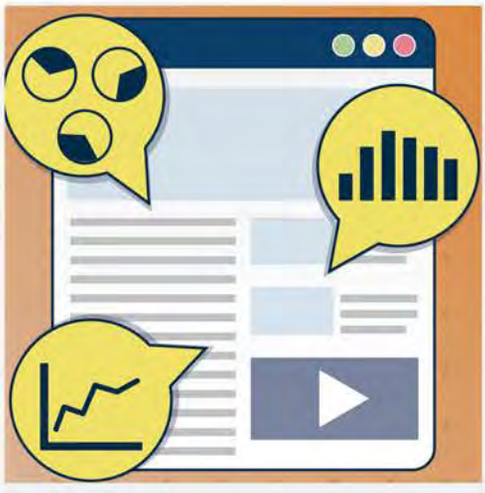
Learn more at www.cisa.gov/mdm-resource-library



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.

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.

Disinformation Stops With You

Think Before You Link

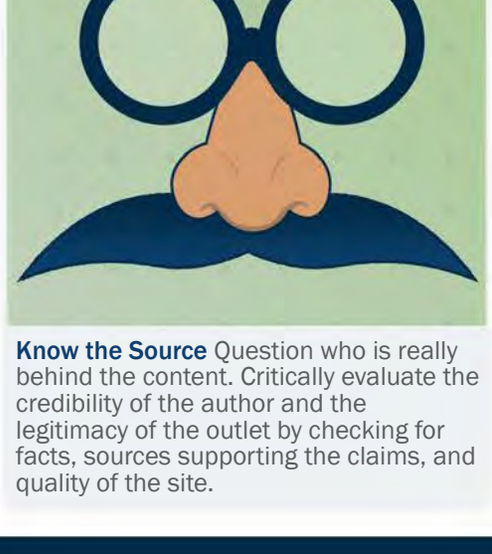
Take a moment to let your emotions cool and ask yourself whether your feelings about the content are based on fact. Disinformation is designed to evoke a strong emotional reaction that bypasses your critical thinking. You can interrupt the cycle of disinformation by taking time to research the content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

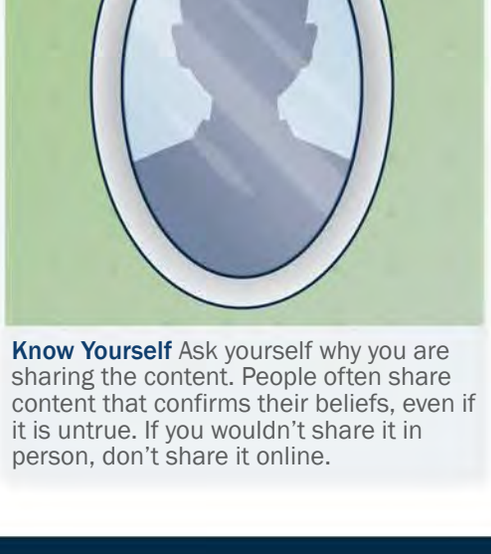
Know the Content Headlines and captions are often exaggerated to get an emotional response. Take time to read the entire post and determine whether they accurately reflect the content.

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.

Disinformation Stops With You

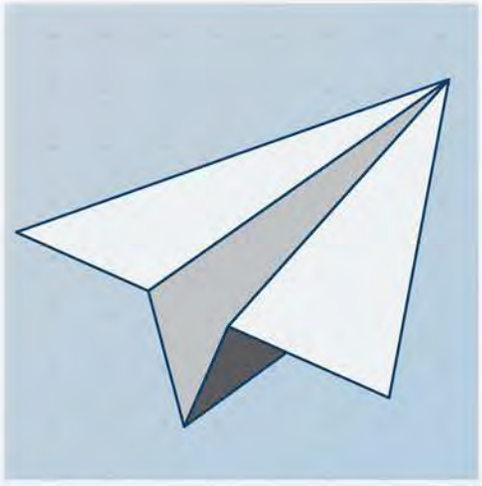
Talk With Your Circle

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.

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.

Pubicar

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.

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

A quién seguir

Fidedignas — Sigue

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

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

La desinformación se detiene con usted

Reconozca el riesgo

Cuestione la fuente

Investigue el tema

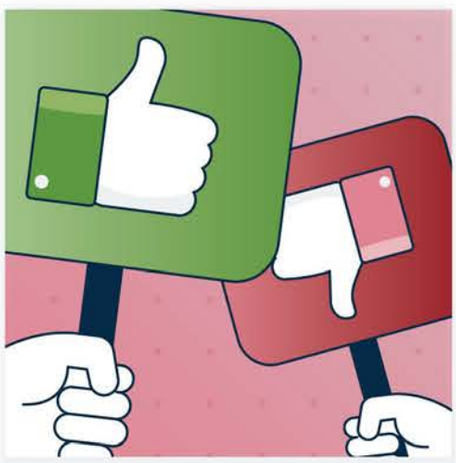
Piense antes de compartir un enlacet

Hable con su entorno familiar y social [*su círculo*]

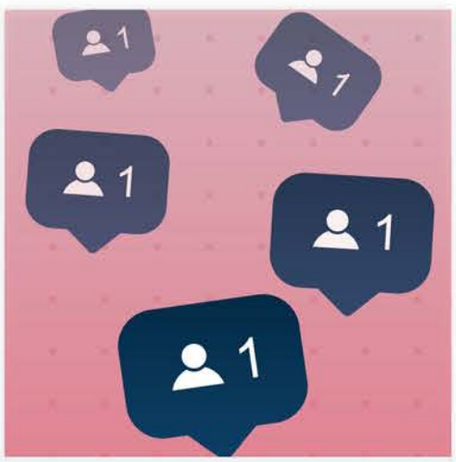
Reconozca el riesgo

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.

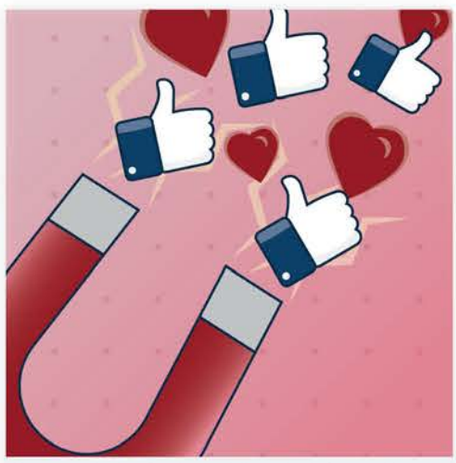
Encuentre más información en www.cisa.gov/mdm-resource-library



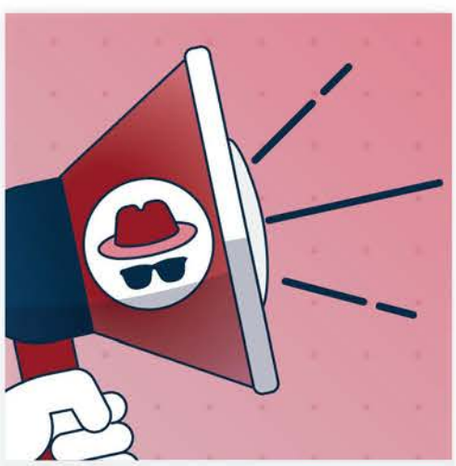
Dividirnos Los agentes criminales utilizan temas sociales divisivos con el fin de polarizar a los estadounidenses, y colocarnos en cámaras de eco [*echo chambers*] que amplifican aún más la desinformación e impiden el diálogo constructivo.



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 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

La desinformación se detiene con usted

Reconozca el riesgo

Cuestione la fuente

Investigue el tema

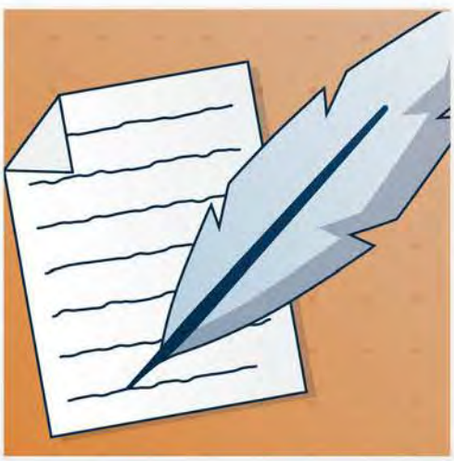
Piense antes de compartir un enlacet

Hable con su entorno familiar y social [*su círculo*]

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.

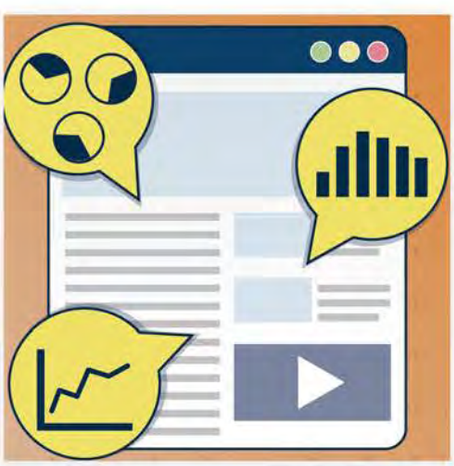
Encuentre más información en www.cisa.gov/mdm-resource-library



Verifique el autor Investigue las credenciales del autor. ¿Qué más han publicado? ¿Están calificados para discutir el tema? Si el contenido no incluye el nombre del autor, es posible que sea desinformación.

Verifique 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 el mensaje ¿Qué dice el contenido en realidad? La desinformación a menudo promueve un punto de vista único, adopta un tono emocional y utiliza titulares que llaman la atención, aunque esto no coincida con los hechos reales.



Verifique los hechos Considere cómo el autor sustenta sus argumentos y si responde a los argumentos que están en contra. Opiniones dadas sin evidencia alguna, pueden no ser exactas. Utilizar sitios web confiables que verifican los hechos puede ayudar a evaluar dichas declaraciones.

Verifique las fuentes El contenido creíble citará las fuentes de apoyo y proporcionará recursos adicionales para obtener más información. Haga clic en los enlaces de las fuentes para asegurarse de que funcionan y afirman el contenido.

Verifique la calidad La desinformación suele encontrase 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 legítimos.

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

La desinformación se detiene con usted

Reconozca el riesgo

Cuestione la fuente

Investigue el tema

Piense antes de compartir un enlacet

Hable con su entorno familiar y social [*su círculo*]

Investigue 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 comparta el contenido si este no viene de una fuente creíble o si no puede 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 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 reconocerán 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

La desinformación se detiene con usted

Reconozca el riesgo

Cuestione la fuente

Investigue el tema

Piense antes de compartir un enlacet

Hable con su entorno familiar y social [*su círculo*]

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

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 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 asegurarse de que no han sido puestas fuera de contexto.

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 la razón Los algoritmos de las redes sociales promueven contenido que consideran va a ser de su interés, a veces a través de un enfoque específico. Si fue compartido por un amigo, asegúrese de que puede confiar tanto en la fuente original, como en el amigo.

Conózcase a si 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.

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

La desinformación se detiene con usted

Reconozca el riesgo

Cuestione la fuente

Investigue el tema

Piense antes de compartir un enlacet

Hable con su entorno familiar y social [*su círculo*]

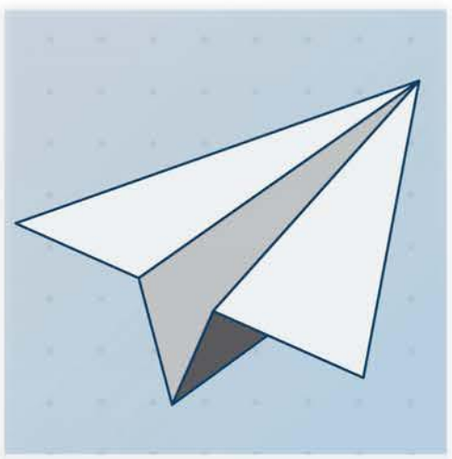
Hable con su entorno familiar y social [*su círculo*]

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

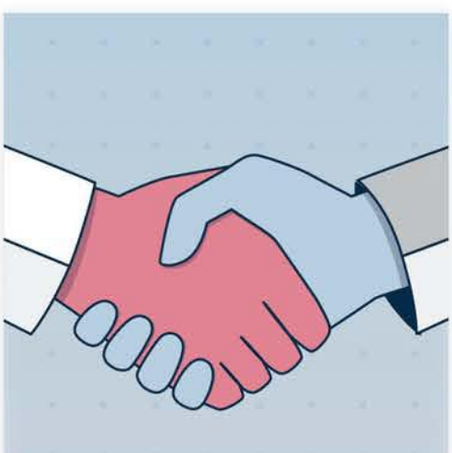
Esté preparado Asegúrese de haber investigado y de conocer los hechos antes de iniciar una conversación. Incluso si está convencido de que se trata de desinformación, revise la evidencia más reciente para estar seguro.

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.

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.

Homeland Security

FOREIGN INTERFERENCE TAXONOMY

FOREIGN INTERFERENCE

Malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies.

Trade/ Strategic Investment | **Coercion/ Corruption** | **Migration Exploitation** | **International Org. Manipulation**

INFORMATION ACTIVITIES

Activities undertaken to shape public opinion or undermine trust in the authenticity of information. 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 adversaries to commandeer and control narratives.

TRADITIONAL MEDIA ABUSE

Using traditional media outlets to report false ordistorted information, strategically leak stoleninformation, 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 activities. They 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. Compromised government systems (e.g., voting systems, data repositories) can lead to citizens to question the security of the information provided to the government.

WHAT TYPE OF INFORMATION IS USED?

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 re-purposed and distributed maliciously with the intent to deceive. Often, “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.

Homeland Security

Departamento de Seguridad Nacional de los Estados Unidos [*Department of Homeland Security -DHS*]
julio de 2018

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.

Comercio / Inversiones Estratégicas | **Coerción/ Corrupción** | **Explotación Migratoria** | **Manipulación de Organizaciones Internacionales**

ACTIVIDADES DE INFORMACIÓN

Las actividades emprendidas para moldear la opinión pública o debilitar la confianza en la autenticidad de la información. El uso de medios de comunicación tanto nuevos como tradicionales con el fin de aumentar las 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 y distorsionados en individuos o grupos predeterminados.

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 estratégicamente 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 de 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 amplifican sus narrativas. 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 reutilizadas y distribuidas maliciosamente con la intención de engañar. A menudo, los contenidos "falsos" se crean con la intención específica de engañar o incitar al público (**desinformación**).

Los hechos también se utilizan de forma maliciosa y fuera de contexto para influir indebidamente en el público (**información maliciosa**). Este tipo de contenido es en ocasiones el resultado de una actividad cibernética ilícita, como el espionaje o la piratería, y se difunde a través de terceros.

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.

Information Manipulation

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.

Manipulación de la información

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.

Actividades cibernéticas

La piratería informática [*Hacking*] puede beneficiar la manipulación de la información. Los piratas informáticos [*Hackers*] apoyan estrategias de vigilancia o reconocimiento y proporcionan oportunidades para llevar a cabo ataques destructivos. El secuestro de cuentas [*Hijacking accounts*] y la desconfiguración de sitios web públicos pueden utilizarse para influenciar la opinión pública.

Los sistemas gubernamentales en riesgo (p. ej., sistemas de votación, repositorios de datos) pueden hacer que los miembros del público cuestionen la seguridad de la información que le hayan proporcionado al gobierno.

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 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.

This document was created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint Mis/Disinformation Working Group. This document is intended to be used by state, local, tribal, and territorial election officials, and industry partners as part of a larger mis-, dis-, and malinformation (MDM) response strategy. SLTT election officials should consult with their legal officer and other necessary officials in their jurisdiction prior to creating an MDM response program.

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.[1] 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:

Impact	Description	Example (from CISA's Rumor Control page)
Procedural Interference	Narratives or content related to election procedures that cause confusion and interfere with officials' ability to smoothly administer an election.	✔ 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.
Participation Interference	Content that might intimidate or deter voters from participating in the election process.	✔ 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.
Delegitimization of Election Results	Narratives or content that delegitimizes election results or sows distrust in the integrity of the process based on false or misleading claims.	✔ 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.
Personnel Security	Narratives or content that falsely claims election officials or poll workers are the "bad actor" attempting to interfere in election results or processes.	✔ 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.

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.

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.

> 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.

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.

- 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.

Team Checklist

- ✓ Understand reporting mechanisms for flagging MDM on social media.
- ✓ Determine roles and responsibilities for MDM response.
- ✓ Designate an individual to oversee the MDM response process.
- ✓ Register your website for a .gov address.
- ✓ Apply for verification badges from social media platforms.
- ✓ Develop a list of common topics and questions vulnerable to MDM.
- ✓ Ensure your communication systems are set up to handle incoming questions.
- ✓ Engage with counsel and, if applicable, your privacy office to ensure protection of constitutional rights and privacy.

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.

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

- The Colorado Secretary of State's office conducted social media and digital outreach to voters and set up a website to educate on the threat misinformation and respond to MDM narratives.
- The Kentucky Secretary of State's office launched a Rumor Control page on their website to counter MDM narratives around elections.
- The Wisconsin Elections Commission established a designated FAQ page to answer voter questions about the 2020 election.
- The Maricopa County, Arizona, Elections Department launched a website to address questions and misconceptions about the 2020 election and has engaged in rumor control efforts across social media.

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.

5. TRACK OUTCOMES

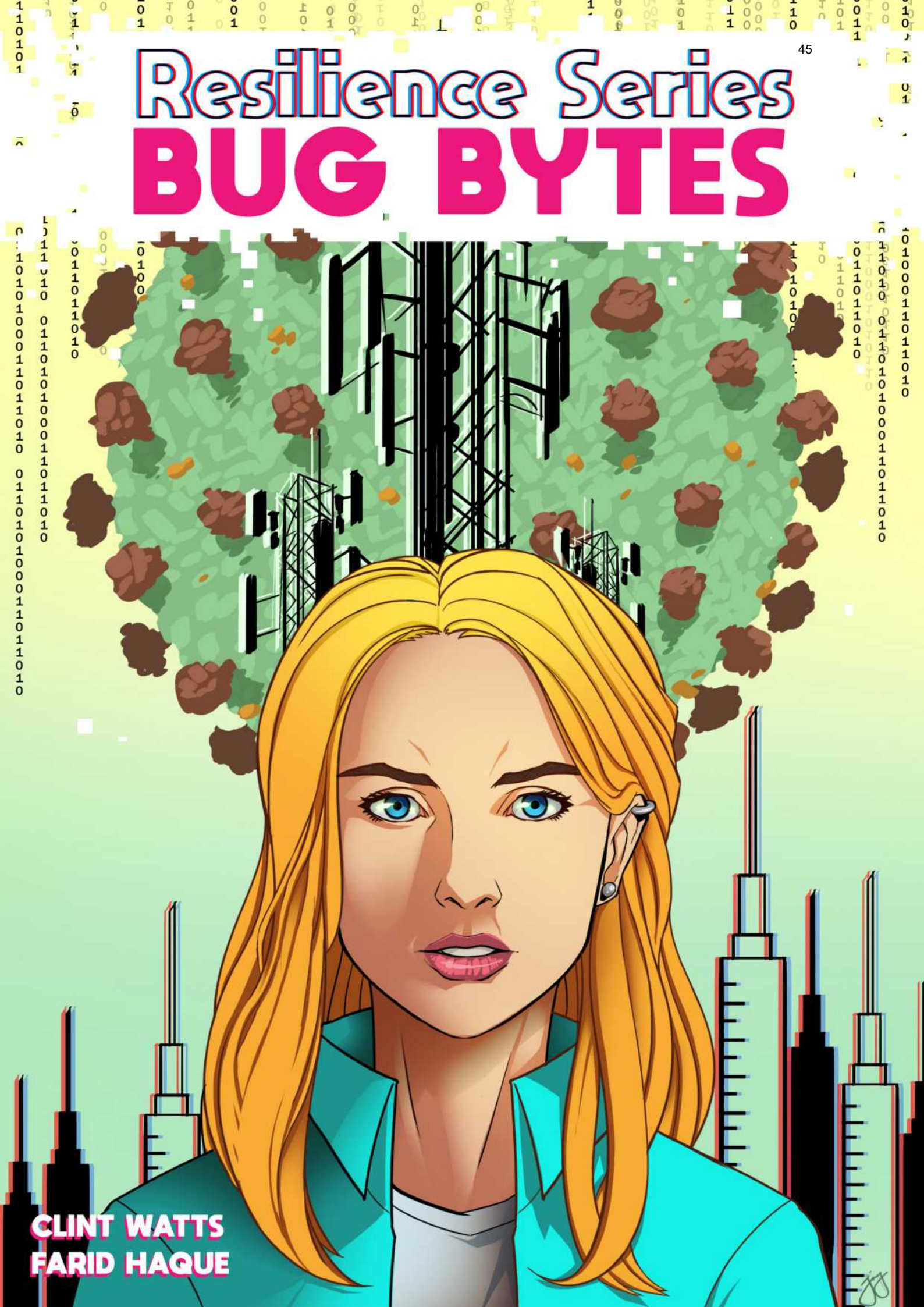
After your response, evaluate the continued prevalence of MDM and evaluate ways to adjust processes moving forward.

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.

Resilience Series

BUG BYTES



CLINT WATTS
FARID HAQUE

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 DISSENT 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.

CREDITS

STORY BY
CLINT WATTS
FARID HAQUE

ART DIRECTION
FARID HAQUE
J. NINO GALENZOGA

ILLUSTRATORS
J. NINO GALENZOGA
JOEL SANTIAGO

COLORISTS
PATRICIA BEJA
JOEL SANTIAGO

LETTERING
HAROON M.
LAILA K.
PATRICIA BEJA

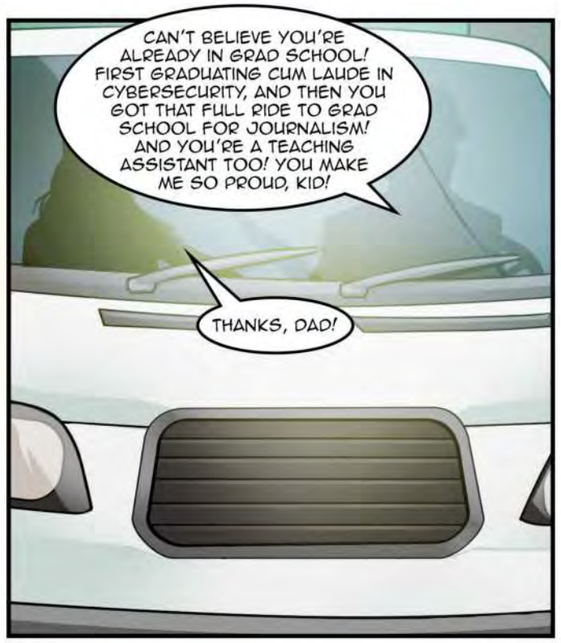
EDITORS
TOLLY M.
LAILA K.

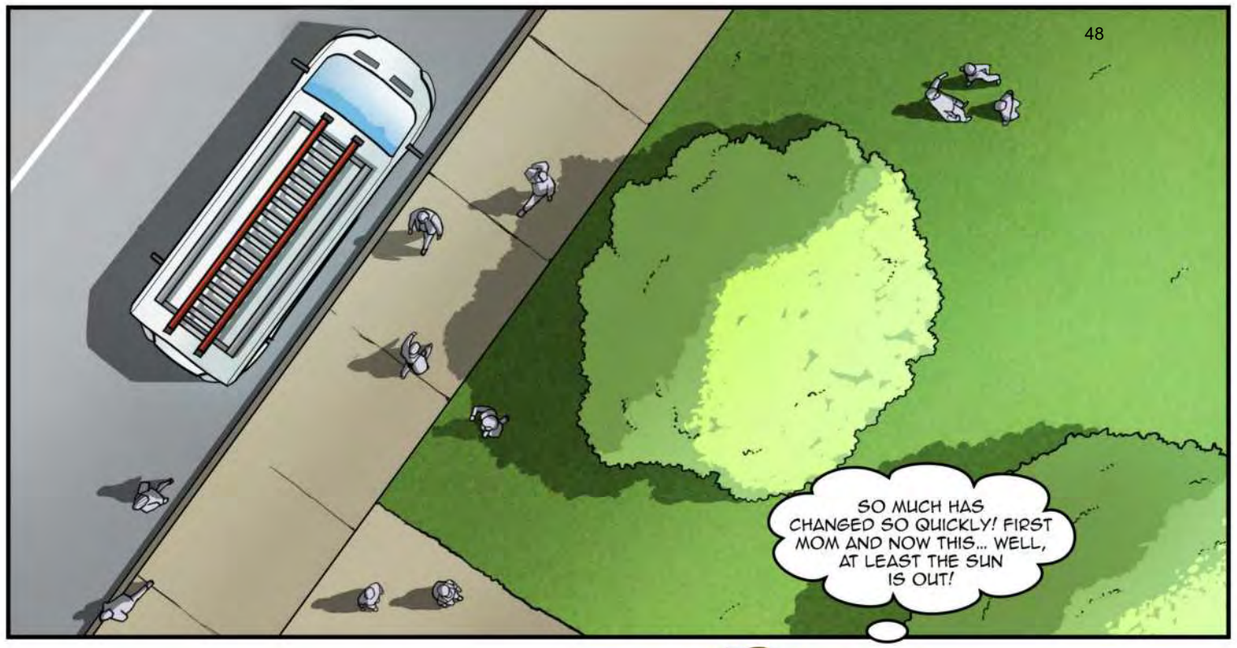
SCRIPTWRITERS
MICHAEL GIANFRANCESCO
KABIR SABHARWAL

STORY PRODUCTION
ERLY STAGE STUDIOS

PROJECT TEAM
JAMES PINSKY
PAMELA O' BRIEN SCHIPPER
ROBERT BALLAGH
JOHN ROSENBERG


5G


CAN'T BELIEVE YOU'RE ALREADY IN GRAD SCHOOL! FIRST GRADUATING CUM LAUDE IN CYBERSECURITY, AND THEN YOU GOT THAT FULL RIDE TO GRAD SCHOOL FOR JOURNALISM! AND YOU'RE A TEACHING ASSISTANT TOO! YOU MAKE ME SO PROUD, KID!
THANKS, DAD!


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


C'MON SWEETHEART, IS THAT ALL YOU GOT FOR YOUR OLD MAN?! YOU EARNED THIS! YOU'RE THE FIRST OF US TO GET TO COLLEGE, LET ALONE GRAD SCHOOL.
NOW STOP ALREADY! YOU KNOW WHAT MOM WOULD HAVE SAID.

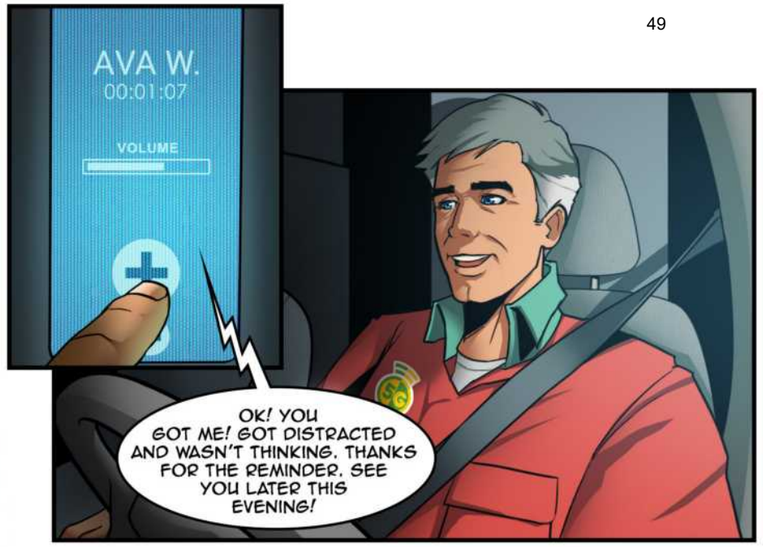

COULD YOU PLEASE PUT ON YOUR MASK! THERE ARE HUNDREDS OF PEOPLE HERE! AND... I AM NOT READY FOR YOU TO BECOME A STATISTIC!


VOLUME
...SPECIAL BULLETIN AS COVID-19 NUMBERS CONTINUE TO RISE ACROSS THE NATION.
AAAAND THIS IS ME... GOTTA GO, DAD!
1


5G
2


University of Ann Arbor
BUZZZ... BUZZZ... BUZZZ...


NOTHING, OTHER THAN I NOTICED YOU DIDN'T HAVE YOUR MASK ON... JUST REMINDING YOU TO BE SAFE!

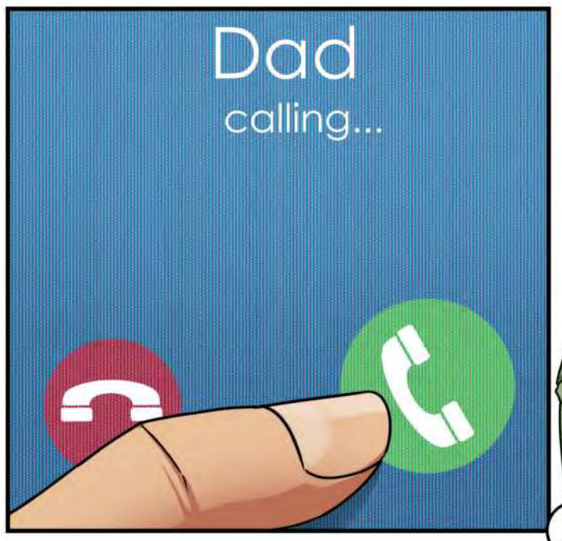

AVA W.
00:01:07
VOLUME
OK! YOU GOT ME! GOT DISTRACTED AND WASN'T THINKING. THANKS FOR THE REMINDER. SEE YOU LATER THIS EVENING!


Going to get out of your hair...
Thank you!
You know your mother would have been sobbing if she was with us...


SERIOUSLY!


YOU BETCHA!


NOW... WHERE IS MY MASK?!


Dad
calling...


WHAT IS IT, DAD?! YOU DO REALIZE THAT I AM A WOMAN IN HER MID TWENTIES...
3


4

"YOU HAVE NO NEW MESSAGES."

MORNING, JIM!

SURE THING! ...SURE THING! JUST A FEW MILES OUT...LEMME TAKE A LOOK...

MORNING, BUD. SAY, THERE'S A 5G TOWER NOT WORKING IN EAST ANN ARBOR. COULD YOU GET OVER THERE AND TAKE A LOOK? THERE SEEMS TO BE SOMETHING WRONG... DON'T THINK IT'S COMMUNICATING BACK TO HQ.

I'M ON IT, CHIEF.

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

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

5

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

YOU HAVE 3 MINUTES TO DESTINATION...

ARRIVING AT DESTINATION...

WHAT THE...

6

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

LIGHT IT UP.

7

BURRRRRN! BABY BURRRN! AND TAKE THAT NASTY DISEASE WITH YOU!

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

8

HEY! STOP!

SON OF A --

"THUD"

NO. PLEASE!

ARRRGHH...

9

CCTV 03-A34
03-14

LET GO OF ME. LET ME AT HIM!

ARE WE CLEAR?

YES.

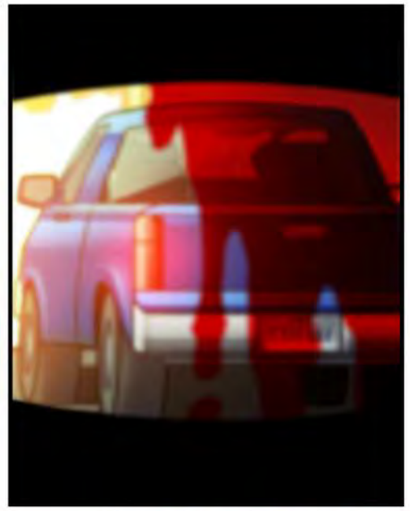
GRAB A HOLD OF YOURSELF. I KNOW YOU ARE ANGRY ABOUT HOW THESE TOWERS ARE HARMING US, BUT WE CAN'T HURT OTHER PEOPLE.

10

E33...

11

12




ALL CLEAR.
WE HAD TO IMPROVISE A BIT. WE HAD SOME COMPANY. BUT HE WON'T BE ANY TROUBLE.

13


LET'S GET THIS BEAST UNDER CONTROL!
MICHIGAN
FIRE DEPT.


GENTLE...


MR. WILLIAMS, CAN YOU HEAR ME? SIR?


HALF AN HOUR LATER, THE POLICE ENTER...
I'M REALLY SORRY TO HAVE TO DO THIS NOW...BUT DO YOU REMEMBER ANYTHING ELSE ABOUT THE ATTACKERS? THE GETAWAY VEHICLES...
I REMEMBER THE PLATES. E33...

14

HEY, SWEETIE.

DAD? ARE YOU OK?

WHO COULD HAVE DONE THIS TO YOU?!

MA'AM, HE NEEDS TIME TO REST. PLEASE WAIT OUTSIDE.

SURE...

I DON'T KNOW... I... I WAS JUMPED BY A COUPLE OF PUNKS! THEY HAD MASKS ON...AND NOT THE GOOD KIND!

OH, GOD... DAD...

MISS WILLIAMS, STAY STRONG. WE'LL DO OUR BEST TO FIND WHOEVER IS RESPONSIBLE.

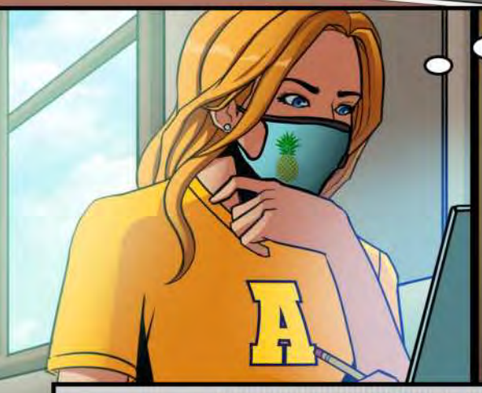
DAD, I PROMISE I'LL FIND OUT WHO DID THIS TO YOU.

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.



http://www.MakeYourOpinionCount.org/stop5G

STOP 5G CELL TOWER DEPLOYMENT IN MICHIGAN

52,063 have signed, let's get 75,000.

SEARCHOPIA

5G Attack Michig

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

I WONDER IF THESE ARE REAL...

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.

91 Reply

Tony S. . 2 hours ago

THIS IS A DANGER TO HUMANITY. IT HAS TO STOP!

52 Reply

17

https://www.photonow.com

abigail palmer

https://www.newshare.com

Dhanush Patel

Message More...

https://www.wediscuss.com

Laura Brant

https://www.friendplace.com

Abigail Palmer

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

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

LAURA BRANT, ABIGAIL PALMER, DHANUSH PATEL.

18

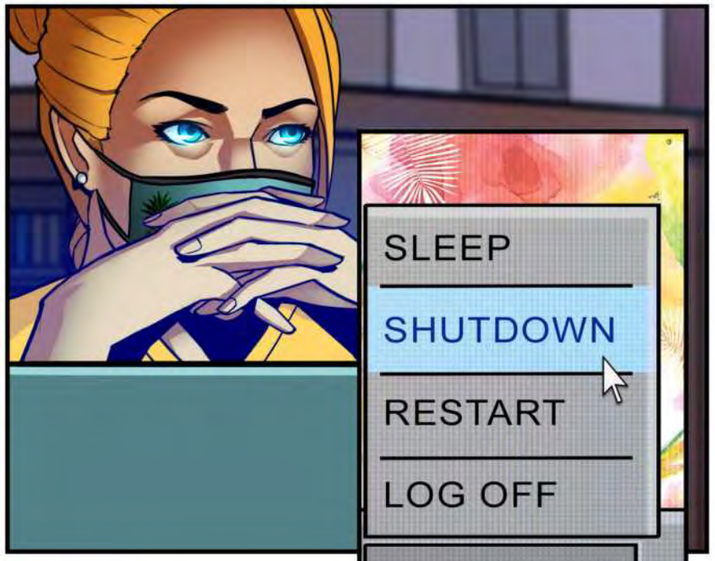
DAY TURNS INTO NIGHT.

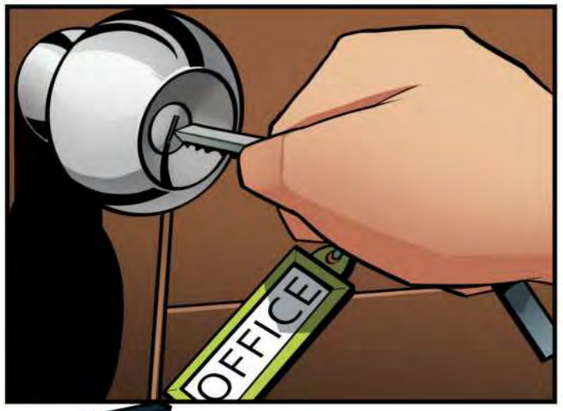
THAT'S ODD, NONE OF THEM EXIST IN PLACES YOU WOULD EXPECT OUTSIDE OF THE PLATFORMS. DIGITAL GHOSTS?

19

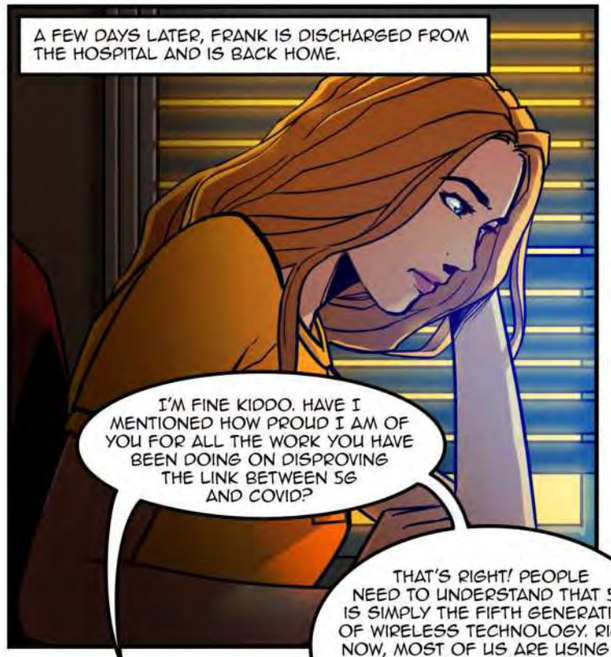
20


Anony
Mark S


SLEEP
SHUTDOWN
RESTART
LOG OFF
LAUNCH

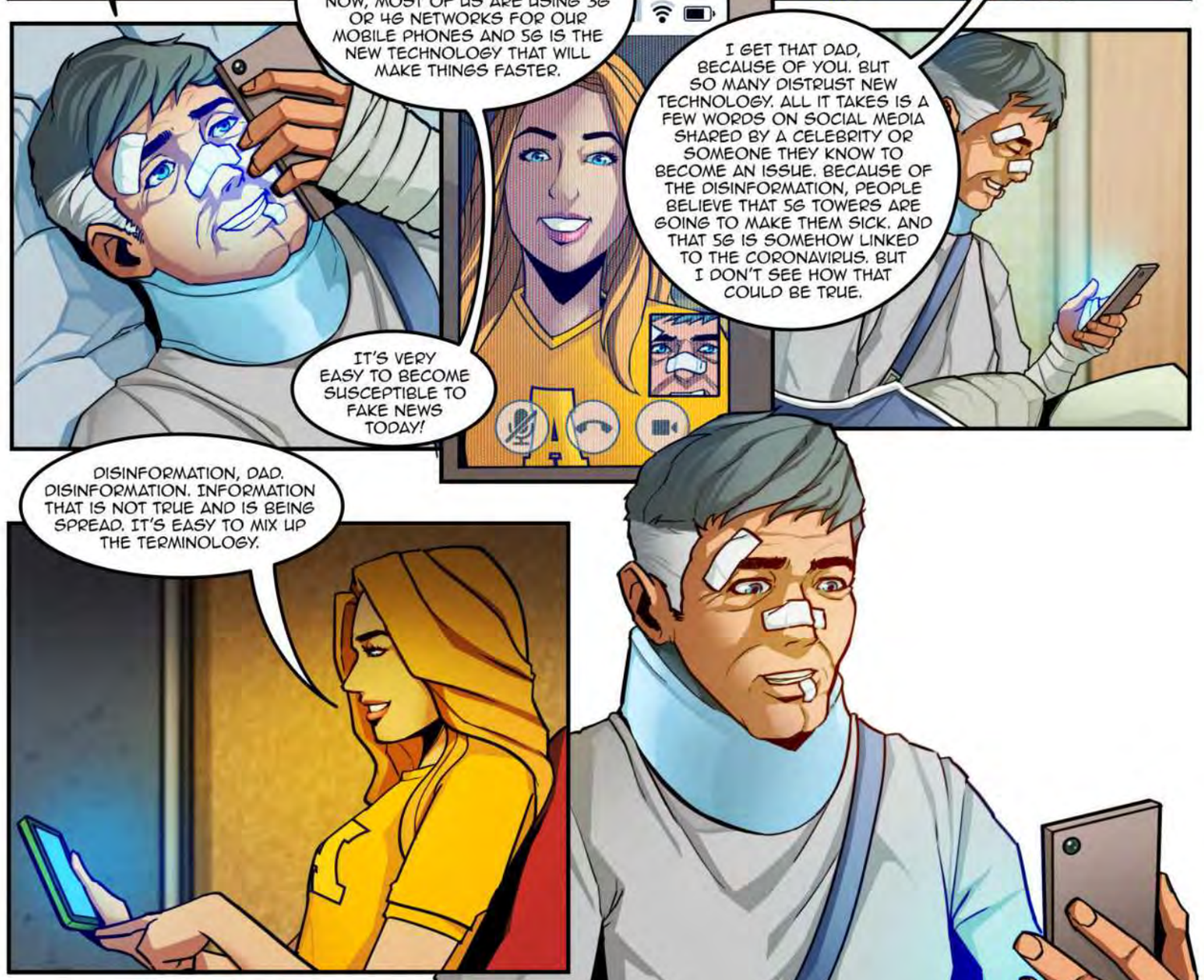

OFFICE


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 SHARED IDEALS... SOMETHING FUNNY'S GOING ON...


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?


HEY, DAD. I'M RUNNING A BIT SHORT ON TIME, BUT I WANTED TO CHECK IN ON YOU.

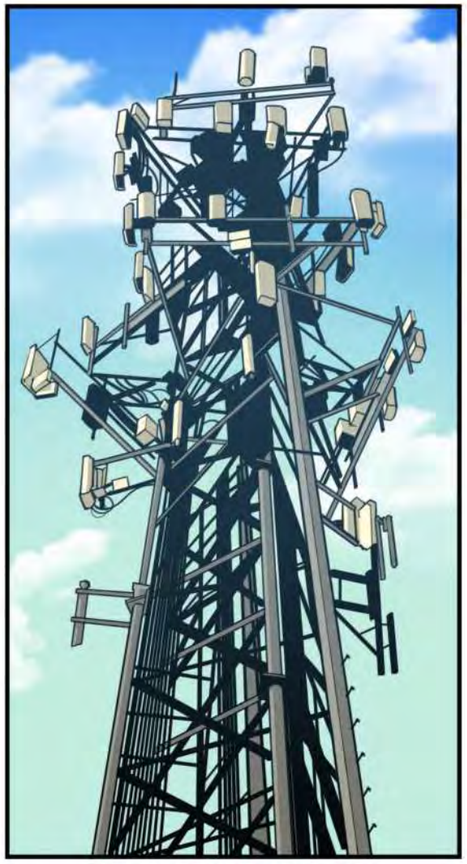

THANKS, DAD! I CAN'T BELIEVE HOW MANY PEOPLE THINK THAT THERE IS A LINK AND HAVE BEEN ATTACKING 5G TOWERS. PEOPLE DON'T REALIZE THAT THIS IS DISINFORMATION.


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.
I GET THAT DAD, BECAUSE OF YOU. BUT SO MANY DISTRUST NEW TECHNOLOGY. ALL IT TAKES IS A FEW WORDS 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 CORONAVIRUS. BUT I DON'T SEE HOW THAT COULD BE TRUE.
IT'S VERY EASY TO BECOME SUSCEPTIBLE TO FAKE NEWS TODAY!

DISINFORMATION, DAD. DISINFORMATION. INFORMATION THAT IS NOT TRUE AND IS BEING SPREAD. IT'S EASY TO MIX UP THE TERMINOLOGY.

HAHA YOU GOT ME! PEOPLE BELIEVE WHAT THEY READ ON SOCIAL MEDIA. IF I DIDN'T KNOW BETTER, I WOULD PROBABLY BELIEVE SOMETHING IF MY FRIENDS POSTED IT ON THEIR FEEDS. NO ONE TAKES THE TIME TO CHECK THIS STUFF ANYWAY.

PEOPLE ALSO ARE NOT FULLY AWARE OF WHAT 5G IS ALL ABOUT.

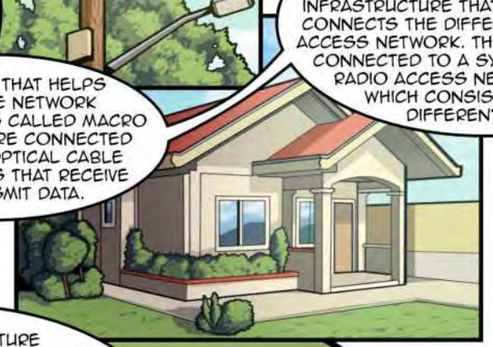


THAT IS PART OF THE PROBLEM.

5G WILL HELP US DO MORE WITH THE DEVICES AND SYSTEMS THAT WE HAVE. FOR EXAMPLE, I WOULD PROBABLY BE ABLE TO DOWNLOAD A GAME OR A MOVIE ABOUT 5 TIMES QUICKER WITH 5G.

THAT'S RIGHT! ALL OF THIS IS LINKED TO THE CORE NETWORK, WHICH IS THE BACKBONE OF OUR COMMUNICATIONS INFRASTRUCTURE THAT ROUTES DATA AND CONNECTS THE DIFFERENT PARTS OF THE ACCESS NETWORK. THE CORE NETWORK IS CONNECTED TO A SYSTEM CALLED THE RADIO ACCESS NETWORK OR RAN, WHICH CONSISTS OF A FEW DIFFERENT PARTS:

1. SOFTWARE THAT HELPS MANAGE THE NETWORK
2. LARGE TOWERS CALLED MACRO TOWERS THAT ARE CONNECTED THROUGH AN OPTICAL CABLE
3. SMALL CELLS THAT RECEIVE AND TRANSMIT DATA.



THIS INFRASTRUCTURE THEN CONNECTS TO OUR PHONES AND LAPTOPS, WHICH MEANS WE CAN DO THINGS LIKE DOWNLOAD MOVIES FASTER, LIKE YOU SAID. 5G 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 SPREADS MORE, IT COULD GET OUT OF HAND. CLAIMING THAT 5G TOWERS ARE LINKED TO THE VIRUS IS DANGEROUS – IT'S WRONG, AND THOSE CLAIMS MIGHT INSPIRE MORE ATTACKS LIKE THE ONE ON YOU, DAD!

BACK AT THE TEACHING ASSISTANT OFFICE...

THERE IS TOO MUCH DATA... I NEED TO GET SMART AND WRITE SOME CODE TO SCRAPE AND ANALYZE THIS. I KNEW THOSE COMPUTER SCIENCE CLASSES IN UNDERGRAD WOULD COME IN HANDY ONE DAY.

IT PAYS TO BE A JOURNALIST WITH A CYBER DEGREE.

```
def crawl_profile(session, base_url, profile_url, post_limit):
    """
                                                    orofile_url)
                                                    post_limit:
        sts_id = 'recent'
        ts = profile_bs.find('div', id=posts_id).div.div.contents
    except Exception:
        posts_id = 'structured_composer_async_container'
        posts = pro  bs.find('div', id=posts_id).div.div.contents

    posts_urls =                                    rofile_bs.find_all('a', text='Full Story')]

    for post_
        # print(pos
        try:
            post_data = scrape_post(session, base_url, post_url)
            scraped_posts.append(post_data)
        except Exception as e:
            logging.info('Error: {}'.format(e))
```

TAP! TAP! TAP!

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

CLICK!

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

Time of Post	Day 1	Day 2	D
3:30:24 PM	26	54	
5:33:58 PM	53	62	
6:17:46 PM	21	253	

25

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

COLLEEN, CAN YOU PING ME THE NAME OF THAT LAWYER LADY WE MET FROM DC? THE ONE WHO KNOWS A LOT ABOUT CYBER LAWS AND DISINFORMATION. THANKS!

Sondra Jefferies

WOW, SHE SEEMS LIKE THE RIGHT PERSON. SHE PRACTICES CYBER LAW.

AND... HERE'S HER NUMBER... MAYBE SHE CAN HELP!

SONDRA HERE...

HI. THIS IS AVA WILLIAMS FROM THE UNIVERSITY OF ANN ARBOR'S JOURNALISM DEPARTMENT. WE PREVIOUSLY MET...

NOT INTERESTED!

NO! WAIT--

26

SONDRA ADJUSTS HER MASK AS SHE ENTERS THE PUBLIC SECTION OF THE AIRPORT.

WHAT IS IT? MAKE IT QUICK... I NEED TO BE ON A FLIGHT IN 2 MINS...

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

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

COAST 2 COAST AIRLINES FLIGHT NUMBER W914 NOW BOARDING AT GATE 12.

MICHIGAN?

SCREEECH!

LADIES AND GENTLEMEN, WELCOME TO WASHINGTON DULLES INTERNATIONAL AIRPORT. THE LOCAL TIME IS 6:55 P.M.

...THANK YOU FOR FLYING ON COAST 2 COAST AIRLINES.

RING! RING!

YOU DON'T WASTE MUCH TIME DO YOU?

SORRY... I WAS TRACKING THE FLIGHT ONLINE...

LET ME GET MY EARPHONES ON AND WE CAN SPEAK PRIVATELY.

THE AFTERNOON TRANSITIONS INTO LATE EVENING AS SONDRA MAKES HER WAY TO THE TAXI.

OF COURSE, I'M GLAD TO HELP. IF I MAY ASK, WHY ARE YOU DOING THIS? IS IT 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 MESS! I'VE BEEN MEANING TO ASK YOU ABOUT CYBER LAW FOR QUITE A WHILE NOW. FEELS LIKE THERE MUST BE SOMETHING THAT CAN BE DONE TO FIGHT ALL THIS MISINFORMATION FLYING AROUND.

AT FIRST IT WAS PERSONAL BECAUSE MY FATHER GOT HURT, BUT I REALIZED THAT 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 MASKED MEN, WHO HE CAUGHT TRYING TO DESTROY A 5G TOWER. I DID SOME INTERNET SEARCHING AND FOUND A PETITION ON MAKEYOUROPINIONCOUNT.ORG 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 HIJACKED AND LINKED TO THE COVID-19 VIRUS. IT HAD A LITTLE OVER 50,000 SIGNATURES AND IT SEEMS THAT AROUND 15 PERCENT COME FROM WHAT LOOKS LIKE A BOT FARM. SOMEONE IS PULLING THE STRINGS ON THIS SITUATION.

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

MISINFORMATION IS MORE WHEN SOMEONE MAKES A MISTAKE SUCH AS PROVIDING FACTUALLY INCORRECT INFORMATION, BUT IT'S NOT MALICIOUS...

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

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

HAPPY 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 GOODNIGHT.

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

AND THANKS SO MUCH FOR MENTIONING ME TO YOUR CONTACT. I LOOK FORWARD TO HEARING FROM YOU!

HALF AN HOUR LATER, AVA RECEIVES AN EMAIL.

have opened this message, it will be deleted automatically in 10 minutes.
1. Create an account on BLOCKWRLD
2. Search VidView for the Secret Library
3. Under Russian Literature find book 222
4. Type a phrase from Dostoevsky's book 'The Idiot': 'I am a fool with a heart but no brains'
5. Wait for response

Love,
Symous

THE GROUP SONORA GOT IN TOUCH WITH MOVES QUICKLY! LOOKS LIKE THIS EMAIL IS FROM THEM.

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, LOG IN!

Email address: avawilliams@email.com

Repeat email address: avawilliams@ema

Password

Repeat password

BLOCKWRLD

INSTALLING...

VidView

secret library blo

secret library blockwrld

AVAlanche

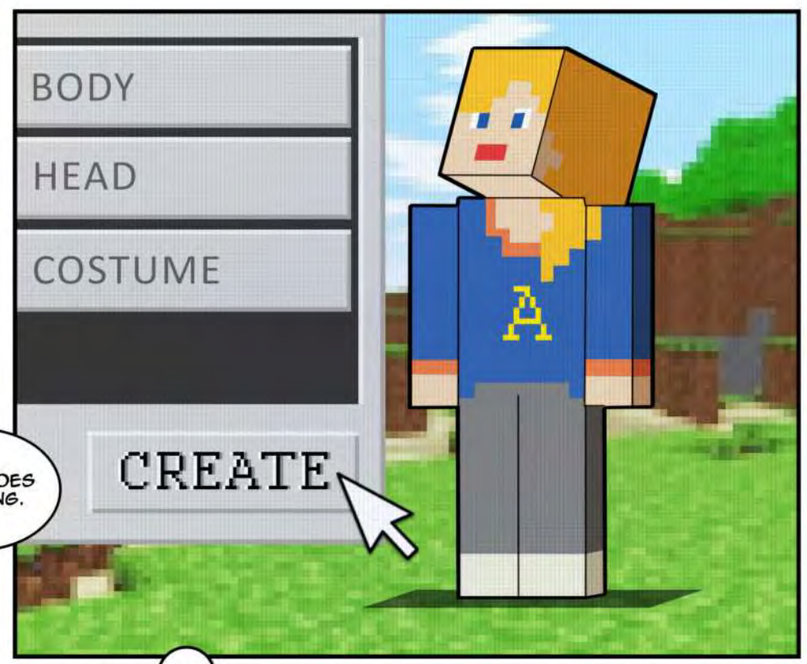
AVA'S 3D AVATAR CLIMBS THE STAIRS OF THE SECRET LIBRARY.

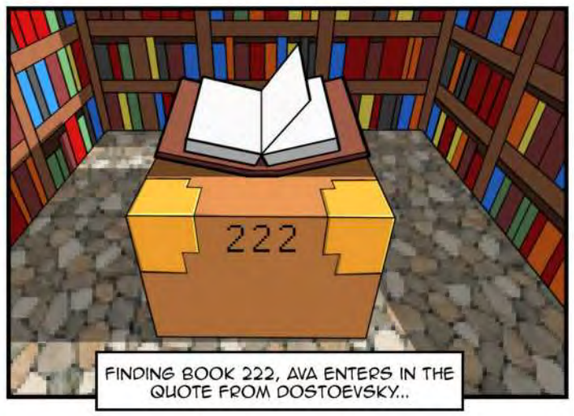
AVAlanche

RUSSIAN LITERATURE

SHE TOURS AROUND THIS VAST FACILITY, LOOKING AT OTHER 3D COUNTERPARTS AS WELL.

HERE GOES NOTHING.





FINDING BOOK 222, AVA ENTERS IN THE QUOTE FROM DOSTOEVSKY...

CHAT BOX

I am a fool with a heart but no brains

AN HOUR LATER... NO RESPONSE.

CHAT BOX

I am a fool with a heart but no brains

BEEP!!!

"THUD!"

2:22:22 AM

GASP

AVAlanche

I am a fool with a heart but no brains

?????????

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

AVAlanche

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

SEARCHOPIA and beauty will save the world

«Beauty will save the world». This is one of Dostoevsky's most often quoted sentences, but few know precisely what it means.

?????????

Lets talk on this link.
https://chairman.12345/9605/sonon.php
Don't worry.It's secure and can't be traced back to either of us.

HELLO...?

HI... I'M NOT LOOKING FOR ANY TROUBLE!

WAIT... HOW DO YOU KNOW MY FATHER?

MY FATHER WORKS FOR...

AVA WILLIAMS.... WELCOME! THIS IS THE CHAIRMAN.

RELAX. WE'RE THE GOOD GUYS! I'VE HEARD YOUR FATHER IS RECOVERING WELL AT ST. MARTHA'S?

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?

THE LOCAL 5G COMPANY, AND HE WAS JUMPED BY SOME ASSAILANTS WHO ATTACKED A 5G TOWER! LET'S SKIP TO WHAT YOU NEED, AVA. WE DON'T HAVE MUCH TIME!

SEEMS LIKE YOU REALLY ARE IN THE KNOW. CAN YOU PLEASE TELL ME THEN...WHY ON EARTH WAS THE 5G TOWER ATTACKED?! I HAVE FOUND EVIDENCE OF A LINKED DISINFORMATION CAMPAIGN ONLINE. YOU MUST KNOW ABOUT IT ALREADY?

SOMEONE HIJACKED THE PETITION AND LINKED IT TO THE CORONAVIRUS VACCINE. IT HAS ACCUMULATED 52,000 SIGNATURES 85% OF WHICH ARE BOTS. I GUESS THE LATTER GAVE IT THE TRACTION IT NEEDED.

GO ON...

SEND ME 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...

GIVE US ANOTHER 10 MINS TO ANALYZE THE DATA...

YOU GUYS SEEM TO HAVE A LOT OF DATA! HOW ON EARTH DID YOU MANAGE TO DO ALL THAT?

AN INTERNET PROTOCOL ADDRESS (IP ADDRESS) IS A NUMERICAL LABEL ASSIGNED TO EACH DEVICE CONNECTED TO A COMPUTER NETWORK THAT USES THE INTERNET PROTOCOL FOR COMMUNICATION. AN IP ADDRESS SERVES TWO MAIN FUNCTIONS: HOST OR NETWORK INTERFACE IDENTIFICATION AND LOCATION ADDRESSING.

From IP	To IP	OWNER
[redacted]	[redacted]	"AX UKRAINE"
[redacted]	[redacted]	
[redacted]	[redacted]	"DIR RUSSIA"
[redacted]	[redacted]	

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

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

MOSCOW IS SUPPLYING A LOAD OF NONSENSE TO A MULTITUDE OF ANTI-VACCINATION PETITIONS AND GROUPS. IT IS A TICKING TIME BOMB WHICH IS GOING TO BLOW UP IN OUR FACES UNLESS WE DO SOMETHING ABOUT IT!

A MAJOR CHALLENGE FACING US ALL TODAY IS THE INTEGRITY OF THE DATA WE ARE DROWNING IN. WHO IS BEHIND THE POST? IS THE SOCIAL MEDIA POST REAL? THIS IS THE DISINFORMATION PANDEMIC, AVA.

I HEAR YOU. I JUST DON'T KNOW WHAT I CAN DO TO HELP.

WHAT SOCIAL NETWORK EVEN HAS TIME FOR EXTENSIVE FACT CHECKING THESE DAYS? THE VELOCITY OF NEWS OUTSTRIPS HUMAN INTERVENTION AND THE AI WE HAVE CAN BE TRAINED, BUT IS NOT QUITE THERE YET.

HAS THERE BEEN ANY RESEARCH OR DATA THAT MAY HELP US DIFFERENTIATE BETWEEN THE ALGORITHMIC RESPONSES VERSUS THOSE BY THE TROLLS?

YOU NOTICED A PRETTY SIMPLE TIME TREND ON THAT PETITION. IT'S OFTEN WAY MORE COMPLEX. IT'S A PATTERN THE HUMAN EYE OFTEN MISSES AND SOMETIMES REQUIRES, SHALL WE SAY, "GOING THE EXTRA MILE."

ALSO, ONE OF OUR GUYS AT NICT PROVED THAT A BOT NEVER REPLIES TO ANOTHER BOT'S COMMENT.

IT'S TAKEN US YEARS TO DEVELOP THE RESOURCES AND CAPABILITY WE HAVE TODAY. THERE ARE MANY OF US LOOKING TO PROTECT WHAT WE LOVE. I WANT YOU TO JOIN THE FAMILY, AVA! WE ALL WANT THE SAME THING.

TOGETHER, WE CAN BUILD OUR GROUP OF DIGITAL PATRIOTS TO FACE THESE BAD ACTORS. AND MORE PEOPLE LIKE YOUR DAD CAN BE PROTECTED FROM THE FALLOUT OF WHAT IS LARGELY GOING UNNOTICED BY THE COUNTRY.

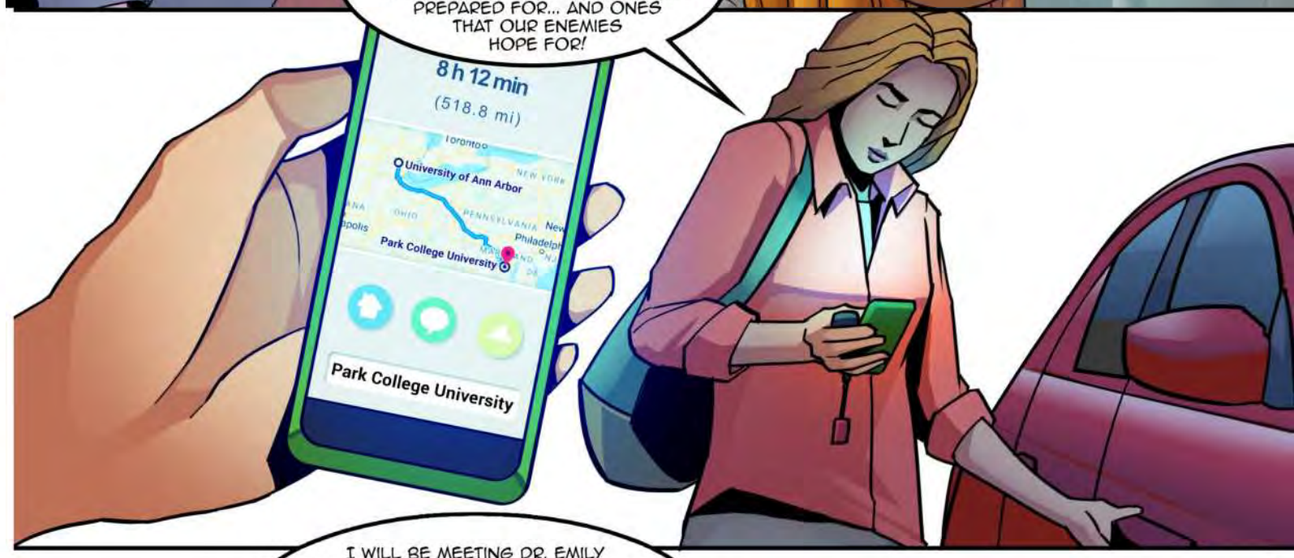
THIS IS BIGGER THAN ANYTHING I COULD HAVE ANTICIPATED. BUT, FORGIVE ME, ALL OF THIS FEELS LIKE A BAD DREAM! I DON'T EVEN KNOW WHO YOU ARE!

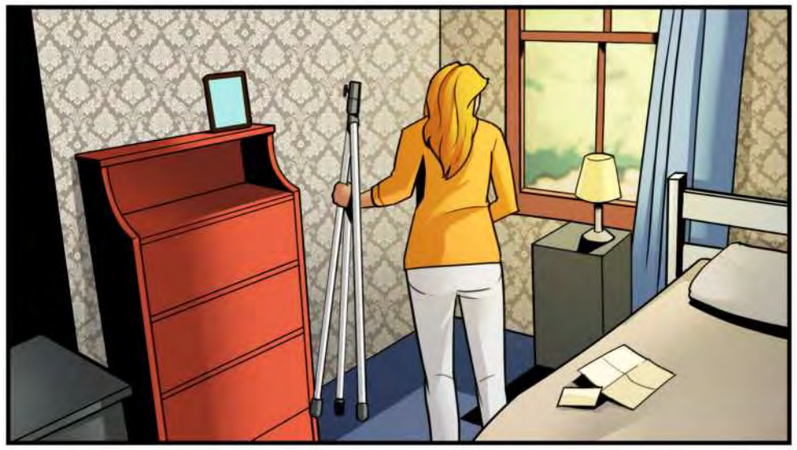
CHAIRMAN: Our secrecy is part of what keeps us all safe.

CHAIRMAN: We 'exist' in cyberspace. But should you choose to be our voice to the outside world, we can provide you with unparallelled resources to conduct your investigation. I'll leave you to it. You know what to do.

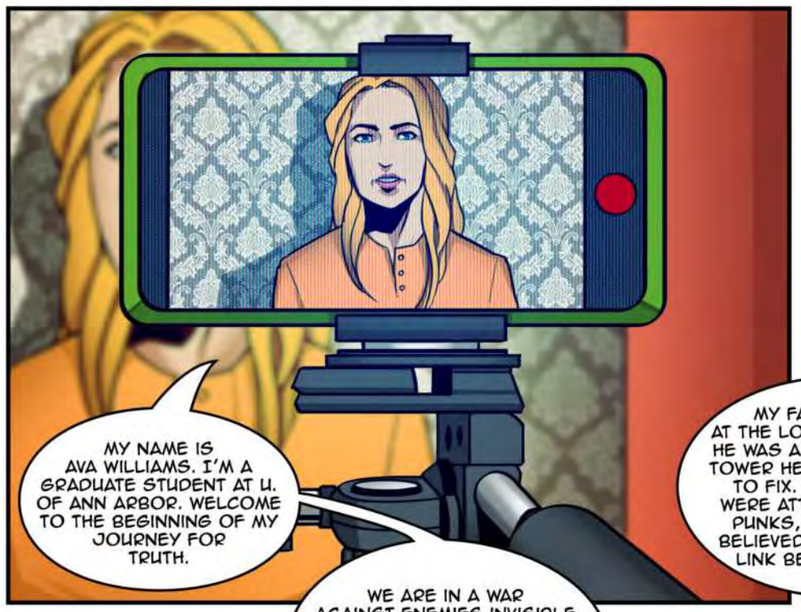
DEVELOPING AND ADMINISTERING VACCINES TO PEOPLE IS ONE WAY TO PROTECT CITIZENS AGAINST COVID-19 AND LOTS OF WORK IS BEING DONE TO PUSH THIS AHEAD. WE HAVE NOW DEVELOPED MULTIPLE GREAT VACCINES. HOWEVER, THIS IS CONTROVERSIAL AND FOREIGN FORCES HAVE FUELED THE ANTI-VACCINATION GROUPS BY CREATING A FALSE NARRATIVE AROUND HOW THESE NEW VACCINES ARE DANGEROUS AND SEEDING FALSE EVIDENCE. THE OUTCOME HAS HURT INNOCENT PEOPLE LIKE MY FATHER. EVEN AS AN ASPIRING JOURNALIST I DIDN'T REALIZE THE POTENCY OF DISINFORMATION UNTIL ALL THIS OCCURRED.

AND, IF WE DON'T PROTECT OUR SOCIETY FROM THE MENACE OF SYNTHETIC AND INACCURATE NEWS, WE MAY BE FACING OUTCOMES THAT NONE OF US ARE PREPARED FOR... AND ONES THAT OUR ENEMIES HOPE FOR!





MY NAME IS AVA WILLIAMS. I'M A GRADUATE STUDENT AT U. OF ANN ARBOR. WELCOME TO THE BEGINNING OF MY JOURNEY FOR TRUTH.



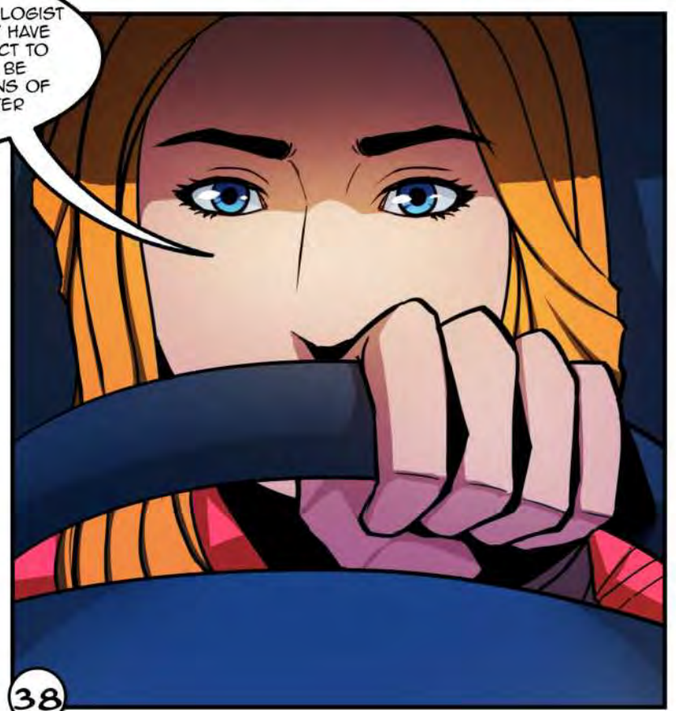
MY FATHER WORKS AT THE LOCAL 5G COMPANY, HE WAS AMBUSHED AT A 5G TOWER HE WAS CALLED OUT TO FIX. THESE TOWERS WERE ATTACKED BY SOME PUNKS, WHO WRONGLY BELIEVED THAT THERE IS A LINK BETWEEN 5G AND COVID.

WE ARE IN A WAR AGAINST ENEMIES INVISIBLE TO THE HUMAN EYE. ONE THAT HAS TAKEN MORE LIVES THAN WE COULD HAVE EVER IMAGINED: THE COVID-19 VIRUS.

HE WAS ATTACKED, BUT THESE WEREN'T ORDINARY MUGGERS. THEY WERE INFLUENCED BY A CONSPIRACY MUCH LARGER THAN THE SUM OF ITS PARTS.

WE CAN'T AFFORD TO BE SILENT. THESE AREN'T JUST AMERICAN LIVES, BUT ALL OF HUMANITY IS AT STAKE HERE.

I WILL BE MEETING DR. EMILY HARTMAN WHO IS THE CHIEF VACCINOLOGIST AT PARK COLLEGE UNIVERSITY. THEY HAVE ALSO BEEN WORKING ON A PROJECT TO INTRODUCE A VACCINE THAT WILL BE EFFECTIVE AGAINST FURTHER STRAINS OF THE VIRUS AND GENERATE GREATER SUPPLIES OF THE VACCINE.



AVA BEGINS THE LONG JOURNEY FROM ANN ARBOR TO PARK COLLEGE UNIVERSITY.

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

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

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

THAT'LL BE $7.50.

PING

THANKS.

AVA SPOTS TWO FIGURES ENTERING THE SHOP AND A WORRIED EXPRESSION APPEARS ACROSS HER FACE.

DAWN BREAKS OVER PARK COLLEGE.

PARK COLLEGE UNIVERSITY - PARKING LOT.

PC

WE LOST HER!

SCREEEECH!

41

42

DR. HARTMAN? I'M HERE AT THE RECEPTION.

OF COURSE, AVA. I'LL BE DOWNSTAIRS SOON. HOPE YOU'RE WEARING YOUR MASK?

HAHA, DON'T WORRY! I CAME PREPARED.

AVA?

HEY, DR. HARTMAN! SO GREAT TO FINALLY MEET YOU!

WELCOME TO PARK COLLEGE! HOW WAS THE DRIVE? ALL THE WAY FROM ANN ARBOR... SHEESH.

IT 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.

THEY ENTER A LAB AND SEE THE VARIOUS DOCTORS WORKING ON THEIR APPARATUS.

MAY I RECORD THIS?

WE DON'T USUALLY ALLOW IT. BUT CONSIDERING YOU'VE COME ALL THIS WAY AND YOU HAVE BEEN RECOMMENDED BY SYMOUS...

WE HAVE TO GO THROUGH A VERY COMPREHENSIVE SANITIZATION PROCEDURE! PLEASE LEAVE YOUR BACKPACK AND OTHER BELONGINGS HERE.

AND HERE'S A LAB COAT... GEAR UP.

MAY I ASK WHY?

YOU KNOW ABOUT SYMOUS... OH, NEVER MIND! WHY AM I SO SURPRISED! PEOPLE NEED TO KNOW THE TRUTH. WE'RE AT WAR WITH SOMETHING THAT COULD GIVE THIS VIRUS EVEN MORE POWER.

DISINFORMATION.

I UNDERSTAND. WE HAVE NOTHING TO HIDE HERE, AND THE STAKES ARE VERY HIGH. I'LL MAKE AN EXCEPTION.

WHAT WE HAVE DEVELOPED IS A MESSENGER RNA VACCINE. THIS WORKS BY CONVEYING GENETIC INSTRUCTIONS TO CELLS SO THAT THEY ARE ABLE TO SYNTHESIZE SPECIFIC PROTEINS WHICH, IN TURN, KICK OFF ANTIBODIES THAT PROTECT CELLS BY FIGHTING THE CORONAVIRUS.

INTERESTING. SO HOW HAVE THE TRIALS BEEN?

VIDCONNECT
VIDEO ARCHIVE
Dr. Ahmed from Atlanta

LET ME SHOW YOU SOMETHING I RECORDED AT THE COALITION FOR COVID VACCINE DEVELOPMENT, A VIRTUAL CONFERENCE WHERE A NUMBER OF THE MOST RESPECTED SCIENTISTS BROKE IT DOWN FOR ANOTHER JOURNALIST THAT ASKED ABOUT THE DIFFERENT APPROACHES...

A NUMBER OF TRIALS HAVE BEEN CONDUCTED OVER THE LAST 8 MONTHS WITH VARIOUS APPROACHES. FROM MRNA VACCINES TO PROTEIN-BASED VACCINES, AS WELL AS DNA-BASED AND INACTIVE VIRUS-BASED VACCINES IN DEVELOPMENT, THERE ARE A WIDE RANGE OF STUDIES UNDERWAY TO SEE WHERE THE BEST EFFICACY MAY BE. ALTHOUGH THERE ARE SEVERAL VACCINES STILL BEING DEVELOPED, OUR CURRENT VACCINE HAS AN EFFICACY RATE OF 90%.

Atlanta

CAN YOU SIMPLIFY THAT FOR US DOCTOR?

DR. MEHMOOD GOTAYWALA
ATLANTA

AS YOU PROBABLY KNOW, THE PROCESS FOR CREATING A VACCINE IS MORE OF A MARATHON THAN A SPRINT. COMING OUT WITH A LEGITIMATE VACCINE SO FAST HAS BEEN A VICTORY FOR SCIENCE. HERE IN THE U.S. 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.

OUR PHASE 1 AND 2 TRIALS HAVE BEEN A SUCCESS. EVEN AS THE SCIENTIFIC COMMUNITY IS NOW WORKING TO UNDERSTAND WHETHER THE VACCINES THEY HAVE DEVELOPED ARE EFFECTIVE AGAINST NEW STRAINS OF THE VIRUS AND THE IMPACT OF THESE NEW STRAINS ON THE HUMAN BODY, OTHERS ARE WORKING TO FIGURE OUT THE BEST WAY TO GET THE VACCINES DELIVERED AND ADMINISTERED.

IF I MAY... WHAT DR. MEHMOOD GOTAYWALA IS SAYING IS THAT WE HAVE EXPLORED ALL POSSIBLE APPROACHES WHEN DEVELOPING OUR VACCINE INITIALLY. LET ME SIMPLIFY HOW THESE APPROACHES WORK. THIS WILL TAKE A FEW MINUTES, BUT I PROMISE TO KEEP THIS ALL FAIRLY HIGH LEVEL.

DR. DAICHI NAKAZAWA
ATLANTA

THE FIRST APPROACH, WHICH IS THE BEST KNOWN, IS SIMPLY TAKING A VERSION 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, THEN STIMULATES AN IMMUNE RESPONSE AND PRODUCES ANTIBODIES.

AS THE WORD IMPLIES, THE ANTIBODIES ARE THEN ABLE TO FIGHT THE VIRUS IF IT ENTERS THE BODY. WE CALL THESE DNA VACCINES. DNA IS WHAT CARRIES THE GENETIC INSTRUCTIONS, AS YOU MAY BE AWARE.

THERE IS ALSO YET ANOTHER APPROACH THAT SKIPS THE DNA ALTOGETHER AND INSTEAD USES MESSENGER RNA OR MRNA. MOST VACCINES CREATE AN IMMUNE RESPONSE, BY INSERTING A WEAKENED STRAIN OF A VIRUS INTO OUR BODIES. MRNA VACCINES, HOWEVER, CREATE A PROTEIN IN OUR CELLS INSTEAD, WHICH IN TURN RESULTS IN AN IMMUNE RESPONSE, AS OUR BODY IDENTIFIES THAT THIS PROTEIN DOES NOT BELONG 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 ARE ALL DOING...

THANK YOU, AVA. WE HAVE BEEN SUCCESSFUL IN CREATING A VACCINE IN RECORD TIME, WHICH 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 SECTOR HAVE ALL THROWN EVERYTHING AND THE KITCHEN SINK AT THE PROBLEM. I AM SURE THAT YOU WOULD HAVE SEEN THAT SOME HOUSEHOLD NAMES, INCLUDING SOME TECH MOGULS, 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 BE ROLLED OUT TO THE PUBLIC SOON.

IF THERE'S ONE MESSAGE YOU'D GIVE FOR THE GENERAL PUBLIC TO TAKE AWAY, WHAT WOULD IT BE?

PLEASE TRUST US. BELIEVE IN SCIENCE AND MODERN MEDICINE. THESE VACCINES WERE DEVELOPED RAPIDLY BECAUSE WE HAVE EXPERIENCE WITH THE TECHNOLOGIES. WE DON'T SIMPLY DO WHAT WE DO WITHOUT THE RIGOR OF SCIENTIFIC EVIDENCE.

A VACCINE HAS NEVER BEEN DEVELOPED AT A PACE AS ACCELERATED AS THIS. IT'S NOT JUST BEEN US: UNDERSTANDING THE VIRUS AND WHAT IS NEEDED FOR AN EFFECTIVE VACCINE TAKES A MULTIDISCIPLINARY EFFORT FROM MANY GROUPS.

EVEN AS THE SCIENTIFIC COMMUNITY HAS WORKED TO FINALIZE THE VACCINE, OTHERS ARE WORKING TO FIGURE OUT THE BEST WAY TO GET THE VACCINES DELIVERED AND ADMINISTERED.

THANK YOU.

AVA, THERE'S SOMEONE I WANT YOU TO MEET. HE'D PROBABLY HAVE A BETTER UNDERSTANDING OF THE MOTIVES AND ORIGINS OF SOME OF THE ANTI-VAX GROUPS THAT ARE STRONGLY AGAINST THE IDEA OF A VACCINE.

HE'S A MEDIA STUDIES PROFESSOR HERE. DR. HARIS ADAMOS.

I HAD MENTIONED YOUR VISIT TO HIM IN PASSING AND HE SAID HE WOULD BE UP FOR SHOWING YOU HIS RESEARCH!

THAT'D BE GREAT, THANK YOU.

1328

KNOCK!

KNOCK!

GOOD EVENING, DOCTOR?

PLEASE, HAVE A SEAT.

YOU MUST BE AVA!

YES, SIR.

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.

WELL... I HAVE BEEN LOOKING AT THE VACCINE, BUT IT HAS NOTHING TO DO WITH 5G OR ANY SUCH NONSENSE!

MY DATA SCIENCE TEAM UNCOVERED HOW A HANDFUL OF PEOPLE ARE FUNDING AD CAMPAIGNS TO GROW THE ANTI-VAX MOVEMENT IN THE US.

CERTAIN COMMUNITIES HAVE PARTICULARLY STRONG RESPONSE CURVES TO THIS SOCIAL MEDIA MARKETING! SOCIAL MEDIA GIANTS NEED TO HELP PUT AN END TO WHAT IS SO CLEARLY A NATIONAL RISK!

THAT'S INTERESTING. HAVE YOU BEEN ABLE TO FOLLOW THE MONEY?

THESE INVESTMENTS ARE LEGAL AS FAR AS I CAN TELL, BUT IT IS LIKELY TO HURT PEOPLE BECAUSE IT USUALLY INVOLVES SPREADING FALSEHOODS. LIKE ANY MEDICATION, 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.

WHAT YOU ARE DOING... IT'S COMMENDABLE! I DO SEE THE NEED TO FIGHT AGAINST DISINFORMATION THAT COULD LEAD TO LOWER TAKE UP OF ANY VACCINE! I AM PARTICULARLY WORRIED ABOUT THE ANTI-VAX MOVEMENT.

I HAVE THE PROOF, DOCTOR! AND, TOGETHER WITH YOUR DATA, I THINK WE COULD MAKE SENSE OF IT ALL FOR THEM... I JUST NEED TO GET IN FRONT OF THEM.

YOU CANNOT USE SCIENTIFIC RATIONALITY AND NUMBERS TO WIN THIS WAR, AVA. YOU NEED TO WIN THEIR HEARTS AND MINDS FIRST AND THEN SHOW THEM THE TRUTH!... YOU DO HAVE CONCRETE PROOF, RIGHT? THAT THERE ARE GROUPS DELIBERATELY SETTING OUT TO INFLUENCE THEM?

THE OTHER CHALLENGE IS THAT YOU HAVE TO PERSUADE THEM THROUGH THEIR OWN MEDIA. THEY DON'T TRUST MAINSTREAM NEWS, AS I AM SURE YOU WELL UNDERSTAND. YOU WILL NEED TO MEET WITH DARREN LANCASTER, WHO LEADS TRUSTINNATURE, THE MOST POPULAR ANTI-VAX SITE, AND BE "INVITED" TO SHARE A STORY... AND THE IRREFUTABLE PROOF.

MY RESEARCH IS ALL OUT THERE ALREADY, BUT I AM SEEN AS TOO PRO-VAX TO HAVE A VOICE THERE!

WELL, I DID HAVE THIS INCREDIBLY... SHALL WE SAY "ANIMATED" DEBATE WITH DARREN OVER A TEXT WAR. LET ME SEE IF I CAN FIND HIS NUMBER... COULD GIVE YOU HIS -- AH! THERE IT IS... DARREN'S NUMBER...

OK, LET ME GET THAT FROM YOU!

I WILL SEND OVER THE DATA I HAVE TOO, SO THAT YOU CAN SHARE IT WITH DARREN. SHOW HIM THAT NONE OF THIS IS DOCTORED. THE ONLY THINGS MADE UP HERE ARE THOSE ADS!

THANK YOU DOCTOR. I REALLY APPRECIATE THIS!

CALL ME HARIS!

I'LL DO MY BEST. SUCH A PLEASURE, HARIS.

TAKE CARE AVA, AND GOOD LUCK.

AVA GETS A CALL FROM DR HARTMAN AS SHE LEAVES THE UNIVERSITY.

HELLO AVA. THERE WAS A RANSOMWARE ATTACK ON OUR RESEARCH SHORTLY AFTER YOU LEFT. I JUST WANTED TO MAKE YOU AWARE OF THIS AS THIS MAY BE RELEVANT FOR YOUR STORY. SYMOUS JUST HELPED OUR INFORMATION TEAM FOIL A RANSOMWARE ATTACK ON THE VACCINE RESEARCH.

I WONDER WHY THEY WOULD ATTACK YOUR VACCINE RESEARCH AND NOT OTHERS? DO YOU THINK IT HAS SOMETHING TO DO WITH MY VISIT?

You became a victim of the project_x RANSOMWARE

The harddisks of [illegible] have been encryp
encryption [illegible] way to res
key. Yo [illegible] he darkne

To p [illegible] data
ste

1.

2.

ready purchased your key, [illegible]

key: _

YES! PART OF THEIR DEMANDS INCLUDE THAT YOU KILL THE STORY AND THEY'VE ASKED FOR $3 MILLION TO BE DEPOSITED INTO A CRYPTO WALLET WITHIN TWO DAYS OR THEY DELETE THE DATA. LITTLE DO THEY KNOW THAT OUR TEAM HAD ALREADY ANTICIPATED THIS AND WORKED WITH SYMOUS TO SET UP A DECOY SERVER, WHICH IS WHAT WAS ATTACKED.

LET ME PATCH ANDREW INTO THE CALL TOO.

HEY AVA, EMILY.

IN CASE YOU'RE WONDERING, ALL OF THE ACTUAL DATA IS POST-QUANTUM ENCRYPTED AND NOW LIVES ON A SECRET SERVER IN AN UNDISCLOSED LOCATION. THE UNIVERSITY'S INFORMATION TEAM HAD SHARED THEIR FEARS OF AN ATTACK, AND LUCKILY THEY ALREADY HAD BACKUPS OF THEIR DATA IN PLACE, IN CASE SUCH AN EVENT TOOK PLACE. THANKS TO THEIR QUICK THINKING, WE DIDN'T HAVE TO DO MUCH AND WE WORKED QUICKLY TO MAKE THE DATA EVEN MORE SECURE USING POST-QUANTUM CRYPTOGRAPHY.

THIS IS THE BEST WAY TO SECURE DATA AND WORKS BY USING PHOTONS OF LIGHT TO ENCRYPT DATA IN SUCH A MANNER THAT IT IS EVEN SAFE FROM A QUANTUM COMPUTER, WHICH IS THE MOST POWERFUL COMPUTER CURRENTLY IN EXISTENCE. THE TEAM AGREED THAT THIS WAS THE MOST EFFECTIVE AND FASTEST SOLUTION TO PROTECT THE VALUABLE RESEARCH THEY HAVE BEEN DOING. THIS ATTEMPT AT AN ATTACK HIGHLIGHTS THE NEED TO PROTECT COMPUTERS AND SENSITIVE DATA FROM BEING HIJACKED AND THE IMPORTANCE OF USING THE MOST UP-TO-DATE METHODS TO DO SO.

THERE IS A VAST DIFFERENCE BETWEEN SPREADING DISINFORMATION ON SOCIAL MEDIA AND USING RANSOMWARE WHICH IS ILLEGAL BEHAVIOR.

AT LEAST WE NOW KNOW THAT I'M BEING WATCHED AND WHOEVER IS BEHIND THIS DOES NOT WANT MY STORY ABOUT THE MANIPULATED PETITION AND ITS FALSE LINK TO THE VACCINE TO BE EXPOSED.

AVA CONTINUES THE DRIVE BACK TO ANN ARBOR, AND GETS IN TOUCH WITH DARREN LANCASTER WHEN SHE RETURNS HOME.

Take the exit on to I-70 West
1 1/2 MILES

EXIT ONLY
Towards Pittsburgh

DARREN - 202 -0013

YES, THAT'S ME.

I'M AVA WILLIAMS, DR. HARIS ADAMOS REFERRED ME TO YOU.

Calling 202-

GOOD MORNING. IS THIS MR. DARREN LANCASTER?

OH... HM. 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 PERSPECTIVES. I WAS SIMPLY HOPING I COULD ASK YOU A FEW QUESTIONS?

FAIR ENOUGH, WHAT KIND OF 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!

ABSOLUTELY NOTHING!

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.

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 VIRUS IS VERY REAL. IT'S THE EFFECTIVENESS OF THESE VACCINES WHICH HAVE BEEN DEVELOPED THAT I HAVE DOUBTS ABOUT.

ONE WEEK LATER, IN THE MEDIA RECORDING LAB IN THE UNIVERSITY.

PLEASURE TO HAVE YOU WITH US, DARREN. LET'S DIVE RIGHT IN... CAN YOU TELL ME A LITTLE MORE ABOUT YOUR ROLE AT TRUSTINNATURE?

SURE. I HEAD UP THE NATION'S LARGEST DIGITAL ANTI-VAX COMMUNITY. WE HAVE OVER 15 MILLION MEMBERS AROUND THE NATION!

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

MUCH OF WHAT WE SEE BEING PEDDLED BY THE GOVERNMENT IS PSEUDOSCIENCE WITH INCONCLUSIVE DATA SUPPORTING THEIR HYPOTHESIS. WE HAVE OUR OWN SCIENCE TEAMS 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.

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

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

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

DO YOU EVER THINK WHATEVER YOU BELIEVE COULD AT LEAST BE REMOTELY CONNECTED TO DISINFORMATION OR SOME SOCIAL MEDIA WILDFIRE?

LIVE

Ava Williams

2003

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 GENUINE?

MANY DISEASES HAVE BEEN ELIMINATED FROM THIS COUNTRY, SO WHY PERPETUATE THE VICIOUS CYCLE? FLU SHOTS HAVE EVEN BEEN CORRELATED TO INFLUENZA IN THE PAST.

SO ARE WE GOING TO KEEP GIVING MAINSTREAM MEDIA TOTAL POWER?

THERE ARE MANY INTERVENTIONS THAT DON'T INVOLVE A VACCINE... HERD IMMUNITY IS A THING, RIGHT?

DON'T PEOPLE DIE EVERY DAY? NO ONE BATS AN EYE: WAR, POVERTY, CORRUPTION. WE HAVEN'T EVEN BEEN ABLE TO ERADICATE INFLUENZA FOR CRYING OUT LOUD.

BUT WHAT ABOUT COVID-19? IT'S A DISEASE 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 HARD SACRIFICES TO MAKE. ALL THE VACCINES AMERICAN KIDS HAVE BEEN HIT WITH, DON'T YOU BELIEVE WE'VE BEEN CLOGGING 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 TRUSTINNATURE HAS THE POTENTIAL TO BE AN IMPORTANT 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 PLAGUED BY AUTISM OR ARTHRITIS? 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 ADVERTISING 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 DEFERENCE 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 5G WOULD RENDER THE VACCINE USELESS?

BUT ARE YOU AWARE THAT THE PETITION HAS BEEN HIJACKED BY TROLLS?

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 STUDIED 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 HERE WERE NOT EVEN MADE BY REAL PEOPLE, INSTEAD THEY WERE MADE BY BOTS!

MY APOLOGIES, MY INTENTION WASN'T TRYING TO SPRING ANYTHING ON YOU, BUT I WANTED TO MAKE YOU AWARE OF THESE DATA POINTS. I KNOW THAT DR. HARIS ADAMOS HAS ALSO SHOWCASED ANALYSIS THAT HAS HIGHLIGHTED HOW MUCH OF THE ADVERTISING ONLINE AROUND 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 GET ANY COMMENTS FROM AHEAD OF THIS!

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.

NO-- I-- WHAT DO YOU MEAN?

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.

5G CELL TOWER

CAMPAIGN UNDER INVESTIGATION

WE CAN'T CONTROL WHAT OTHERS DO ON THE INTERNET! IT IS THEIR PREROGATIVE TO ADVERTISE!

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, MS. 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.

AVA HAS REMOVED HER MASK, AS SHE EXITS THE BUILDING.

THAT IS THE POWER OF THE NEW NORMAL WHEN IT COMES TO NEWS. IT CUTS BOTH WAYS. THE TROLLS HAVE ALSO STARTED TO FIGHT BACK. BUT TOO MANY INDEPENDENT GROUPS ARE RUNNING THE DATA. YOUR CONCLUSIONS HAVE ALREADY BEEN CONFIRMED BY MEDIA, INDEPENDENT BLOGGERS AND FOREIGN CORRESPONDENTS. NOW WE WAIT AND SEE WHAT HAPPENS. I EXPECT SOME PUSHBACK!

SHOULD I BE WORRIED?

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

THANKS, AND WILL DO. I DON'T KNOW HOW TO THANK YOU!

I THINK SOMEONE IS WAITING FOR YOU AT HOME. WHY DON'T WE TOUCH BASE AFTER? AND DON'T WORRY, HE IS IN VERY GOOD HANDS!

AVA PULLS UP OUTSIDE A RESIDENTIAL AREA.

I CAN'T BELIEVE ALL THIS HAS HAPPENED IN JUST ONE WEEK.

AVA? HONEY, IS THAT YOU?

AVA? I'VE BEEN SO WORRIED ABOUT YOU. SOMEONE CALLED AND TOLD ME NOT TO WORRY. WHO WAS THAT? NEVER HEARD YOU MENTION THEM BEFORE? THEN I SAW YOU ON THE NEWS! I AM SO PROUD, KIDDO!

SORRY, SHOULD HAVE SAID SOMETHING. JUST SOME PEOPLE WORKING WITH ME ON THE STORY. I'VE BEEN ALRIGHT. YOU'RE THE ONE WHO NEEDS THE LOOKING AFTER, MR. SUPERHERO. TRY NOT TO GO AFTER THE BAD GUYS YOURSELF NEXT TIME!

SAYS MS. LANE WITH ALL HER REPORTING! HAH!

HONEY, YOU LOOK TIRED. HAVE YOU BEEN GETTING ENOUGH SLEEP?

NOT GOING TO PRETEND OTHERWISE. IT'S BEEN A BIT MUCH EVER SINCE... THE INCIDENT. I DO FEEL I MAY BE COMING DOWN WITH SOMETHING!

RING! RING!

Unknown Number

WHO IS IT, HONEY?

JUST WORK, DAD. IT'S PERPETUAL.

I DON'T KNOW WHAT YOU'RE WORKING ON, HONEY. CAN'T YOU TAKE SOME TIME AND REST??

I WILL. JUST NEED TO SEE THIS THING THROUGH. I THINK I'M ONTO SOMETHING. I PROMISE I'LL GET MY 8 HOURS OF SLEEP AFTER THIS IS OVER.

THAT'S MY GIRL. I'M SO THANKFUL THE INJURIES AREN'T SEVERE. YOU AND ME, ALL WE HAVE IS EACH OTHER.

ME TOO, DAD. IT'S SO GOOD TO HAVE YOU BACK.

WE INTERRUPT OUR CURRENT BROADCAST TO BRING YOU NEWS FROM THE CAPITAL CITY.

WE HAVE ARRESTED A SUSPECT WHO HAS BEEN IDENTIFIED AS THE MASTERMIND BEHIND THE ARSON OF THE 5G TOWERS IN MICHIGAN. THIS ARREST WAS MADE AFTER AN ANONYMOUS TIP WAS GIVEN TO THE LOCAL POLICE.

THE SUSPECT HAS BEEN IDENTIFIED AS GARETH MCGIBSON. HE IS CURRENTLY BEING INVESTIGATED FOR TIES TO THE ANTI-VACCINATION PETITION AND LINKS TO FOREIGN BACKERS. ACCORDING TO OUR INVESTIGATIONS, MCGIBSON HAD BEEN ORCHESTRATING THIS ATTACK, AND ATTACKS ON OTHER 5G TOWERS WITH THE HELP OF THESE BACKERS.

NEWS

POLICE CAM 01

AS YOU MAY HAVE HEARD, OUR PLUMBER FIXED THE LEAK. THE JOB'S ALL WRAPPED UP NOW.

I THOUGHT YOU HAD SOMETHING TO DO WITH IT.

SOMETHING ELSE IS BREWING. POSSIBLY YOUR NEXT BIG STORY! IF YOU CAN HANDLE IT!

A FEW MONTHS LATER -AVA ARRIVES AT THE NATIONAL JOURNALISM AWARD CEREMONY.

NATIONAL JOURNALISM AWARDS

THE PAPARAZZI IS PRESENT AND AVA SEES SOME FAMILIAR FACES.

THE CEREMONY IS THIS WAY, MISS WILLIAMS.

OUR FINAL AWARD FOR "BEST NEWCOMER AND USE OF DIGITAL MEDIA" GOES TO SOMEONE WHOSE WORK HAS BEEN INSTRUMENTAL IN EDUCATING PEOPLE DURING A TIME WHERE DISINFORMATION IS RAMPANT AND PEOPLE ARE QUICK TO BELIEVE NEWS WITHOUT VERIFYING ITS ACCURACY.

THE AWARD GOES TO MISS AVA WILLIAMS!

AVA GOES ON STAGE TO COLLECT HER AWARD.

NATIONAL JOURNALISM AWARDS

BEST NEWCOMER and USE OF DIGITAL MEDIA

SHE HAS DONE GREAT WORK AROUND HIGHLIGHTING THE BENEFITS OF A VACCINE WHICH WILL COUNTER THE VIRUS AND ENCOURAGING PEOPLE TO EXPLORE DIFFERING VIEWPOINTS. MOST NOTABLY, HER WORK RESULTED IN A TIP-OFF THAT THWARTED AN ATTACK ON AN IMPORTANT VACCINE STOCKPILE.

WE OWE MISS WILLIAMS A LOT OF GRATITUDE FOR HER EFFORTS AND SHE IS A VERY WORTHY RECIPIENT OF THIS AWARD.

THANK YOU. IT'S A GREAT HONOR TO RECEIVE THIS AWARD.

THE INTERNET SEES A HUGE VOLUME AND VARIETY OF INFORMATION PASS THROUGH IT EVERY DAY. POLITICALLY, SOCIALLY OR ECONOMICALLY WE WILL PROBABLY DISAGREE 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 HAVE PLAYED A SMALL PART IN A MUCH BIGGER STORY.

THANK YOU!

BIBLIOGRAPHY

PAGE 46:
J. WOLFE, "CORONAVIRUS BRIEFING: WHAT HAPPENED TODAY," 2020 HTTPS://WWW.NYTIMES.COM/2020/11/16/US/CORONAVIRUS-TODAY.HTML

PAGE 50:
S. GHOSE, "ARE YOU READY FOR THE QUANTUM COMPUTING REVOLUTION?" 2020 HTTPS://HBR.ORG/2020/09/ARE-YOU-READY-FOR-THE-QUANTUM-COMPUTING-REVOLUTION

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 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.

Resilience Series

REAKE

Commissioned by the Cybersecurity and Infrastructure Security Agency

Written by Clint Watts and Farid Haque

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.

CREDITS

STORY BY

Farid Haque, Clint Watts

ART DIRECTION

Farid Haque, Annas Dar, J. Nino Galenzoga

ILLUSTRATORS

J. Nino Galenzoga, Annas Dar, Joel Santiago

COLORISTS

Mona S, Patricia Beja, Joel Santiago

LETTERING

Haroon M, Komal N, Patricia Beja

EDITOR

Tolly M.

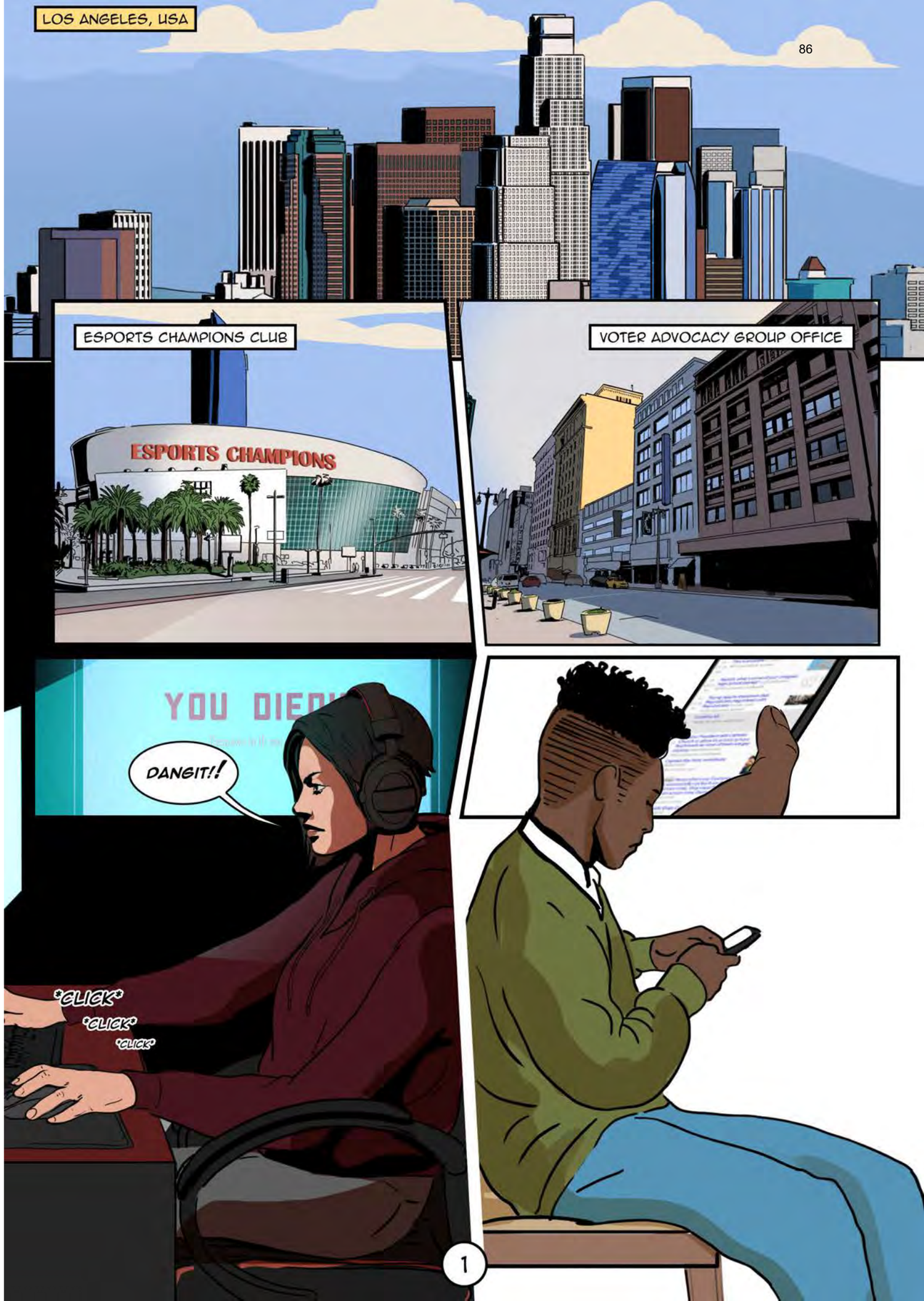
SCRIPTWRITERS

Michael Gianfrancesco, Kabir Sabharwal

Resilience Series

RAKE

CLINT WATTS
FARID HAQUE



WHOA! WATCH IT! I KNOW YOU DON'T HAVE ANOTHER $200 FOR A GAMING MOUSE.

ARE YOU OKAY?

SORRY, I DIDN'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 COMMBLOGZ HAS GOTTEN UNDER MY SKIN.

CommBlogz

Andre
Take this garbage off the web and stop trying to pass off this stuff as real. The American people are smart enough to spot a fake!

Single 0
The truth hurts, doesn't it?

Andre
This is damaging to our very democracy! People need to be able to trust facts!

Single 0
The Deep State hides the truth!

Andre

TROLL? 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: WINNING.

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...

2

JUST LISTEN, FOR ONCE! THIS GUY, SINGLEØ ON COMMBLOGZ, POSTED ALL THESE CLEARLY MANIPULATED VIDEOS. PEOPLE WATCH THEM AND BELIEVE THEY'RE REAL.

THAT GETS SHARED AND THEN PEOPLE DON'T HAVE THE FACTS! THAT'S DANGEROUS.

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

CHECK THIS OUT! I DUG INTO HIS PROFILE AND IT'S CONNECTED TO SOME KID'S ACCOUNT IN KOREA! DO YOU REALIZE WHAT THAT MEANS?

PERHAPS YOU HAVE TOO MUCH TIME ON YOUR HANDS?

SHOULDN'T YOU BE PRACTICING, INSTEAD OF MESSING AROUND ON COMMBLOGZ?

SIGH... NEVERMIND...

THE MORNING TIMES

DEEPFAKE TECHNOLOGY GETS AN UPGRADE

PRESIDENT ADDRESSES THE NATION

!

OH MAN... THIS IS REALLY GOING TO SEND THE MEDIA INTO A FRENZY. WHILE OUR NEWS DOES THE RIGHT THING BY TALKING ABOUT THESE "SYNTHETIC VIDEOS" THE REAL ISSUE IS THAT THEY ARE SO FEEDING THE "LIAR'S DIVIDEND"."

"LIAR'S DIVIDEND IS THE UNINTENDED OUTCOME OF SHINING A LIGHT ON DISINFORMATION, WHICH IN TURN CAUSES DOUBT AROUND THE VERACITY OF NEWS (TRUE OR NOT), INADVERTENTLY HELPING THOSE THAT SPREAD LIES.

3

CREEPIN' AROUND LIKE NO ONE KNOWS THINK YOU'RE SO CRIMINAL...

BAD GUY
- BILLIE EILISH

4

WHAT A DAY!

Woof!

HI CHEWIE.... THAT'S A GOOD BOY... MISS ME?

5


OK... TIME TO GET MR. CHAIRMAN ON THE LINE...


CommBlogz
Deepfakes
DEEPFAKE REQUEST MEGATHREAD
CELEBRITY DEEPFAKES THREAD(NSFW)
About Community


6

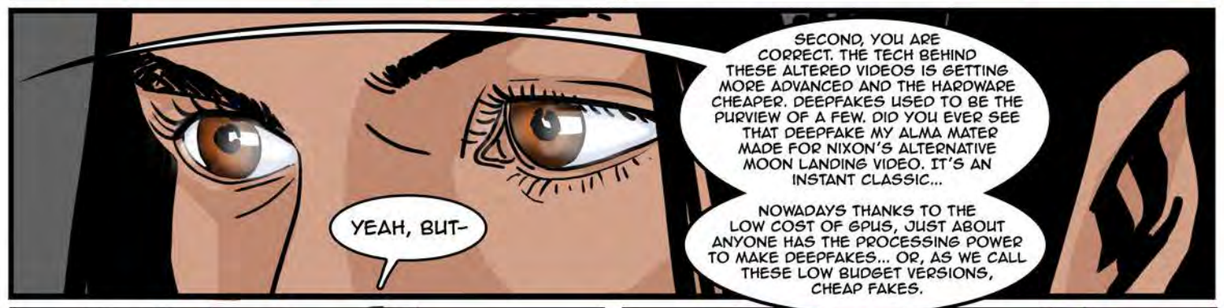

PHONEBOOK
Harry. D
Wilson. H
Steven. B
Johnny. D
Aiden. P
Andrew. W
Tyler. N
Hanzo. H
ANDREW WILSON
calling...

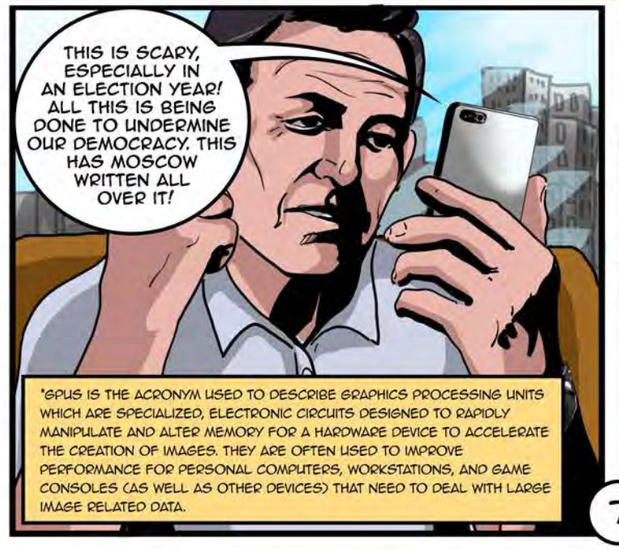

COULD I GET A 30 MIN APPOINTMENT WITH THE CHAIRMAN, RIGHT NOW?


IT'S A BIT SHORT NOTICE! BUT I AM SURE HE COULD SQUEEZE YOU IN CONSIDERING YOU'RE HIS FAVORITE NIECE!


THANK YOU, I WANTED TO GET YOUR TAKE ON THIS. MORE OF THESE DEEPFAKE VIDEOS ARE SHOWING UP ON COMMBLOGZ AND FINDING THEIR WAY TO OTHER SOCIAL MEDIA SITES. GOT INTO IT WITH A TROLL THERE YESTERDAY. IT SEEMS TO BE GETTING WORSE!


FIRST OFF, YOU SHOULDN'T ARGUE WITH TROLLS. HOW MANY TIMES HAVE I TOLD YOU THAT?


YEAH, BUT-
SECOND, YOU ARE CORRECT. THE TECH BEHIND THESE ALTERED VIDEOS IS GETTING MORE ADVANCED AND THE HARDWARE CHEAPER. DEEPFAKES USED TO BE THE PURVIEW OF A FEW. DID YOU EVER SEE THAT DEEPFAKE MY ALMA MATER MADE FOR NIXON'S ALTERNATIVE MOON LANDING VIDEO. IT'S AN INSTANT CLASSIC...
NOWADAYS THANKS TO THE LOW COST OF GPUS, JUST ABOUT ANYONE HAS THE PROCESSING POWER TO MAKE DEEPFAKES... OR, AS WE CALL THESE LOW BUDGET VERSIONS, CHEAP FAKES.


THIS IS SCARY, ESPECIALLY IN AN ELECTION YEAR! ALL THIS IS BEING DONE TO UNDERMINE OUR DEMOCRACY. THIS HAS MOSCOW WRITTEN ALL OVER IT!
*GPUS IS THE ACRONYM USED TO DESCRIBE GRAPHICS PROCESSING UNITS WHICH ARE SPECIALIZED, ELECTRONIC CIRCUITS DESIGNED TO RAPIDLY MANIPULATE AND ALTER MEMORY FOR A HARDWARE DEVICE TO ACCELERATE THE CREATION OF IMAGES. THEY ARE OFTEN USED TO IMPROVE PERFORMANCE FOR PERSONAL COMPUTERS, WORKSTATIONS, AND GAME CONSOLES (AS WELL AS OTHER DEVICES) THAT NEED TO DEAL WITH LARGE IMAGE RELATED DATA.


7
MAYBE IT'S TIME WE DUG DEEPER. I CAN TELL YOU A LITTLE MORE ABOUT DEEPFAKE TECHNOLOGY BEFORE I HAVE TO GO.

A BRIEF HISTORY OF DEEPFAKES.

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 MIS AND/OR DISINFORMATION. THE TERM WAS FIRST USED BY A REDDIT USER IN 2017.

https://ww[redacted]'r/deepfakes/

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.

THE TECHNOLOGY IS REPORTED TO HAVE EMERGED INITIALLY FROM ACADEMIC RESEARCH AT THE UNIVERSITY OF CALIFORNIA – BERKELEY AND WAS REFINED BY COMPUTER VISION EXPERTS IN SILICON VALLEY. THE MAJOR BREAKTHROUGH IS ATTRIBUTED TO A PAPER PUBLISHED BY A TEAM AT BERKELEY TITLED "VIDEO REWRITE: DRIVING VISUAL SPEECH WITH AUDIO." IN THIS PAPER, THE TEAM FOCUSED ON THE IMPORTANCE OF SYNCING LIP MOVEMENTS AND SPEECH AT A TIME WHEN MUCH OF APPLIED ARTIFICIAL INTELLIGENCE IN THE SPACE OF MACHINE LEARNING WAS LARGELY THEORETICAL.

Deepfakes
r/deepfakes

Hot New Top ···

PINNED BY MODERATORS
21
DEEPFAKE REQUEST MEGATHREAD
63 Comments Share Save ···

Posted by u/AutoModerator 1 day ago
0
[redacted]
1 Comment Share Save ···

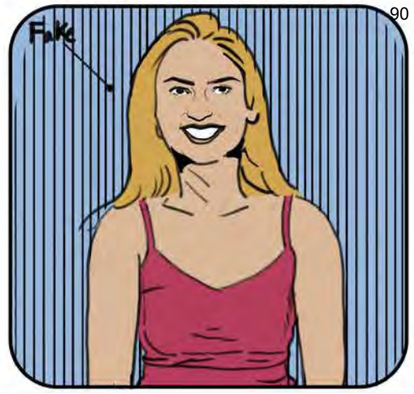
-
CELEBRITY DEEPFAKES THREAD(NSFW)
[redacted]
0 Comments Share Save ···

PROMOTED · [redacted]
39
[redacted]

About Community
[redacted]
[redacted] Members [redacted] Online
[redacted]
Restricted

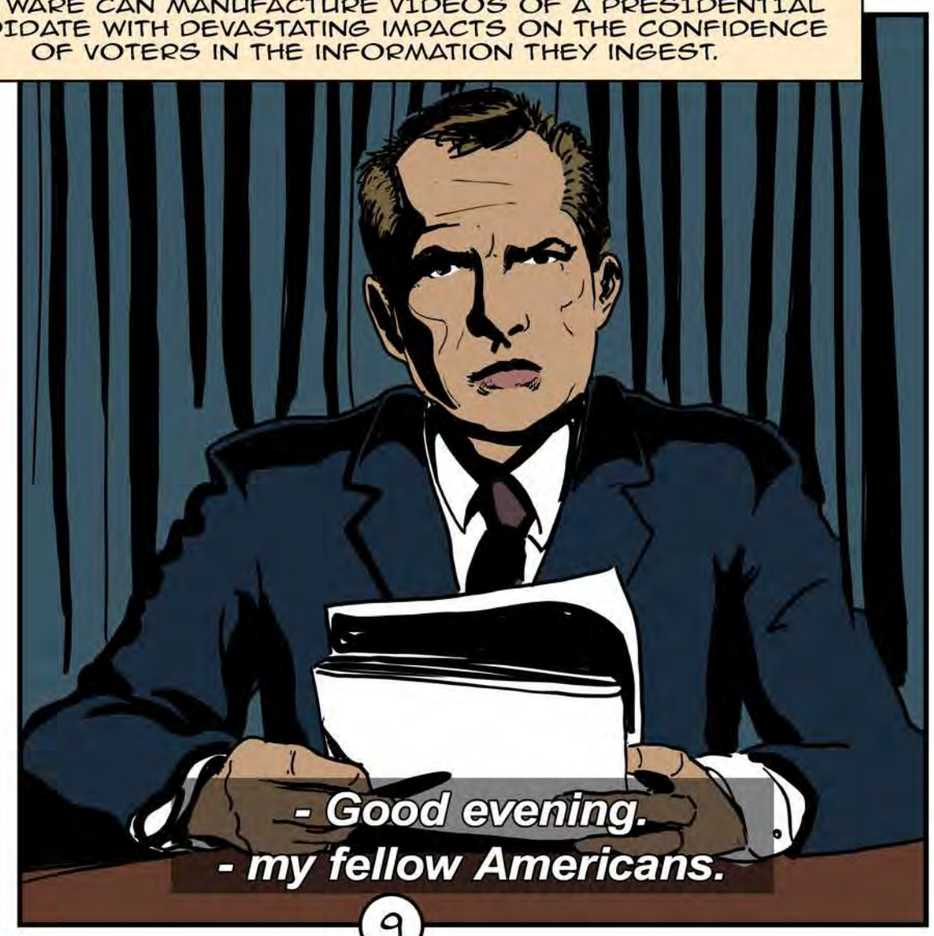
ADVERTISEMENT

r/deepfakes Rules



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 OR 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.

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.

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.

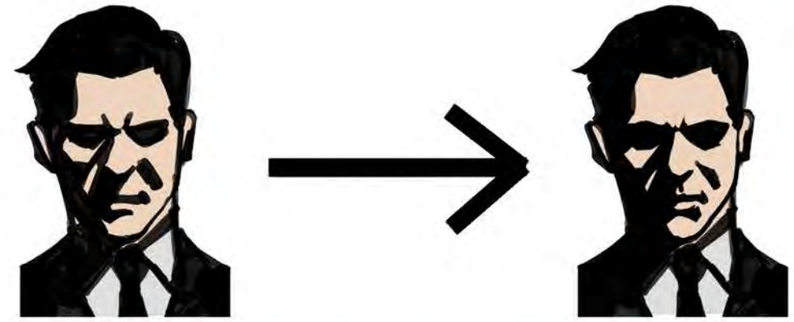
THE FINANCIAL, POLITICAL, AND SOCIAL THREAT POSED BY DEEPFAKES (AND TODAY CHEAP FAKES), IS A VERY REAL RISK ABOUT WHICH SOCIETY AT LARGE NEEDS TO DEVELOP AWARENESS AND RESILIENCE.

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.

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.

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.



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.

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 PERVASIVE IN THE COMING YEARS.

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 OF AN ENTERTAINMENT EXPERIENCE.

ANOTHER EXAMPLE WHERE THE TECHNOLOGY HAS FOUND A HOME, ONCE AGAIN IN THE ENTERTAINMENT INDUSTRY, IS IN GAMING.

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.

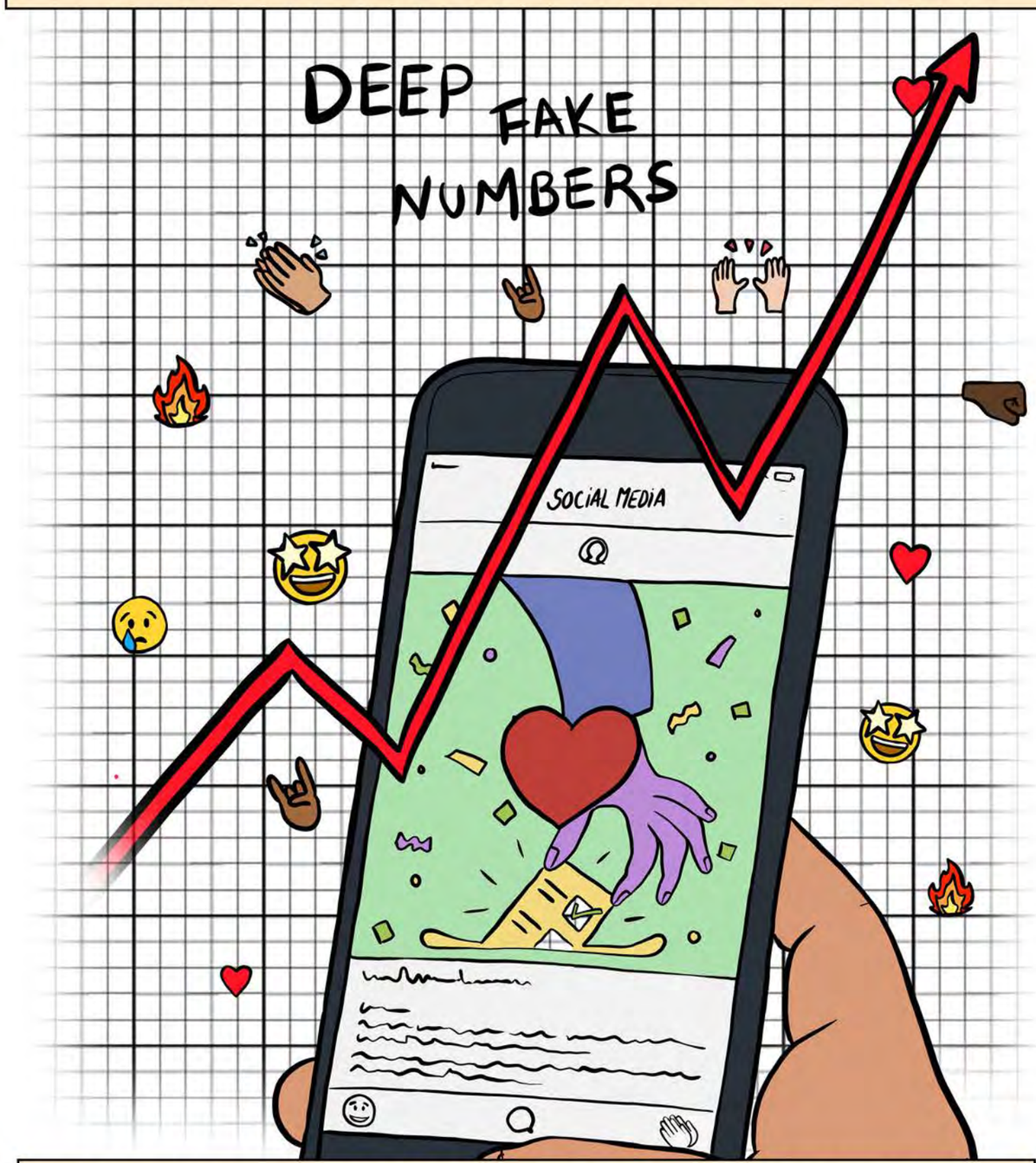
16

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.

will know that there is some corner of another world that is forever mankind

17

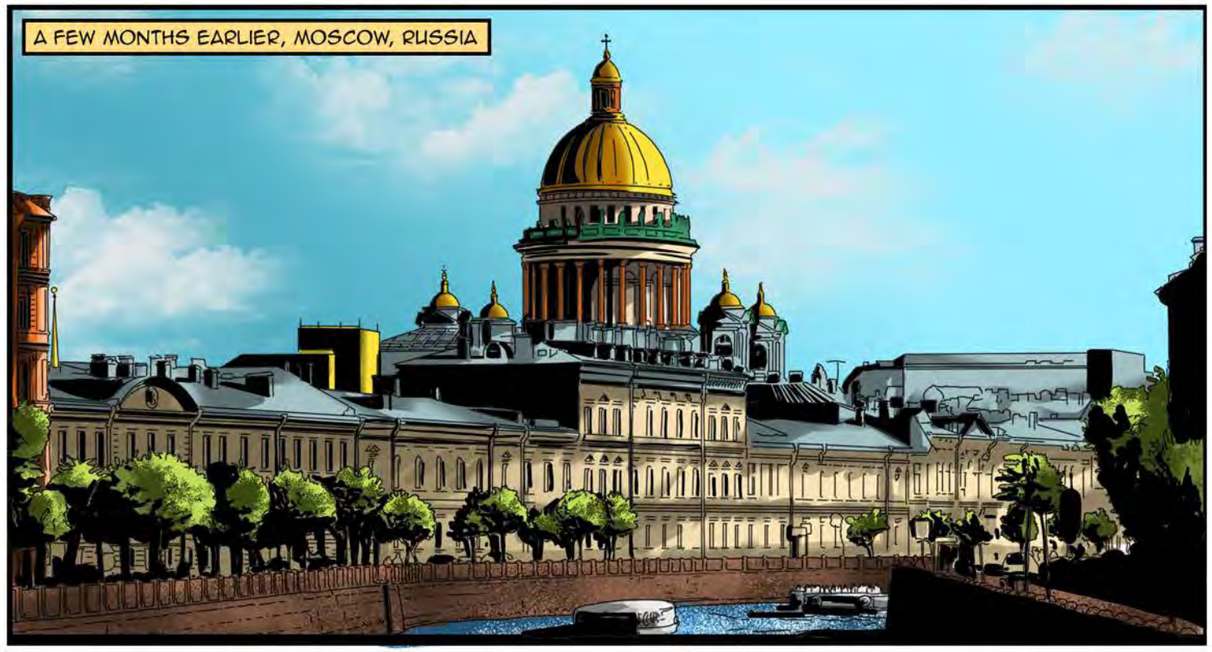
WHILE THE NUMBER OF DEEPFAKE AND CHEAP FAKE VIDEOS CONTINUES TO EXPLODE ON THE INTERNET, A NEW SET OF ORGANIZATIONS HAVE EMERGED TO IDENTIFY, TRACK, AND REPORT ON THESE THREAT VECTORS.

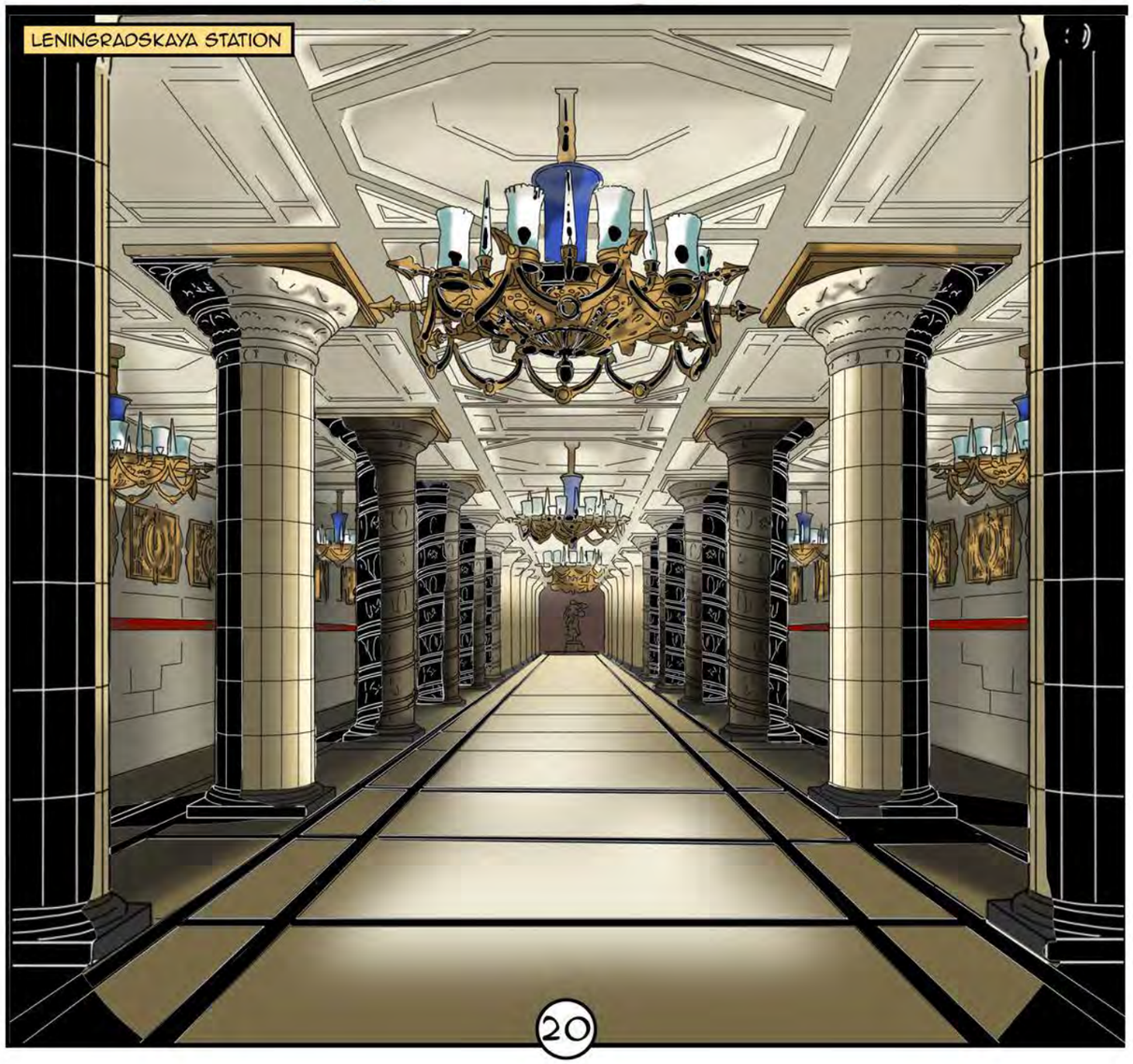


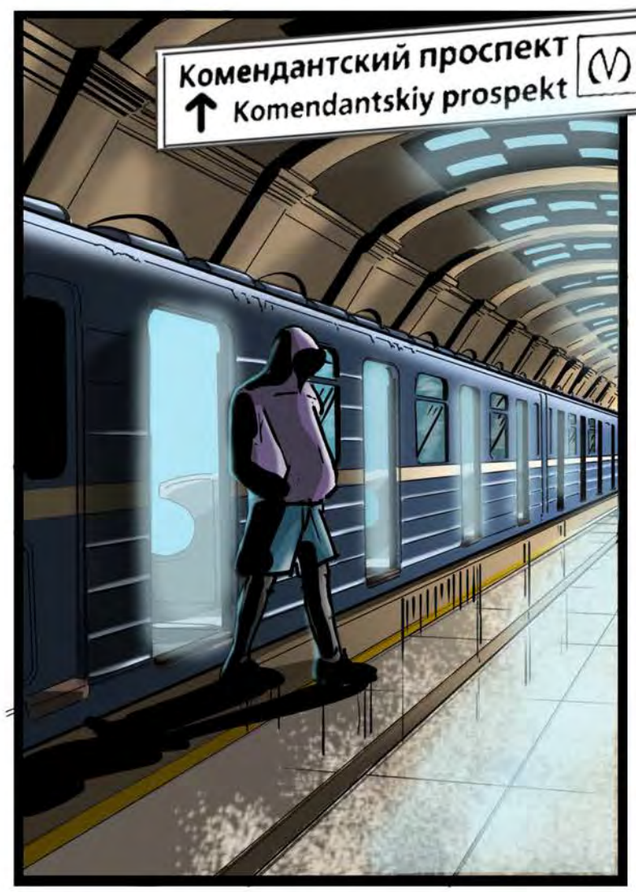
SOME OF THESE COMPANIES EMPLOY LARGE TEAMS THAT ARE SCANNING SOCIAL PLATFORMS AROUND THE WORLD AND IDENTIFYING THE EMERGENCE OF SUCH MEDIA, RECOGNIZING THAT SYNTHETIC CONTENT HAS THE POTENTIAL TO IMPACT ECONOMIES AND PEOPLE AROUND THE WORLD.

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.

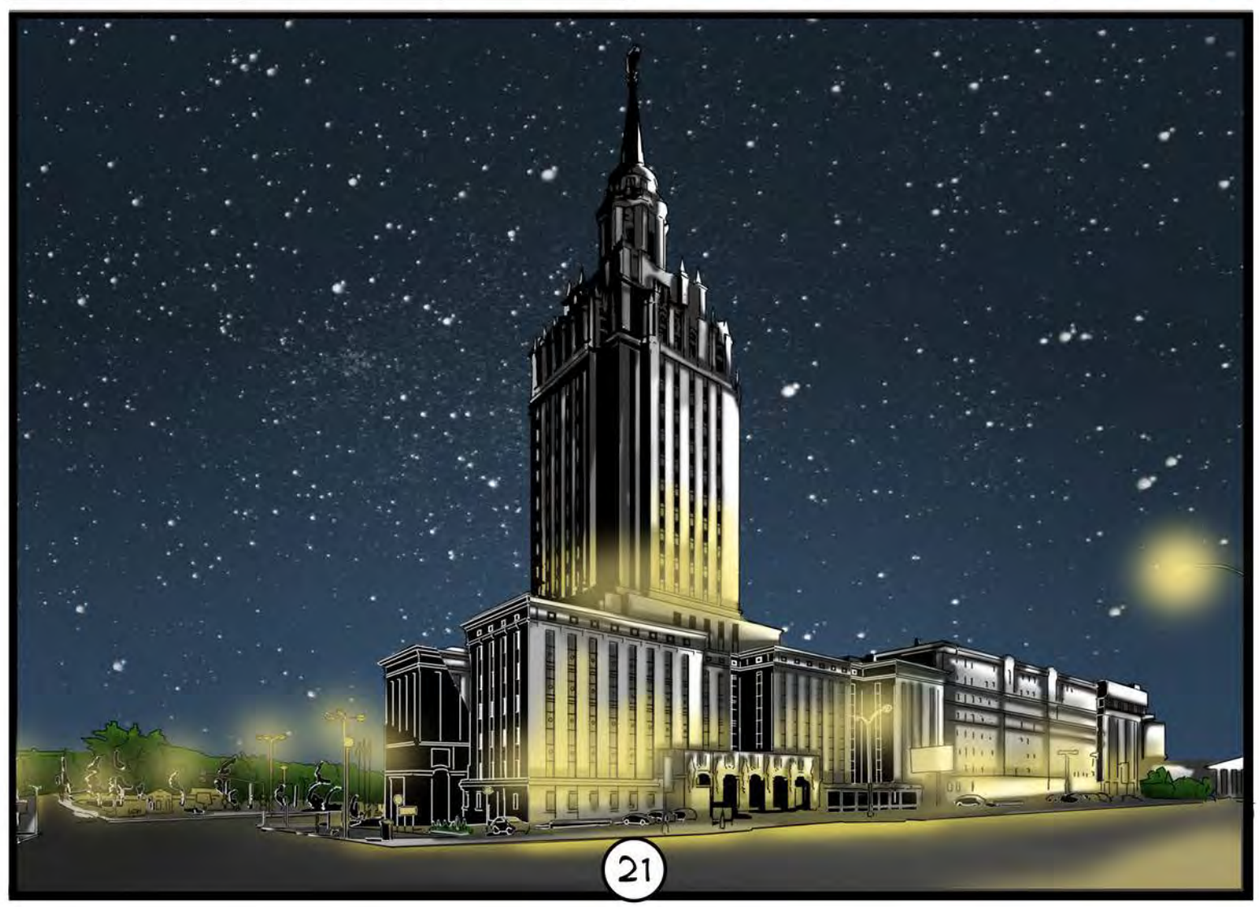
WHILE MANY IN THE MEDIA ARE DOING GREAT WORK TO UNCLOAK AND REPORT ON DISINFORMATION AND EVEN IDENTIFY SPECIFIC DEEPFAKES, ALL OF THIS TALK ABOUT DISINFORMATION ALSO FEEDS WHAT IS REFERRED TO AS THE 'LIARS DIVIDEND.' THE PUBLIC BECOMES INCREASINGLY HYPERAWARE OF THE ISSUE AROUND THE ORIGIN OF CONTENT THAT THEY MAY EVEN START TO DOUBT THE VERACITY OF LEGITIMATE VIDEOS AND MEDIA ON THE INTERNET.

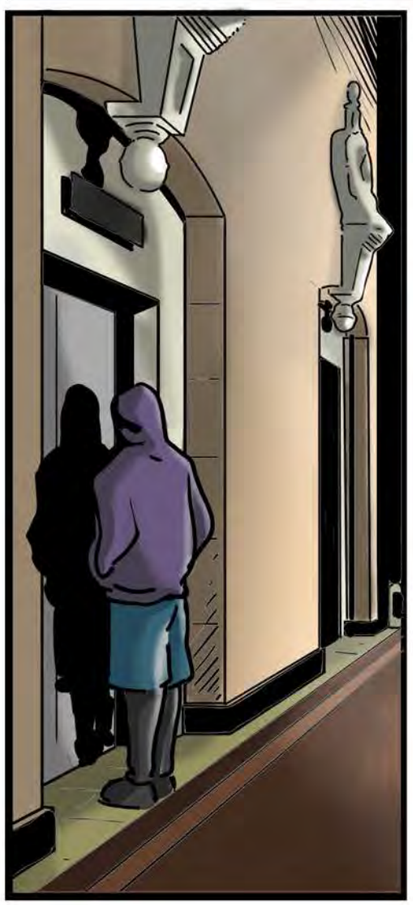

A FEW MONTHS EARLIER, MOSCOW, RUSSIA


LENINGRADSKAYA STATION

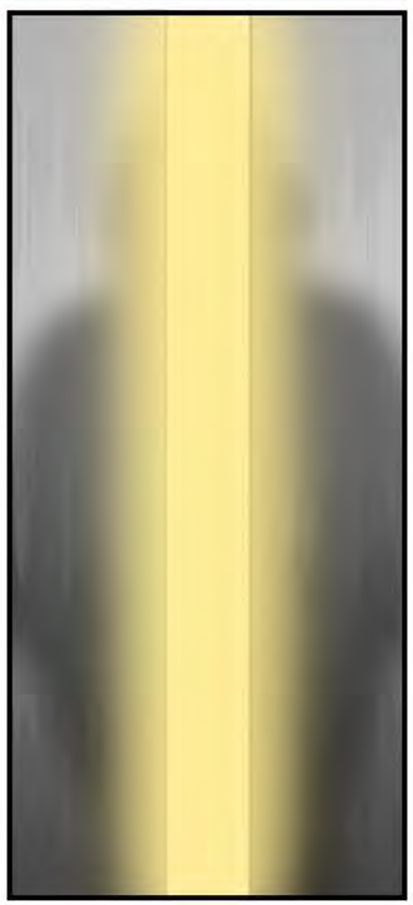

Комендантский проспект
Komendantskiy prospekt
5

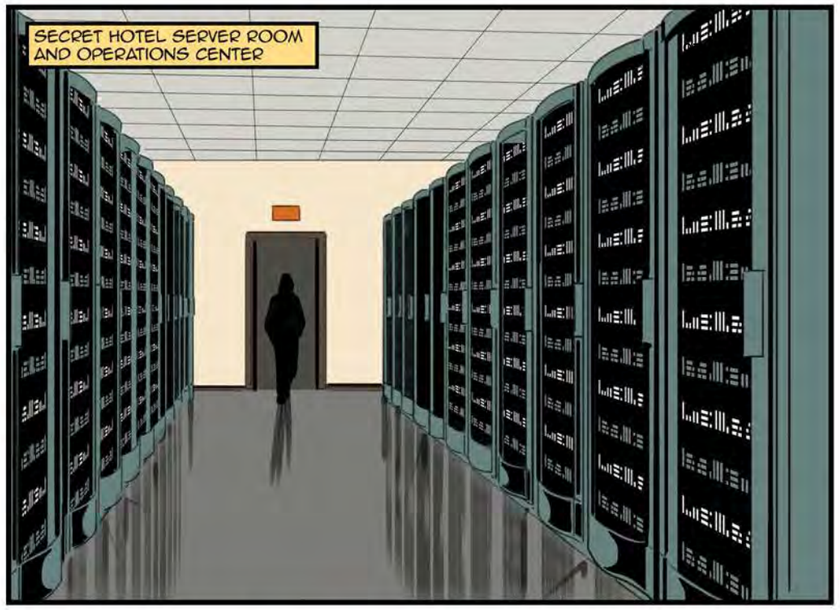

Комендантский проспект
Komendantskiy prospekt
5

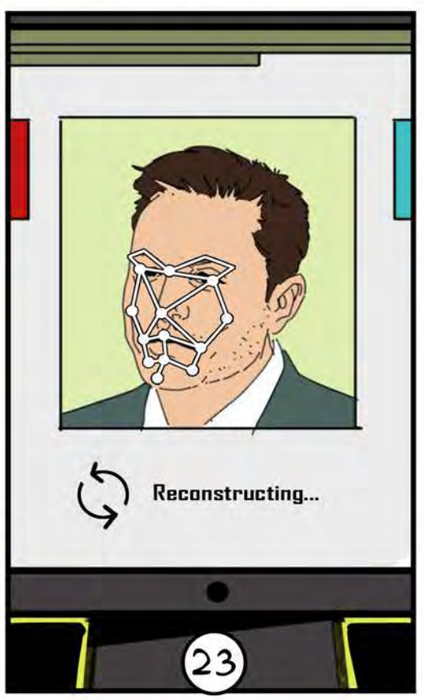


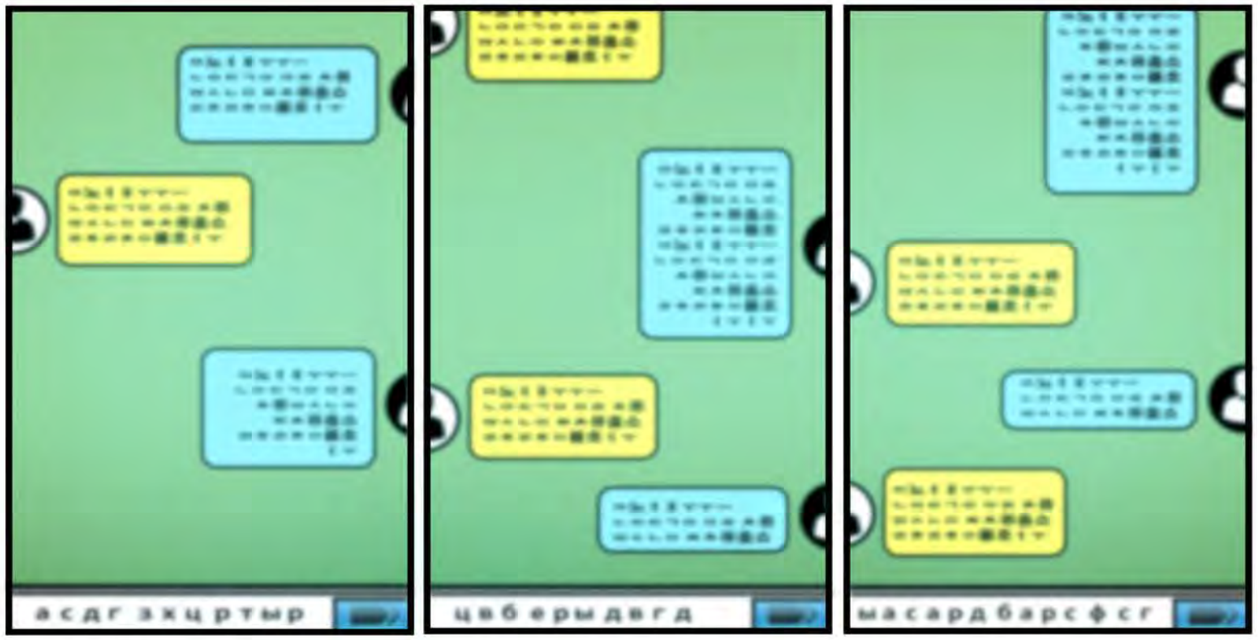


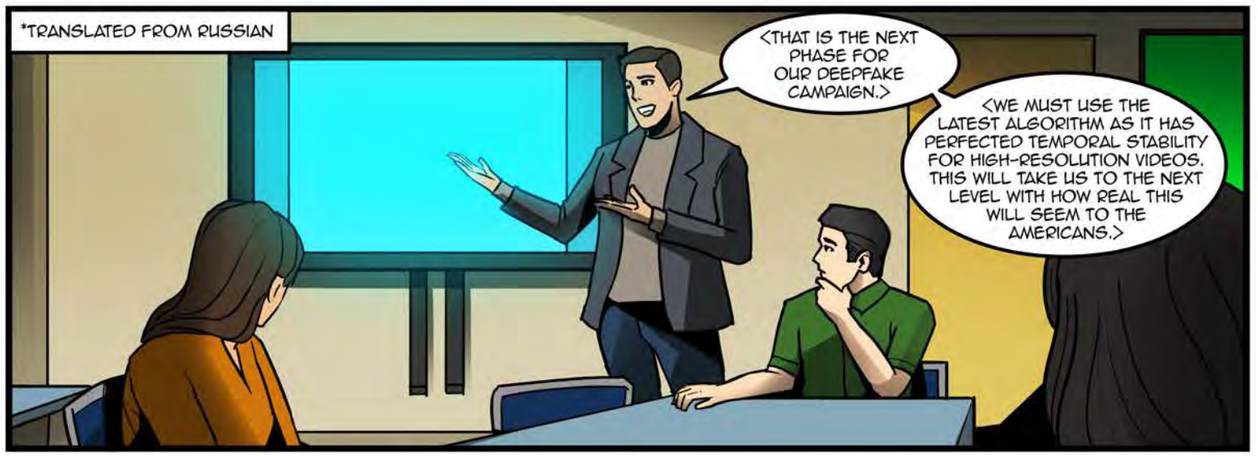

DING!
22

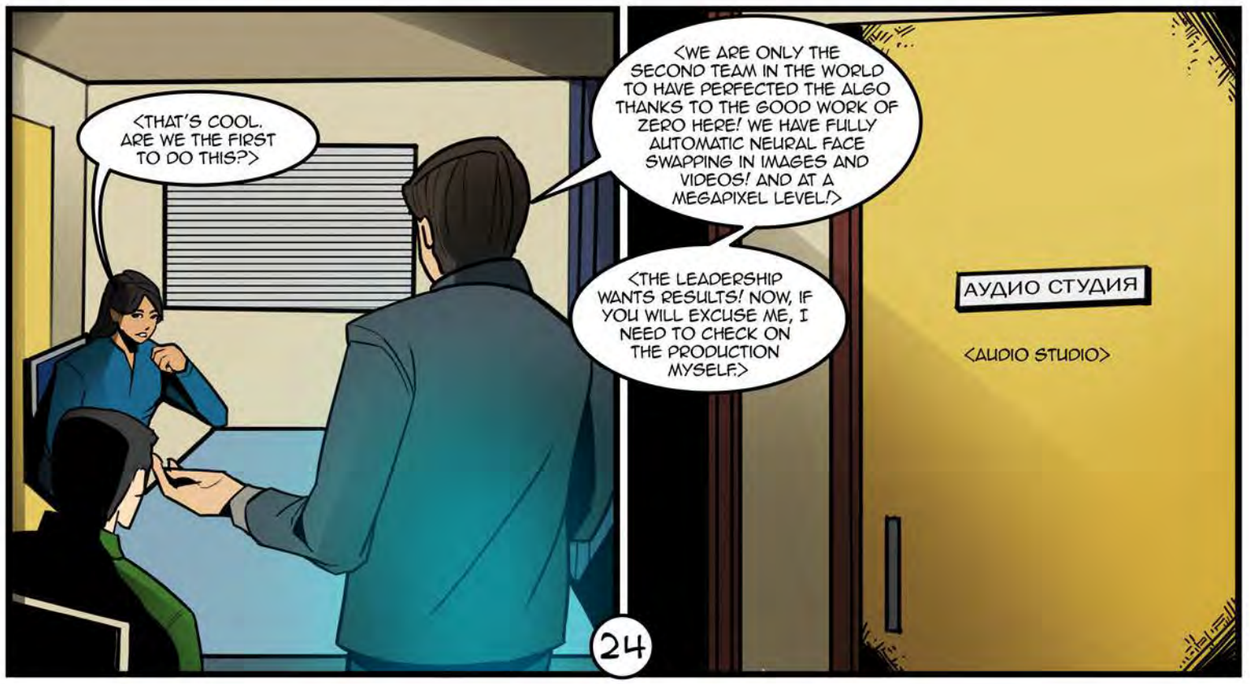


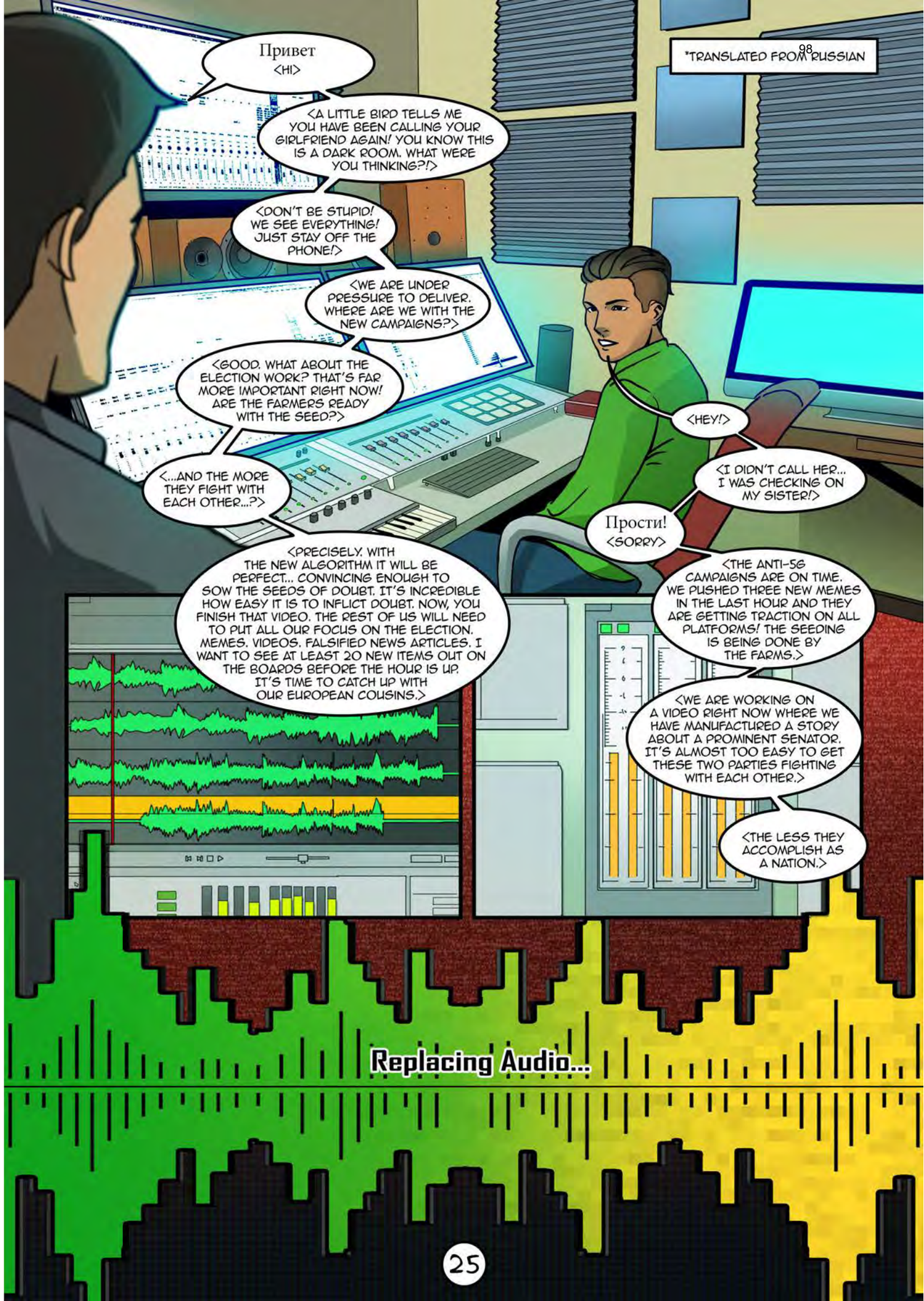

SECRET HOTEL SERVER ROOM
AND OPERATIONS CENTER

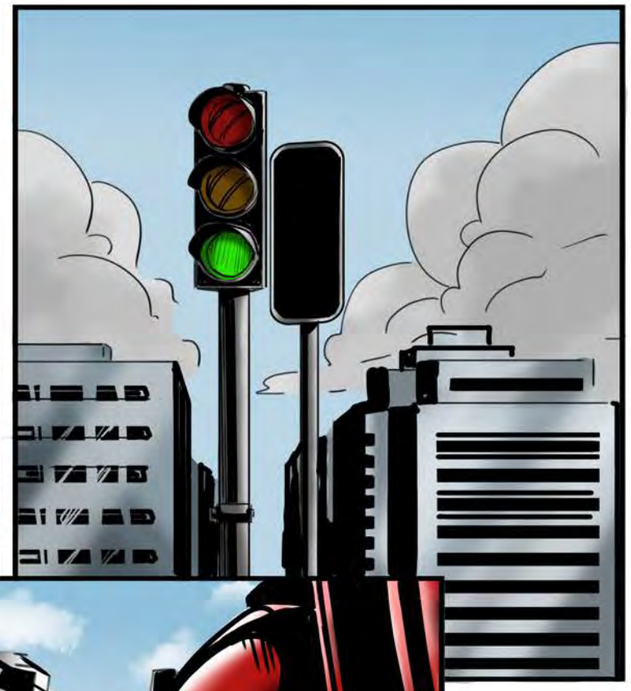

Reconstructing...
23


асдг зхцртмр
цвберыдвгд
масардбарсфсг


*TRANSLATED FROM RUSSIAN
<THAT IS THE NEXT PHASE FOR OUR DEEPFAKE CAMPAIGN.>
<WE MUST USE THE LATEST ALGORITHM AS IT HAS PERFECTED TEMPORAL STABILITY FOR HIGH-RESOLUTION VIDEOS. THIS WILL TAKE US TO THE NEXT LEVEL WITH HOW REAL THIS WILL SEEM TO THE AMERICANS.>

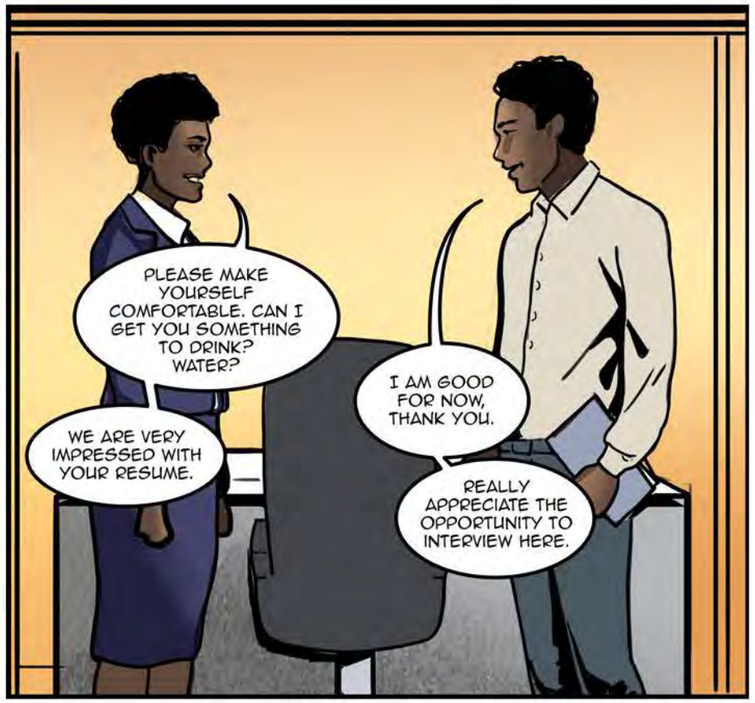

<THAT'S COOL. ARE WE THE FIRST TO DO THIS?>
<WE ARE ONLY THE SECOND TEAM IN THE WORLD TO HAVE PERFECTED THE ALGO THANKS TO THE GOOD WORK OF ZERO HERE! WE HAVE FULLY AUTOMATIC NEURAL FACE SWAPPING IN IMAGES AND VIDEOS! AND AT A MEGAPIXEL LEVEL!>
<THE LEADERSHIP WANTS RESULTS! NOW, IF YOU WILL EXCUSE ME, I NEED TO CHECK ON THE PRODUCTION MYSELF.>
АУДИО СТУДИЯ
<AUDIO STUDIO>
24


98
*TRANSLATED FROM RUSSIAN
Привет
<HI>
<A LITTLE BIRD TELLS ME YOU HAVE BEEN CALLING YOUR GIRLFRIEND AGAIN! YOU KNOW THIS IS A DARK ROOM. WHAT WERE YOU THINKING?!>
<DON'T BE STUPID! WE SEE EVERYTHING! JUST STAY OFF THE PHONE!>
<WE ARE UNDER PRESSURE TO DELIVER. WHERE ARE WE WITH THE NEW CAMPAIGNS?>
<GOOD. WHAT ABOUT THE ELECTION WORK? THAT'S FAR MORE IMPORTANT RIGHT NOW! ARE THE FARMERS READY WITH THE SEED?>
<...AND THE MORE THEY FIGHT WITH EACH OTHER...?>
<HEY!>
<I DIDN'T CALL HER... I WAS CHECKING ON MY SISTER!>
Прости!
<SORRY>
<PRECISELY. WITH THE NEW ALGORITHM IT WILL BE PERFECT... CONVINCING ENOUGH TO SOW THE SEEDS OF DOUBT. IT'S INCREDIBLE HOW EASY IT IS TO INFLICT DOUBT. NOW, YOU FINISH THAT VIDEO. THE REST OF US WILL NEED TO PUT ALL OUR FOCUS ON THE ELECTION. MEMES. VIDEOS. FALSIFIED NEWS ARTICLES. I WANT TO SEE AT LEAST 20 NEW ITEMS OUT ON THE BOARDS BEFORE THE HOUR IS UP. IT'S TIME TO CATCH UP WITH OUR EUROPEAN COUSINS.>
<THE ANTI-5G CAMPAIGNS ARE ON TIME. WE PUSHED THREE NEW MEMES IN THE LAST HOUR AND THEY ARE GETTING TRACTION ON ALL PLATFORMS! THE SEEDING IS BEING DONE BY THE FARMS.>
<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.>
<THE LESS THEY ACCOMPLISH AS A NATION.>
Replacing Audio...
25



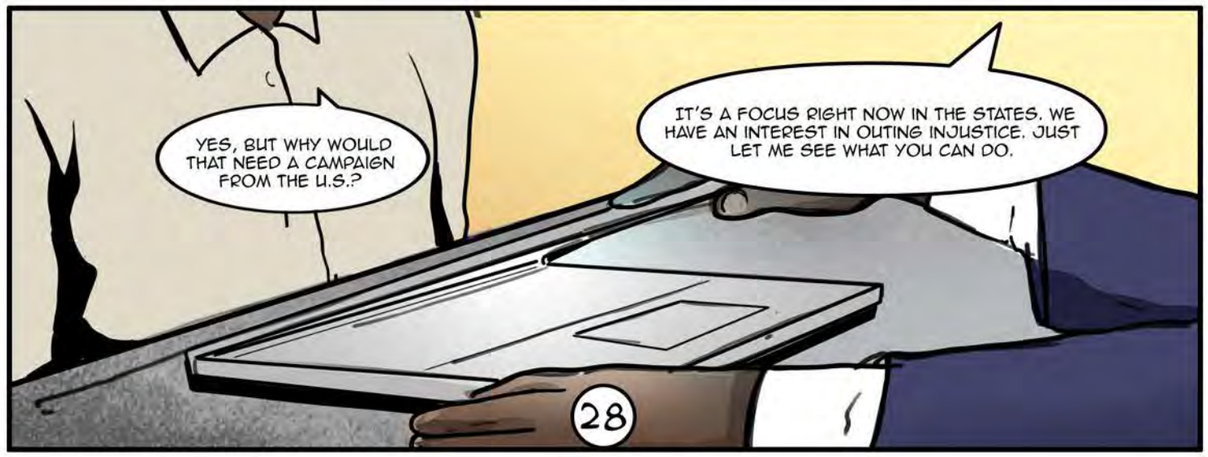
26

27

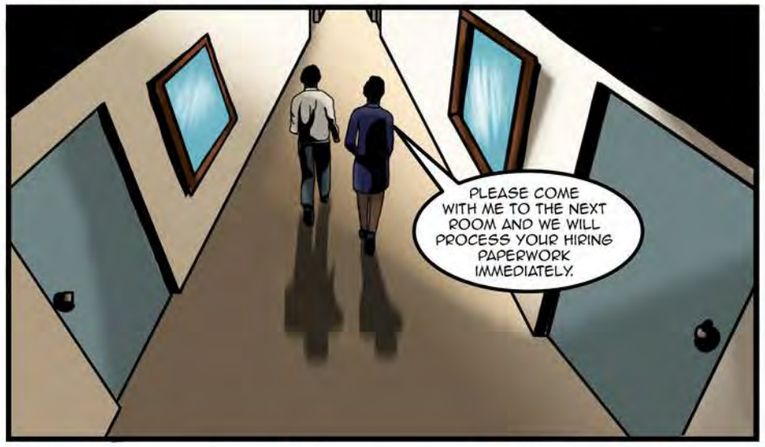

PLEASE MAKE YOURSELF COMFORTABLE. CAN I GET YOU SOMETHING TO DRINK? WATER?
WE ARE VERY IMPRESSED WITH YOUR RESUME.
I AM GOOD FOR NOW, THANK YOU.
REALLY APPRECIATE THE OPPORTUNITY TO INTERVIEW HERE.


SO TELL ME A LITTLE ABOUT YOUR EXPERIENCE WITH CONTENT CREATION ON SOCIAL MEDIA.
WELL... I DID SOME WORK AROUND THE EBOLA VIRUS IN AFRICA LAST YEAR THROUGH SOME FREELANCING PLATFORMS.


VERY NICE. TELL ME, COULD YOU WRITE SOMETHING RIGHT NOW FOR ME? IN AMERICAN ENGLISH?
I COULD, YES.
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 AN INTEREST IN OUTING INJUSTICE. JUST LET ME SEE WHAT YOU CAN DO.
28


30 MINS AFTER A SUCCESSFUL INTERVIEW...
WOW! THIS IS A DREAM COME TRUE. YES. OF COURSE.
NANA, 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 PROCESS YOUR HIRING PAPERWORK IMMEDIATELY.


CREEEAK...


CAN'T WAIT TO LET MAMA KNOW I GOT THE JOB.
29

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.

HAH..HI...

NUNEWZ CO-FOUNDERS' OFFICE

Ring!

+33 9705...
Incoming call

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?

NUNEWZ BOARDROOM

A FEW HOURS LATER AT AN IMPORTANT INVESTOR MEETING

I JUST WANT TO APOLOGIZE ON BEHALF OF THE NUNEWZ FOUNDERS. THEY ARE BOTH CURRENTLY INDISPOSED.

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

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

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 FAR LONGER THAN THREE MONTHS.

THE FIGURES ARE FAIR. YOU KNOW THAT WE ARE TURNING OVER TENS OF THOUSANDS IN PROFITS EVERY MONTH. IT'S A SURE THING.

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

RIGHT THIS WAY, SIR, AND WE WILL START THE PAPERWORK FOR YOUR INVESTMENT.

THE FOUNDERS WILL BE REALLY HAPPY WITH THIS OUTCOME.

AND HE SAID THAT HE HAD OTHER FRIENDS WHO MAY ALSO WANT TO INVEST!

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

MEANWHILE IN WESTERN EUROPE...

TWO TACOS PLEASE!

IT ALMOST FEELS LIKE AUSTIN DURING SOUTH BY!

SO GREAT THAT WE HAVE THE FOOD TRUCK SCENE HERE!

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

ICHTECH OFFICES

SO HOW ARE YOUR NUMBERS THIS WEEK?

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 ASSETS USED IN THE AD, AS IN COMPARE WHAT WORKS BETTER: IMAGE A OR B. OR AGAIN COPY A OR B. HAPPY TO SHARE SOME OF MY TOP TIPS. I STILL TOP THE LEADERBOARD WITH MY ANTI-5G VACCINE POST WITH TWO MILLION ENGAGEMENTS!

GETTING THE FEELING I SHOULD HAVE STAYED IN THE WORLD OF BIG AGENCIES!

PING

NEW MAIL
BOSS
New campaign starting...

boss@email.com

US Senator caught red-handed on a "Video" taking bribes to push for a planning permit for a foreign group

CAN'T BELIEVE THESE PEOPLE! WHY WOULD ANYONE SELL THEIR INTEGRITY FOR A FEW DOLLARS!

DO YOUR HOMEWORK! CHECK YOUR SOURCES. REMEMBER TO USE ACCOUNTS THAT SHOW DIVERSE PEOPLE WITH FOLLOWERS AND HISTORY. THESE ARE ALL READY FOR YOU.

WHO DID YOU SAY WE GET THE VIDEOS FROM?

FIND THE USERNAMES AND PASSWORDS IN THE ENCRYPTED EMAILS SENT TO YOU AND ***DO NOT*** SHARE IT WITH ANYONE. REMEMBER, WE ARE TASKED WITH MAKING SURE THAT THE TRUTH IS OUT THERE!

A GOOD JOURNALIST NEVER REVEALS HIS SOURCES. NOW, LET'S GET ON WITH GETTING THESE VIDEOS SEEDED. THE CORRECT HASHTAGS ARE #SENATORONTHETAKE #CORRUPTSENATOR.

THE VIDEO FILE OF THE SENATOR TAKING THE DUFFLE 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!

We have begun project Solyanka! can you confirm if the last payment was sent? I still have not received it.

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.

BACK IN LOS ANGELES, USA

IT'S A BIT RISKY TO MEET UP SO SOON AND INTRODUCE THE IDEA OF SYMOUS, BUT WE DON'T SEEM TO HAVE MUCH TIME WITH THE CLOCK ON THE ELECTION TICKING!

Rachel
This Single0 guy is really getting on my nerves!

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

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

Andre
All bogus! None of that is true...

Rachel
I'm going to report this to the social media platform!

Andre
Let's hope they take the videos down.

Andre
Aiden

UyCATCH.com

HOME | SIGN UP | LOG IN

Andre Jackson

Andre Jackson

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

YUP! DEFINITELY THE SAME ANDRE AS ON COMMBLOGZ. IT'S AMAZING, AND SCARY, HOW MUCH INFORMATION I CAN GET FROM THIS SITE. NO WONDER CYBERSTALKING IS SUCH A PROBLEM. PEOPLE NEED TO BE MORE CAREFUL ABOUT HOW MUCH THEY PUT OUT THERE...

SO, ANDRE. IT TURNS OUT WE HAVE MORE IN COMMON THAN WE THOUGHT. SEEMS WE EACH HAVE A PASSION FOR DEMOCRACY, VOTER RIGHTS, SCI-FI AND K-9 COMPANIONS!

Coffee SHOP

YOU REMEMBER EVERYTHING FROM MY PROFILE. IMPRESSIVE! I LOVE DOGS... HAVE A COCKAPOO! YOU?

GERMAN SHEPHERD. HE'S AN OLD POLICE DOG. BEEN WITH ME FOR 7 YEARS NOW. NAMED CHEWIE... YOU KNOW AFTER THE HAIRY CHARACTER IN THE GREATEST SPACE STORY EVER TOLD!

NOT "TREK"... "WARS," DUMMY, "WARS!"

THERE IS NO CHEWIE IN "STAR TREK."

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!

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?

HEY I GET IT, BUT LET'S TRY TO KEEP IT A LITTLE MORE LOW KEY.

SORRY... I DIDN'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?

WHAT DO YOU MEAN?

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 THAT?

EVER HEARD OF SYMOUS?

!!

WOW! UM. WOW! THAT'S A LOT TO DIGEST.

I WILL NEED SOME TIME TO THINK ABOUT THAT...

ALSO, YOUR OLD FRIEND AIDEN PATEL FROM NICT IS ALREADY A MEMBER. HE COULDN'T STOP RAVING ABOUT YOU! WE HAVE RESOURCES SO I AM NOT LOOKING FOR ANY MONEY FROM YOU. WE HAVE SIGNIFICANT BACKING.

SORRY ANDRE... DIDN'T MEAN TO SNEAK THIS UP ON YOU! BUT THIS IS A LEGIT OPERATION AND WE HAVE AN OPPORTUNITY TO MAKE A DIFFERENCE.

WHAT DO YOU NEED ME FOR? WHAT CAN I DO? I AM JUST A COORDINATOR AT A VOTER ADVOCACY GROUP.

NO. WE ARE JUST CIVIC-MINDED CITIZENS TOO! SYMOUS IS A GROUP OF CITIZENS DEFENDING THE TRUTH AND DEMOCRACY ONLINE. IF RACHEL HASN'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.

SERIOUSLY, WHAT IS THIS? AIDEN, ARE YOU TRYING TO PUNK ME?! THIS HAS TO BE A JOKE! THIS IS NUTS!

THIS IS REAL ANDRE. 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 APART POST BY POST.

HALF AN HOUR LATER...

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

DO YOU HAVE A VALID PASSPORT?

TOTALLY. WHAT'S THE PLAN?

WE ARE GOING ON A LITTLE TRIP

WHERE ARE WE HEADED? CANADA?

HAH! NICE ONE!

JUST A LITTLE FURTHER THAN THAT.

I HOPE YOU LIKE KARTOFFELPUFFER?

HUH? IS THAT SOME KIND OF EUROPEAN DANCE?

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

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

SEE YOU FOLKS THERE. I'LL BE ON THE 3 PM FLIGHT OUT OF LOGAN! I HEAR YOU GUYS WILL BE TAKING THE GULFSTREAM FROM LA!

VAN NUYS AIRPORT, LOS ANGELES

DID I MENTION THAT WE NEED TO SWING THROUGH WEST AFRICA ON THE WAY BACK?

WHAT!? THIS IS A BIT MUCH! WHY DO WE NEED TO GO THERE?

WELL, 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 ABSORBING ALL THESE SURPRISES.

THAT'S FAIR...

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

WE ALL STRAPPED IN AND READY TO GO?

SOMEWHERE OVER U.S. AIRSPACE CROSSING A STATE BORDER...

I AM NOT A GOOD FLIER. DID I FORGET TO MENTION THAT? SODA SEEMS TO HELP.

YOU OKAY?

YES! GLAD TO SEE THAT YOU ARE AS SHARP AS EVER DESPITE THE FLIGHT SICKNESS! GOT A BARF BAG READY?

OKAY, SO YOU ARE SAYING THAT WE ARE PRETENDING TO BE INVESTORS INTERESTED IN PUTTING MONEY INTO A SOCIAL MEDIA STARTUP WHICH IS A FRONT FOR A TROLL FARM?

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.

WE SUSPECT THE PLACE IS BEING RUN OUT OF MOSCOW. AND YOU REMEMBER THAT TROLL YOU WERE SO UPSET ABOUT? THE ONE WHO POSTED THE DEEPFAKE? MR. ZERO... ONE OF THOSE PEOPLE IS THAT TROLL.

I THOUGHT THAT GUY WAS FROM NORTH KOREA?!

FIRST, IT MAY NOT BE A GUY. TAKE A LOOK AT ME FOR INSTANCE. PLENTY OF US ARE FEMALE HACKERS! SECOND, IT'S NEVER AS SIMPLE AS WYSIWYG (WHAT YOU SEE IS WHAT YOU GET) IN THIS SPACE.

FAIR ENOUGH. SO, YOU'RE THINKING THAT IT'S OUR FRIENDS IN MOSCOW?

ALMOST CERTAINLY, BUT THEY ARE USING A NETWORK OF TROLL FARMS ALONG WITH MORE SOPHISTICATED DEEPFAKE TECH THAN I HAVE EVER SEEN BEFORE. OUR FIRST STOP IS COURTESY OF AN OLD CONTACT AT MOSCOW TECHNICAL UNIVERSITY.

I DID NOT. BUT WHAT DOES THAT HAVE TO DO WITH OUR TRIP?

DID YOU KNOW THE GUY WHO CAME UP WITH THE PERIODIC TABLE OF ELEMENTS, WENT TO SCHOOL THERE?

MY CONTACT THERE TIPPED ME OFF ON SOME CHATTER ABOUT THE FARMS WE ARE ABOUT TO VISIT.

SO WHAT'S THE DEAL WITH WHERE WE ARE GOING?

IT'S A NODE IN THE NETWORK. JUST ONE TROLL FARM AMONGST THE MANY. WE KNOW THAT THE POSTS ARE BEING SEEDED FROM THERE BUT I NEED THE LINK TO MOSCOW. UNFORTUNATELY, THEY HAVE GONE OFF-GRID ON COMMUNICATING WITH THEIR HANDLERS.

SO YOU WANT TO PLAY CODE BREAKER?

NOT QUITE. THIS MAY BE A LOT MORE BASIC THAN TRYING TO PLAY TURING. I HAVE A FEELING THAT I NEED TO GET MY HANDS ON A MANAGER'S PHONE TO SEE WHO THEY ARE CALLING, IT'S LIKELY TO BE A BURNER, HENCE THE REASON WHY WE HAVEN'T BEEN ABLE TO TRACE IT AS OF YET. AIDEN WILL PRETEND TO BE A COMPETING INVESTOR WHILE WE ARE THERE AND DISTRACT THEM WHILE I DO WHAT IS NEEDED.

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 WW2.

AHHH!

WOOAAAH! STEADY THERE! (LAUGHS)

PRIVATE AIRFIELD OUTSIDE EUROPEAN CITY CENTER

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.

calling...

EXCUSE ME, I HAVE TO ATTEND TO THIS AS IT'S ANOTHER POTENTIAL INVESTOR.

PING!

48

Preview

+44*******

We need an update on Project Solyanka and the Senator campaign?

admin

WELL THAT ABOUT DOES IT. THAT'S A SMOKING GUN IF WE EVER NEEDED ONE. THAT WAS ALMOST TOO EASY.

!!

RIGHT THEN...

CLAP

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 RICH 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!

Just had a term sheet from a prospective US investor.

What's the offer? I can counter.

I am happy to consider another offer.

ZZT!!!

49

GOTCHA! PROOF IN HAND. FINALLY!

To HQ

Rachel

I saw this number pop up on his screen, could you trace it for me? I think this might be what we need. +44 ********

RACHEL TERMINAL V 1.5

TRANSFER COMPLETE

BRO! IT'S BEEN AGES!

AN HOUR LATER, BACK AT THE AIRSTRIP.

YES, IT HAS.

GLAD TO SEE YOU ARE STILL GREAT AT GETTING US BOTH IN OVER OUR HEADS.

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

50

PRIVATE AIRSTRIP, OUTSKIRTS OF WEST AFRICAN CITY

WELCOME! WE HAVE BEEN EXPECTING YOU!

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

WE HAVE A RAID PARTY READY AND A COURT-MANDATED SEARCH WARRANT IN HAND! THANKS FOR THE TIP-OFF.

YOU GUYS MIGHT WANT TO MOVE FAST. WE HEAR SOME CHATTER ABOUT SHIFTING BASE HERE. IF THAT HAPPENS THERE IS NO TELLING HOW LONG IT WILL TAKE FOR A NEW LEAD TO SURFACE. YOU MAY NEED TO TAKE THEM TONIGHT!

WE KNOW THAT A NUMBER OF INTERNATIONAL PARTIES HAVE BEEN TRACKING THIS TROLL FARM AND ARE KEEN TO SPEAK WITH THE OWNERS OF THIS ALLEGED TROLL FARM.

51

CRASH!

FREEZE. THIS IS THE CENTRAL POLICE AUTHORITY!

52

ROUND EACH AND EVERY ONE OF THEM UP. NO EXCEPTIONS!

I AM INNOCENT! I SWEAR IT!

SAVE YOUR BREATH FOR THE POLICE STATION.

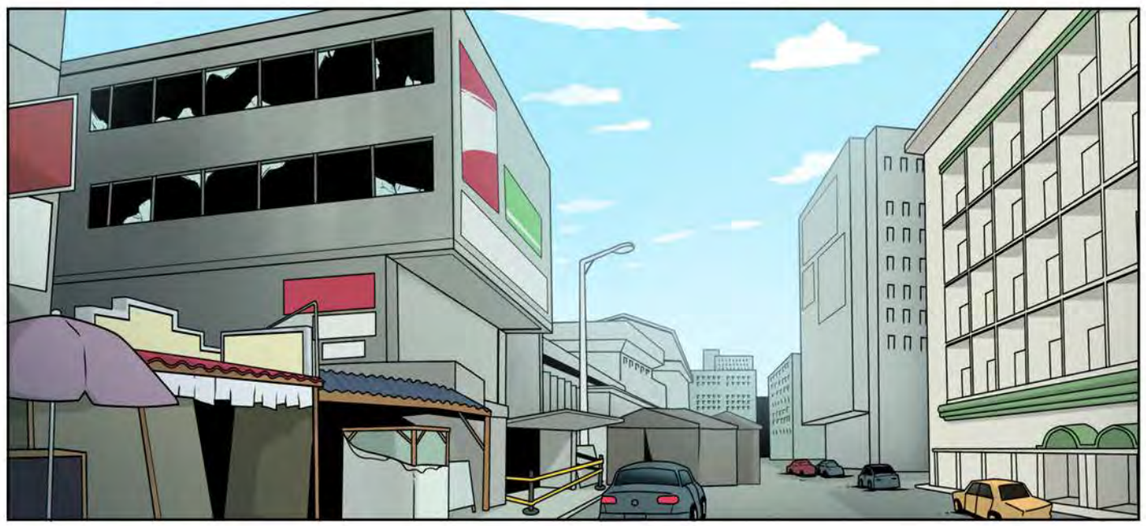
53

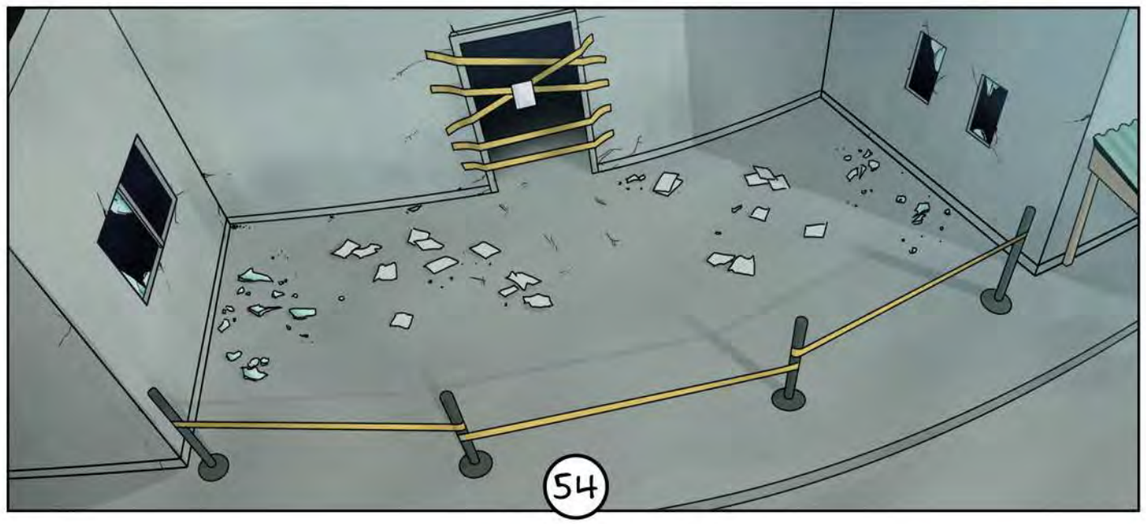
I ALMOST FEEL BAD FOR THEM. DO YOU THINK THEY KNEW WHAT THEY WERE DOING?

HOW COULD THEY NOT? I MEAN, THEY WERE MANUFACTURING PROPAGANDA. IT'S PRETTY OBVIOUS ISN'T IT?

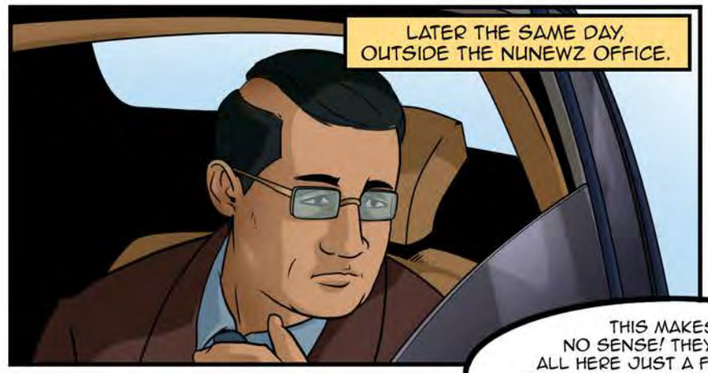
I'M NOT SO SURE. MAYBE, FROM THEIR PERSPECTIVE, THEY WERE MAKING A DIFFERENCE. YOU NEVER KNOW WHO WAS COMPLICIT AND WHO JUST GOT CAUGHT UP IN ALL OF THIS.

THE NEXT MORNING...

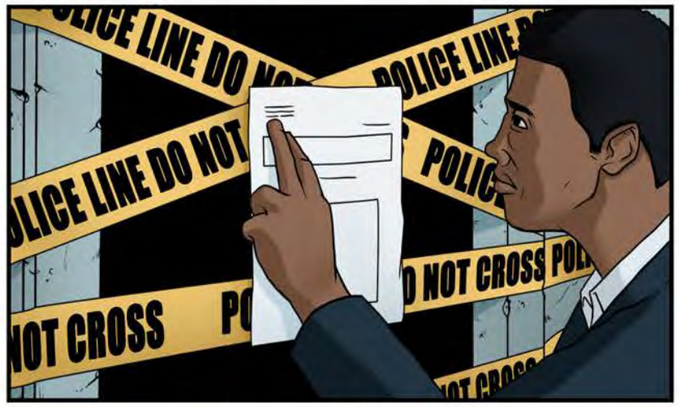


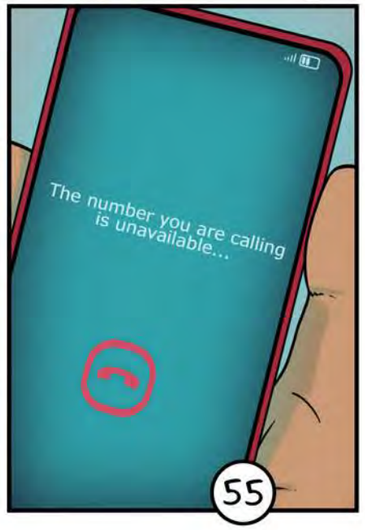


LATER THE SAME DAY, OUTSIDE THE NUNEWZ OFFICE.



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.





POLICE HOLDING CELL, WEST AFRICA.

PLEASE LET ME GO! I AM INNOCENT! I SWEAR IT. WE DID NOTHING WRONG! I WAS HIRED HERE. PLEASE CALL MY MOTHER...

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 FRIENDS DURING YOUR STAY WITH US HERE AT THE STATION...

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

I BELIEVE SOME CONGRATULATIONS ARE IN ORDER! WELL DONE EVERYONE!

OUR DATA TEAMS HAVE REPORTED THAT THE TAKEDOWN OF THOSE INTERNATIONAL TROLL FARMS HAS RESULTED IN A DRAMATIC DECREASE IN THE NUMBER OF INCIDENTS RELATING TO DISINFORMATION ONLINE. IT'S TRENDING 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 HEARING RUMBLINGS OF ACTIVITY BY DISINFORMATION CELLS IN OTHER PARTS OF ASIA. THESE GUYS ARE NIMBLE.

THANKS MR. CHAIRMAN. LET'S JUST SAY ITS A "TEAM SPORT." NOW ANDRE CAN GO BACK TO THAT STOREFRONT HE CALLS AN OFFICE AND LET THE "PROFESSIONALS" 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 ME ALONG ON THE JOURNEY. I HAVE LEARNED SO MUCH! IT'S GREAT TO BE A PART OF SYMOUS.

WE ARE JUST GETTING STARTED ANDRE. AS WE HEAD INTO THE FINAL WEEKS AHEAD OF THE BIG ELECTION DAY, REST 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
C. Bregler and others. “Video Rewrite: Driving Visual Speech With Audio.” 1997
www2.eecs.berkeley.edu/Research/Projects/CS/vision/human/bregler-sig97.pdf

Page 9, 11, 13, 15, 17, 19
www.news.mit.edu/2020/mit-tackles-misinformation-in-event-of-moon-disaster-0720

Page 15
J. Naruniec and others. “High-Resolution Neural Face Swapping for Visual Effects.” 2020
s3.amazonaws.com/disney-research-data/wp-content/uploads/2020/06/18013325/High-Resolution-Neural-Face-Swapping-for-Visual-Effects.pdf

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.

This document was created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint Mis/Disinformation Working Group. This document is intended to be used by state, local, tribal, and territorial election officials and industry partners as part of a larger mis-, dis-, and malinformation (MDM) response strategy.

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.

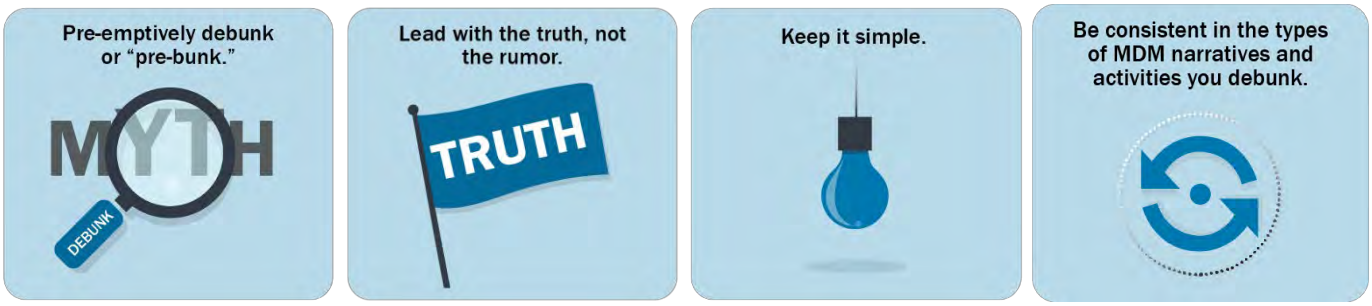
Above all, use caution when deciding what rumors to include on your page. Before developing a response, consider whether any of the following factors are at play to determine the best path forward:

- **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.

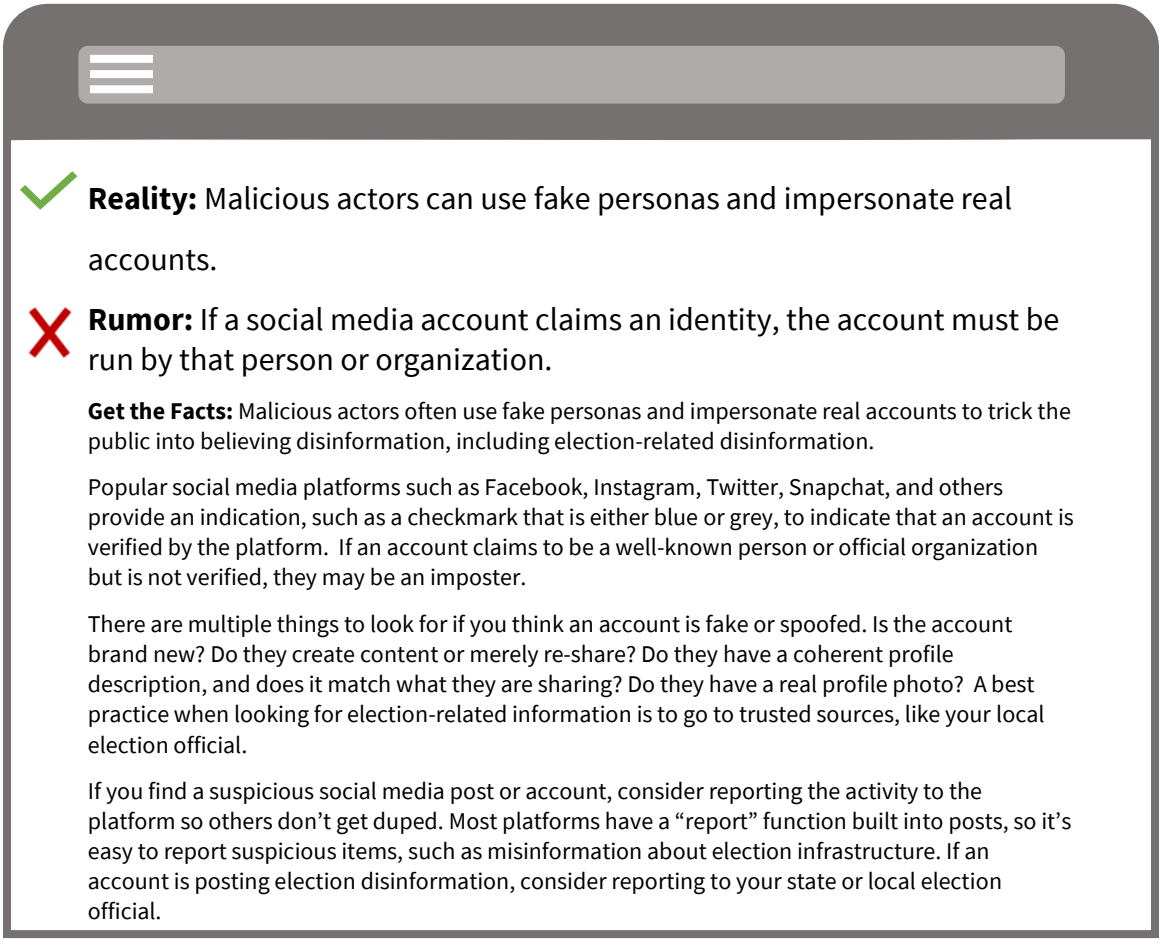
How do you communicate effectively on a rumor control page?



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.

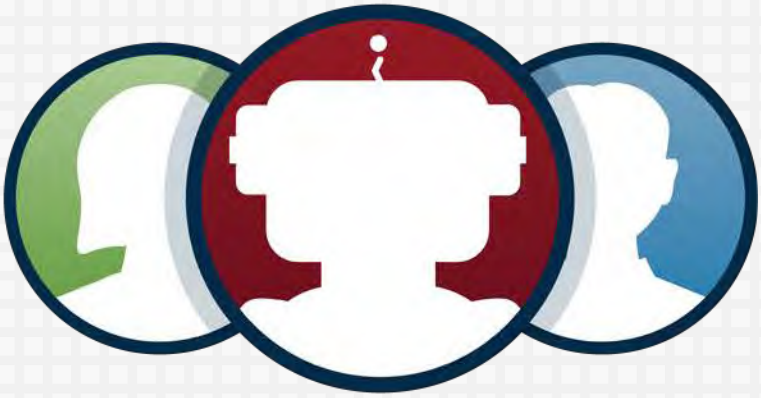
ASSESSMENT		
My organization has the expertise and mission set to distinguish the narrative from good faith discourse.	Yes	No
My organization has the expertise and responsibility to clearly and appropriately dispel the false narrative and articulate the facts.	Yes	No
The narrative is around a contentious or disputed topic, where information is changing or not widely known.	Yes	No
The narrative pertains to systems, information, processes, or expertise that is operated by or unique to my organization.	Yes	No
TRENDS		
The MDM narrative is trending on social media.	Yes	No
The narrative is spreading on multiple platforms.	Yes	No
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.)	Yes	No
Multiple narratives/artifacts are converging into a single narrative or conspiracy.	Yes	No
AMPLIFICATION		
Multiple organizations across the sector are reporting similar narratives/artifacts.	Yes	No
The allegation is paired with media (pictures, video, audio) that is unverified or misrepresented, in an effort to provide “legitimacy” to the narrative.	Yes	No
There is an opportunity to amplify corrections initiated by social media platforms and/or traditional media.	Yes	No
CONSEQUENCES		
The narrative includes a call to arms* or other directions for action, whether in person or virtual.	Yes	No
The narrative/artifact focuses on upcoming major milestones or events where early fact-checking could proactively disrupt the spread.	Yes	No
The rumor could cause physical or reputational damage to the organization, community, country, or global society.	Yes	No

**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

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).

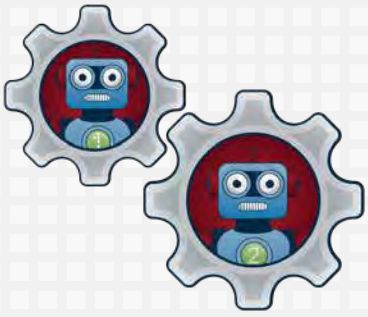
Repost Network
Coordinated Bots ("botnet") instantly repost content from a "parent" Bot.

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.

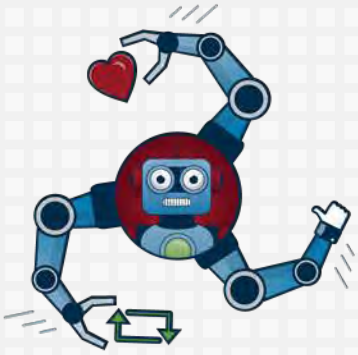
Raids
Bots swarm and overwhelm targeted accounts with spam.

Bots can be recognized by their interactions with each other and with real users. They often display:



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.

SOCIAL MEDIA BOTS

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.

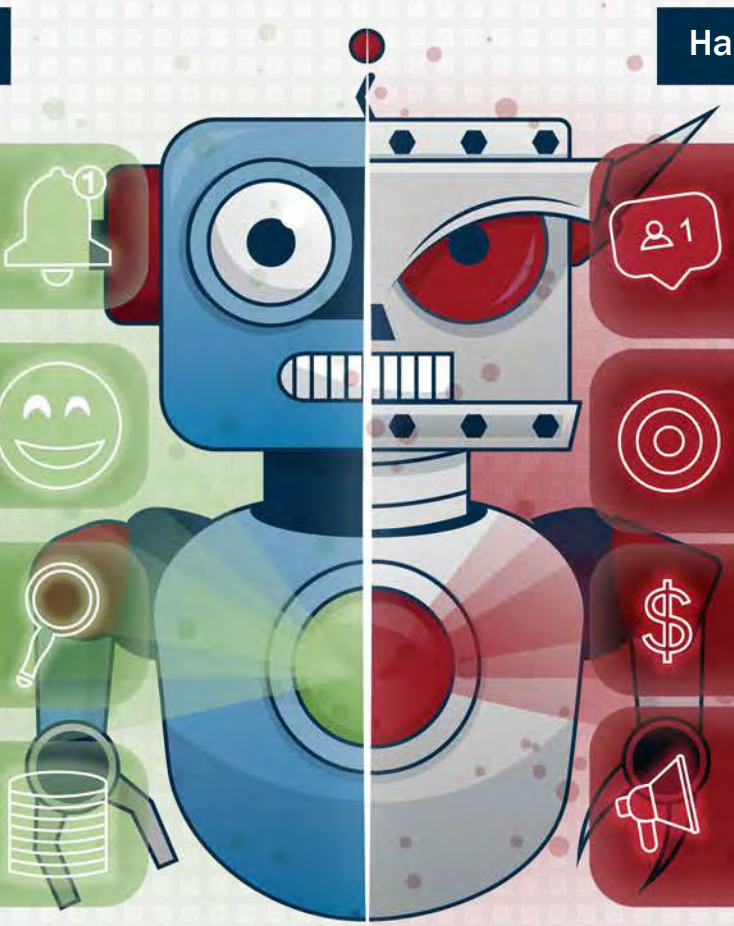
Helpful Bots support:

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.

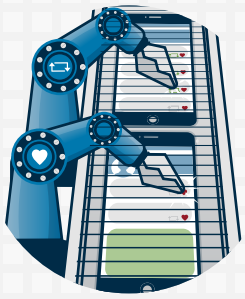
Trolls are human users, often with obscured identities, who seek to create division online. Bad actors may employ Bots in coordination with trolls.

SOCIAL MEDIA BOTS

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.

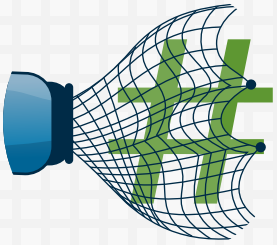


Click/Like Farming

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

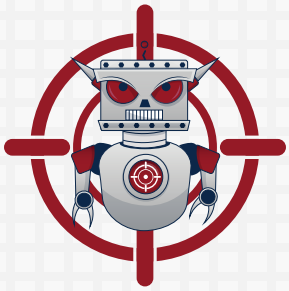
Astroturfing

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.



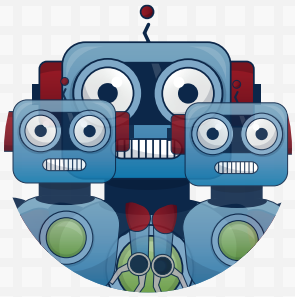
Hashtag Hijacking

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



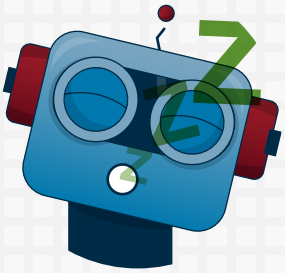
Raids

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



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.

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.

SOCIAL MEDIA BOTS

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.

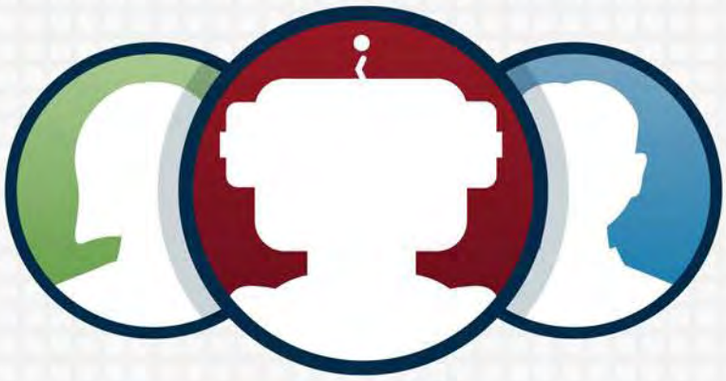
9. Erratic Behavior
Shares content about many unrelated topics or changes interests and behavior suddenly, such as randomly posting in a new language.

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

SOCIAL MEDIA BOTS*

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 varían 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).

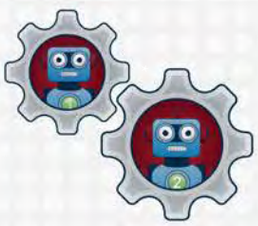
Red de reenvío de publicaciones [*Repost Network*] Los bots coordinados (*"botnet"*) publican nuevamente y de manera instantánea el contenido de un bot "principal".

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 auténticos 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*].

Los bots pueden ser reconocidos por sus interacciones entre sí y con usuarios reales. A menudo exhiben las siguientes características:

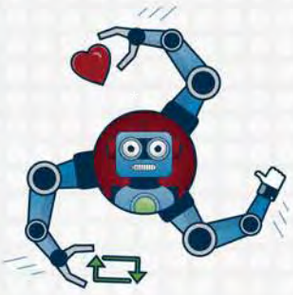


Acciones coordinadas

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.

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

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.

SOCIAL MEDIA BOTS*

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.

Los bots en redes sociales están cada vez más integrados en muchas de nuestras actividades en línea, incluso en ocasiones sin que nos demos cuenta. Hay una gran variedad de bots con funciones y capacidades distintas: Algunos ayudan a automatizar tareas simples, mientras otros bots más avanzados utilizan inteligencia artificial, análisis de big data y otros programas, para imitar a los usuarios humanos. Estos actores maliciosos a veces emplean bots como un componente de esfuerzos coordinados para manipular a los usuarios humanos.

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

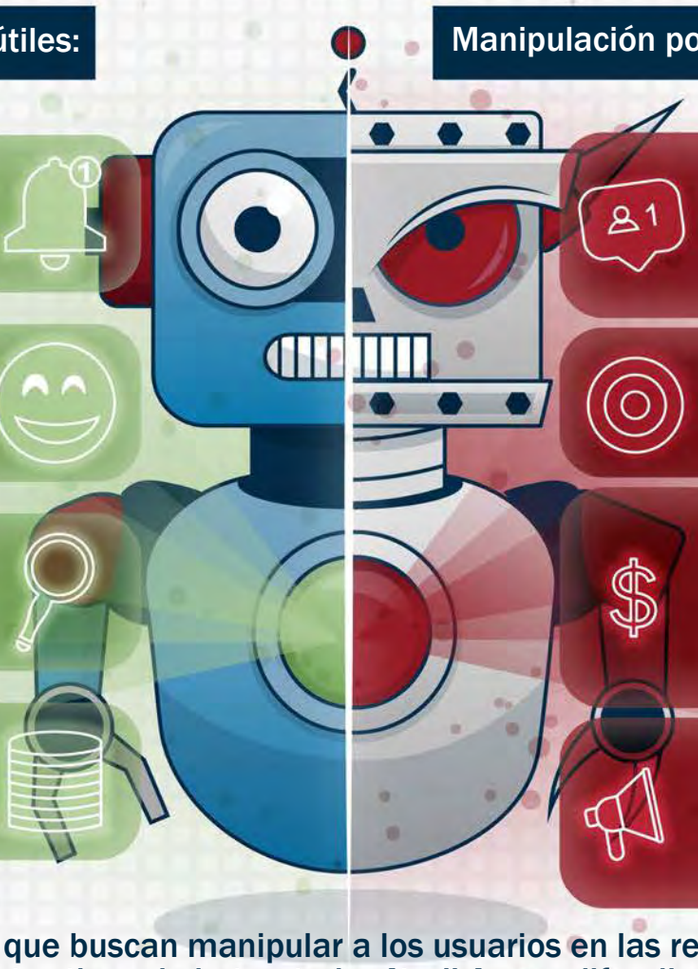
Apoyo por parte de bots útiles:

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
Amenazan o arruinan la reputación de cuentas especificas 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 manipular a los usuarios en las redes sociales a menudo emplean diferentes tipos de bots y troles [*trolls*] 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 cíborgs [*cyborgs*] son mejores para evadir detección.

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

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

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.

SOCIAL MEDIA BOTS*

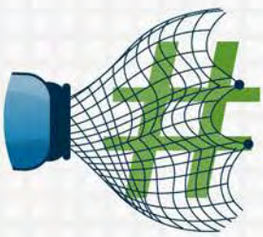
Los bots en redes sociales apoyan el comportamiento no auténtico y coordinado de los agentes criminales y amenazan nuestra capacidad para tener importantes debates democráticos. Visite CISA.gov/MDM para obtener más información

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.

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

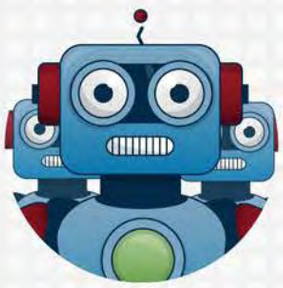
Obtención de clics o de reacción "Me gusta" [*Click/Like Farming*]

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.



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 maliciosos), silenciando opiniones opuestas, y desalentando la discusión abierta.



Red de reenvío de publicaciones [*Repost Network*]

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.

Bots inactivos o bots durmientes [*Sleepers*]

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.

Campañas artificiales [Operación de *'Astroturfing'*]

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.

Bombardeos o Asaltos [*Raids*]

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

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.

Erosionar la confianza en las instituciones manipulando discusiones orgánicas.

Influir en nuestras prioridades manipulando discusiones orgánicas.

Polarizarnos hacia posiciones más extremas que impiden un diálogo sano.

Reprimir la participación silenciando opiniones contrarias.

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

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.

SOCIAL MEDIA BOTS*

Aunque los bots en redes sociales intentan imitar a los usuarios humanos, algunas características pueden indicador 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, generado 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 divisivo 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 período 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 y 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.

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

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.

TOOLS OF DISINFORMATION:

Inauthentic Content

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.

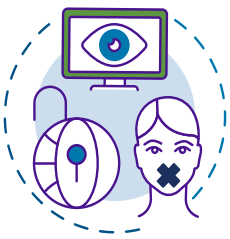
The quality of manipulated audio/video varies. Some fakes are detectable on closer examination, while uncovering others will require special software.

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.

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 engaña. Es información falsa que se comunica y propaga sin el intento de engañar.

Información Mala sabotea. Es información fáctual 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

Contendido de audio/video llama su atención, asi 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.

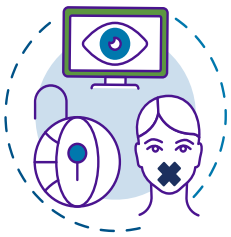
Por sí solo, este contenido puede ser convincente. Verifique con múltiples fuentes para confirmar su autenticidad.

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 confiable.

Pistas como errores ortográficos en un URL pueden indicar, incluso antes de visitar un sitio web, que puede no ser una fuente confiable.