COMPUTER SECURITY: Health Care Systems, Democracies and Social Networks

Roy Campbell

Week 3: Democracies and their computer security concerns.

Friday Feb 17 9:30-11:00am.

Osher Lifelong Learning Institute

Illinois Classroom

DEMOCRACY & CYBERSECURITY

PRESERVING DEMOCRATIC INSTITUTIONS

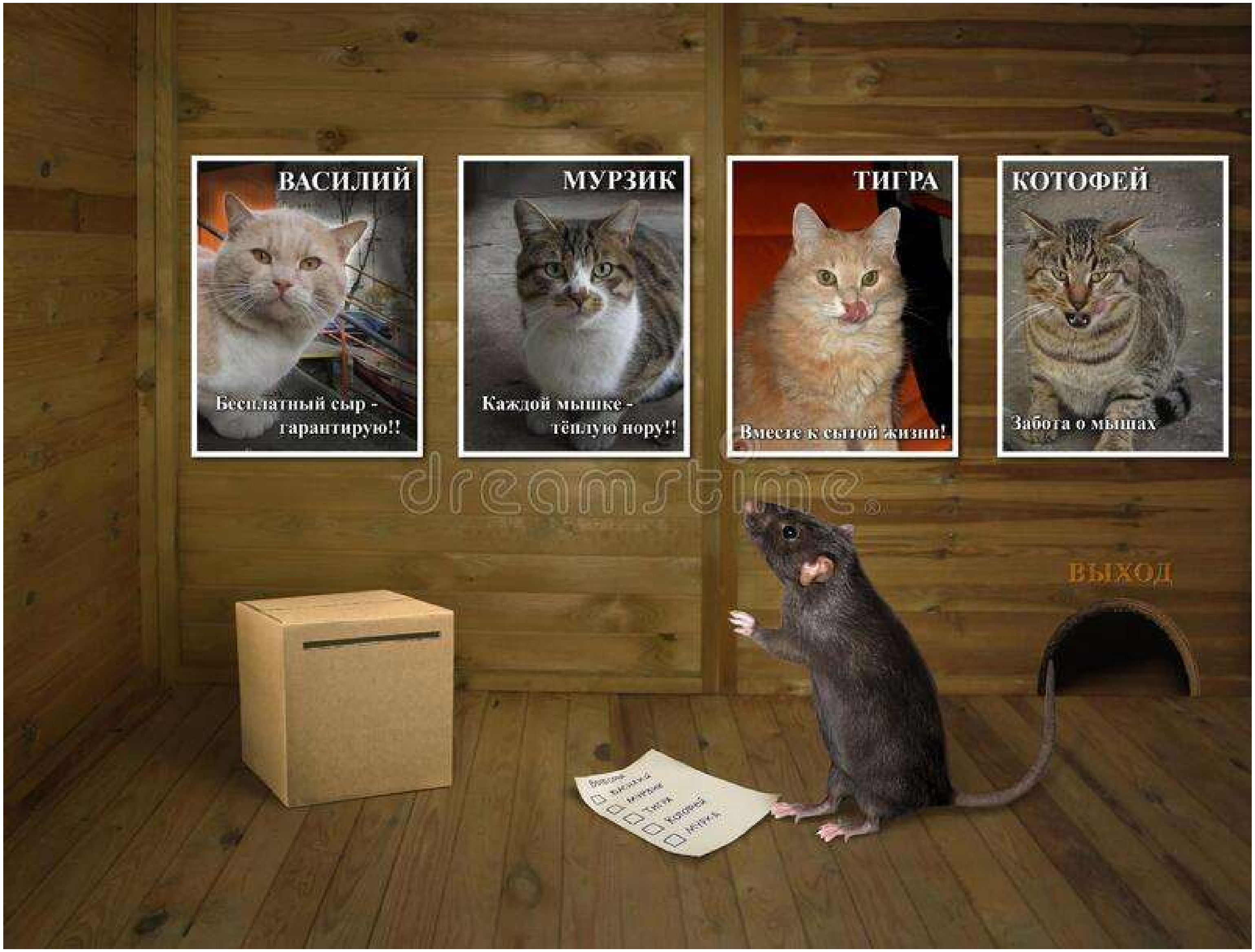
BALLO
BOX

CHATGDP: EXPLAIN SECURITY AND DEMOCRACY

- Security and democracy are two important concepts that are often discussed in relation to each other. While they can be seen as separate concepts, they are also closely interconnected in a variety of ways.
- Security refers to the protection of individuals and communities from harm, including physical harm, economic harm, and harm to personal freedoms and rights. In the context of national security, governments are responsible for protecting the safety and well-being of their citizens from external and internal threats, such as terrorism, crime, and cyber attacks.
- Democracy, on the other hand, refers to a system of government in which power is held by the people through free and fair elections, and where individuals are guaranteed certain political and civil rights, such as the right to free speech, the right to a fair trial, and the right to vote. Democracy values the participation and representation of citizens in the political decision-making process, and aims to ensure that the government serves the interests of the people.
- While security and democracy are both important, there can be tensions between the two. For example, efforts to enhance security may involve limiting civil liberties or infringing on privacy rights. On the other hand, efforts to protect democratic freedoms may make it more difficult to enforce security measures. Finding a balance between security and democracy can be challenging, but it is crucial to ensure that both are upheld in a society.

WEEK 3: COMPUTER SECURITY: DEMOCRACY

1. Dissemination and Disinformation
   - a) Dissemination, Disinformation and Conspiracy Theories
   - b) Advertising Bias
   - c) Fake news – Information Disorder
   - d) Pictures, Video and Audio
2. Democracy [27]
   - a) Voting process and voting machines, Voting systems, Governmen



ВАСИЛИЙ
Бесплатный сыр - гарантирую!!
МУРЗИК
Каждой мышке - тёплую нору!!
ТИГРА
Вместе к сытой жизни!
КОТОФЕЙ
Забота о мышах
ВЫХОД

dreamstime

WEEK 3: COMPUTER SECURITY: DEMOCRACY

1. **Dissemination and Disinformation**
   - a) **Dissemination, Disinformation and Conspiracy Theory**
   - b) **Advertising Bias**
   - c) **Fake news – Information Disorder**
   - d) **Pictures, Video and Audio**
2. Democracy [28]
   - a) Voting process, Voting machines, Voting systems

DEFINITIONS

Dissemination

- Broadcast a message to the public without direct feedback from the audience.

Disinformation

- False information which is intended to mislead, especially propaganda issued by a government organization to a rival power or the media

Conspiracy Theory

- A belief that a conspiracy has actually been decisive in producing a political event of which the theorists strongly disapprove
- Relying on the view that the universe is governed by design, and embody three principles: nothing happens by accident, nothing is as it seems, and everything is connected
- Evolves to incorporate whatever evidence exists against them, so that they become, as a closed system that is unfalsifiable, and therefore "a matter of faith rather than proof." Michael Barkin

TACTICS OF DISINFORMATION (CISA)

1. **Cultivate Fake or Misleading Personas and Websites**: Disinformation actors create networks of fake personas and websites to increase the believability of their message with their target audience. Fake expert networks use inauthentic credentials (e.g., fake "experts", journalists, think tanks, or academic institutions) to lend undue credibility to their influence content and make it more believable.

2. **Create Deepfakes and Synthetic Media:** Synthetic media content may include photos, videos, and audio clips that have been digitally manipulated or entirely fabricated to mislead the viewer. Artificial intelligence (AI) tools can make synthetic content nearly indistinguishable from real life. Synthetic media content may be deployed as part of disinformation campaigns to promote false information and manipulate audiences.

https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

TACTICS OF DISINFORMATION (CISA)

3. **Devise or Amplify Conspiracy Theories:** Conspiracy theories attempt to explain important events as secret plots by powerful actors. Conspiracy theories not only impact an individual's understanding of a particular topic; they can shape and influence their entire worldview. Disinformation actors capitalize on conspiracy theories by generating disinformation narratives that align with the conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience.

https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

TACTICS OF DISINFORMATION (CISA)

4. **Astroturfing and Flooding the Information Environment:** Disinformation campaigns will often post overwhelming amounts of content with the same or similar messaging from several inauthentic accounts. This practice, known as astroturfing, creates the impression of widespread grassroots support or opposition to a message, while concealing its true origin. A similar tactic, flooding, involves spamming social media posts and comment sections with the intention of shaping a narrative or drowning out opposing viewpoints.

https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

TACTICS OF DISINFORMATION (CISA)

5. **Abuse Alternative Platforms:** Disinformation actors may abuse alternative social media platforms to intensify belief in a disinformation narrative among specific user groups. Disinformation actors may seek to take advantage of platforms with fewer user protections, less stringent content moderation policies, and fewer controls to detect and remove inauthentic content and accounts than other social media platforms.

6. **Exploit Information Gaps:** Data voids, or information gaps, occur when there is insufficient credible information to satisfy a search inquiry. Disinformation actors can exploit these gaps by generating their own influence content and seeding the search term on social media to encourage people to look it up. This increases the likelihood that audiences will encounter disinformation content without any accurate or authoritative search results to refute it.

TACTICS OF DISINFORMATION (CISA)

7. **Manipulate Unsuspecting Actors:** Disinformation actors target prominent individuals and organizations to help amplify their narratives. Targets are often unaware that they are repeating a disinformation actor's narrative or that the narrative is intended to manipulate.

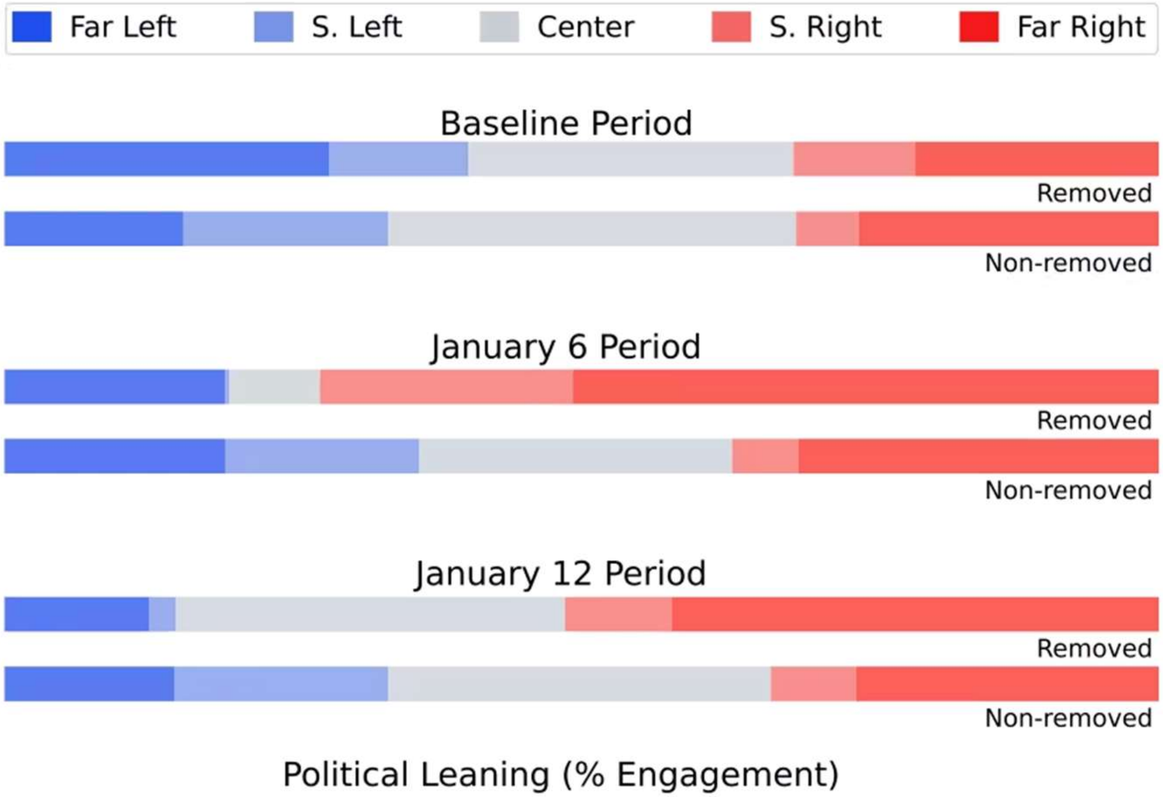
8. **Spread Targeted Content:** Disinformation actors produce tailored influence content likely to resonate with a specific audience based on their worldview and interests. These actors gain insider status and grow an online following that can make future manipulation efforts more successful. This tactic often takes a "long game" approach of spreading targeted content over time to build trust and credibility with the target audience.

MEDIA REACTION TO DISINFORMATION

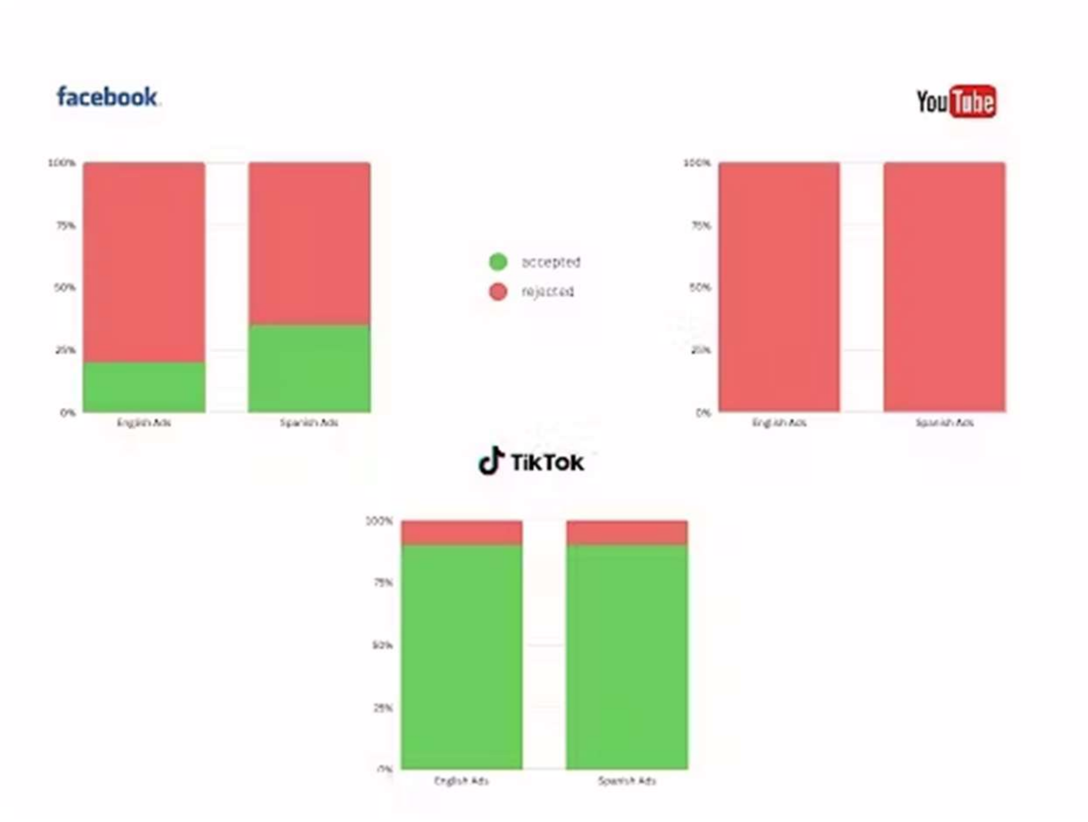
- In the afternoon of January 6, 2021, Facebook leadership announced they were "appalled by the violence at the Capitol today," and were approaching the situation "as an emergency." Facebook staff were searching for and taking down problematic content, such as posts praising the storming of the U.S. Capitol, calls to bring weapons to protests, and encouragement about the day's events. At the same time, Facebook announced it would block then-President Donald Trump's account – a decision the company is now, two years later, considering reversing

https://cybersecurityfordemocracy.org/facebook-capitol-riot-2021-misinfo

ENGAGEMENT WITH REMOVED AND NON-REMOVED POSTS FROM U.S. NEWS PAGES BY PARTISANSHIP FOR THE BASELINE, JANUARY 6, AND JANUARY 12 PERIODS, RESPECTIVELY.



TIKTOK AND FACEBOOK FAIL TO DETECT ELECTION DISINFORMATION IN THE U.S., WHILE YOUTUBE SUCCEEDS



WORLD HEALTH STUDY OF MIS/DISINFORMATION DURING COVID

- 1. Assess the source
  - https://support.google.com/websearch/answer/1325808
  - https://tineye.com/
  - https://citizenevidence.amnestyusa.org/
- 2. Go beyond headlines
- 3. Identify the author
- 4. Check the date
- 5. Examine the supporting evidence
- 6. Check your biases
- 7. Turn to fact-checkers

https://www.who.int/news-room/spotlight/let-s-flatten-the-infodemic-curve

REACTION TIME

- By the time harmful content posted to Facebook during the Capitol riot period came down, millions had already engaged
- Time is important for other reasons ----

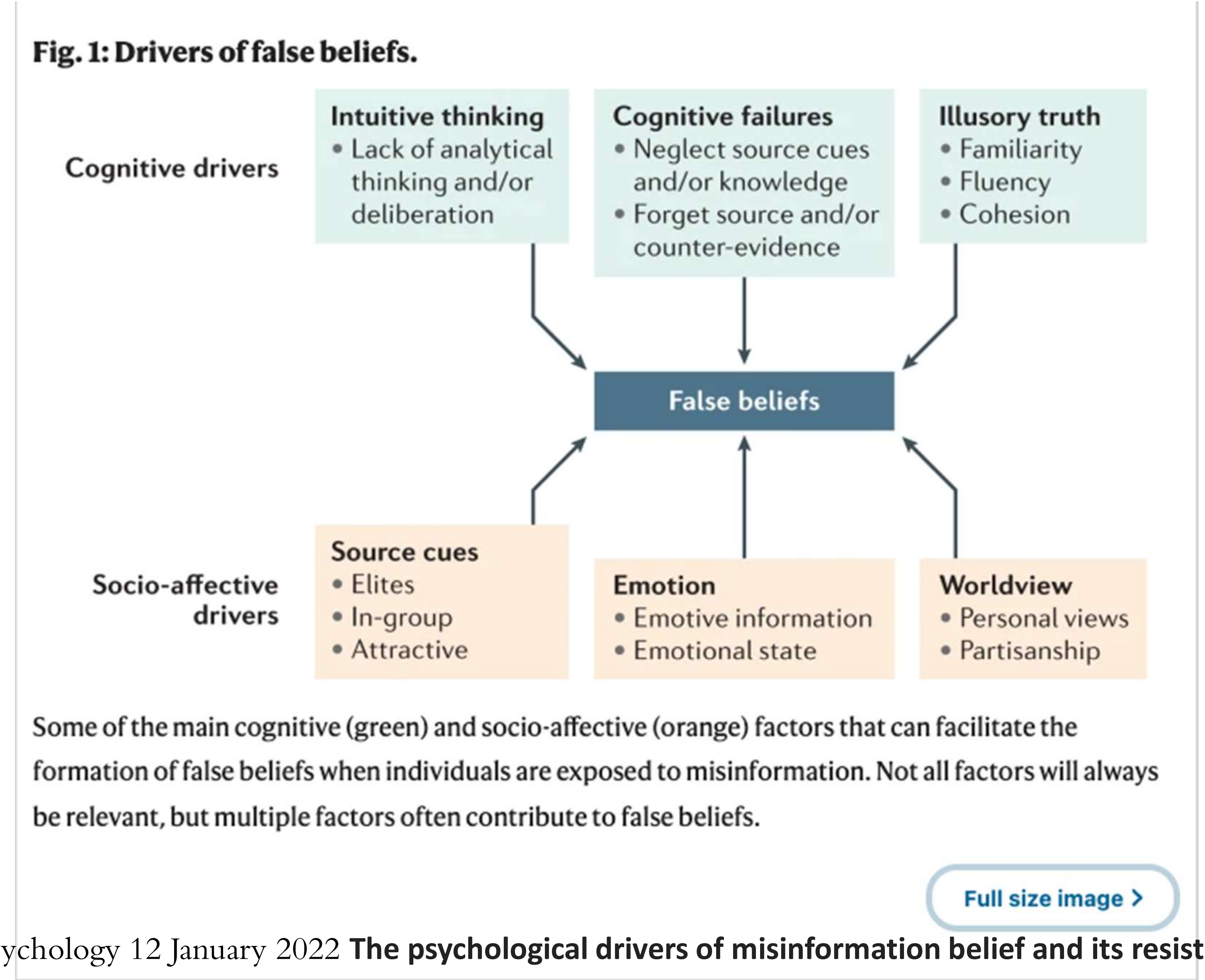


Fig. 1: Drivers of false beliefs.

Cognitive drivers

Intuitive thinking
- Lack of analytical thinking and/or deliberation

Cognitive failures
- Neglect source cues and/or knowledge
- Forget source and/or counter-evidence

Illusory truth
- Familiarity
- Fluency
- Cohesion

False beliefs

Socio-affective drivers

Source cues
- Elites
- In-group
- Attractive

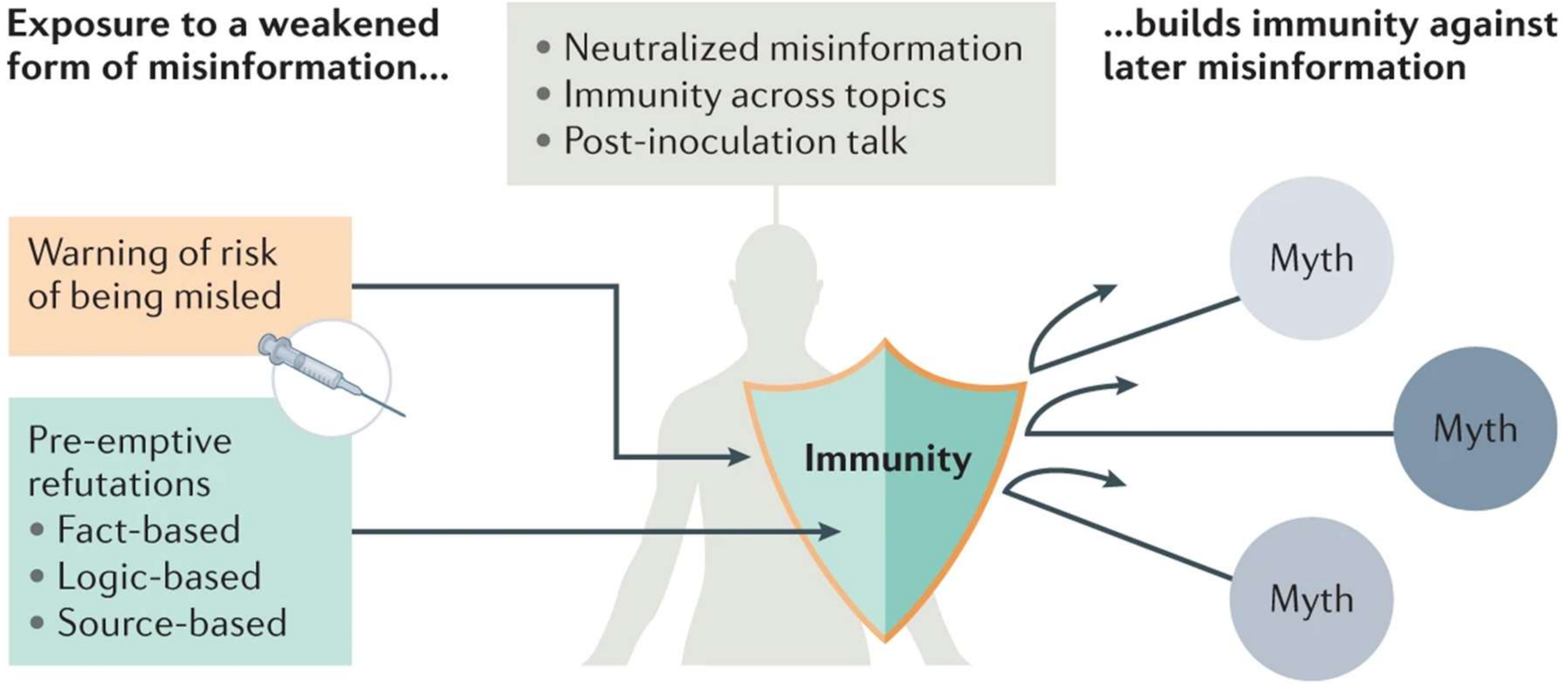
Emotion
- Emotive information
- Emotional state

Worldview
- Personal views
- Partisanship

Some of the main cognitive (green) and socio-affective (orange) factors that can facilitate the formation of false beliefs when individuals are exposed to misinformation. Not all factors will always be relevant, but multiple factors often contribute to false beliefs.

Nature Reviews Psychology 12 January 2022 **The psychological drivers of misinformation belief and its resistance to correction**

IMMUNIZATION



Exposure to a weakened form of misinformation...

- Neutralized misinformation
- Immunity across topics
- Post-inoculation talk

...builds immunity against later misinformation

Warning of risk of being misled

Pre-emptive refutations
- Fact-based
- Logic-based
- Source-based

Immunity

Myth

Myth

Myth

ADVERTISING BIAS

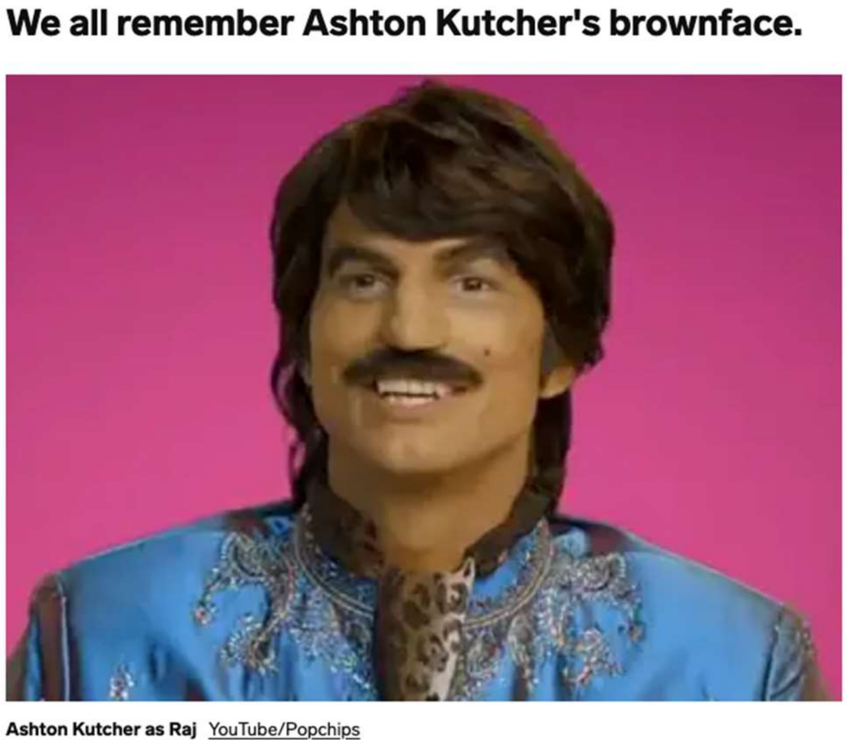
- Unconscious bias (Stereotypes)

  Racial bias (black or White – MRI study Stanford)

  Gender bias (political leaders favor men)

  Ageism (55 or older)
- Statistical bias (choice of group)
- Cognitive bias (mental shortcuts)
  - Confirmative Bias (preexisting beliefs)
  - Exposure Bias (people like product they are more often exposed to)
- Systemic bias (organizational policies, laws, or practices that cause discriminatory effects against particular social groups)

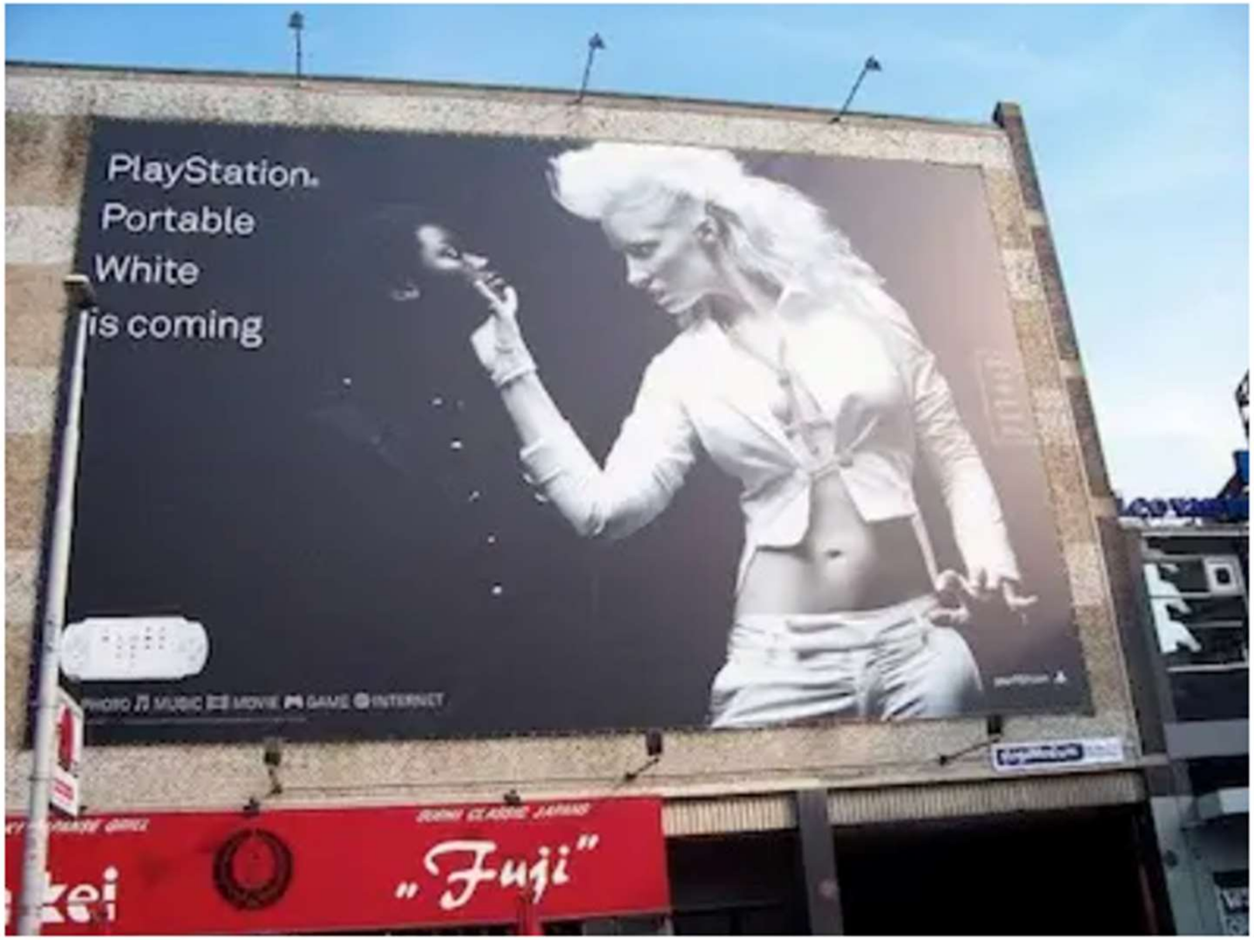
https://www.ibm.com/watson-advertising/thought-leadership/bias-in-advertising



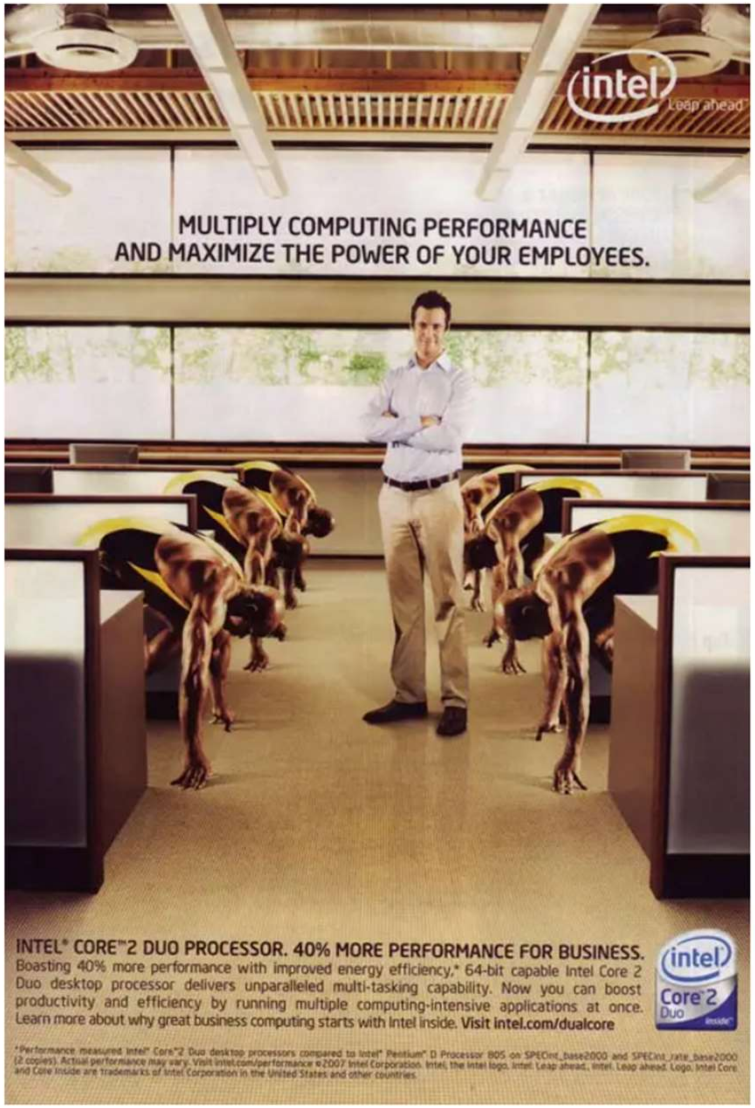
We all remember Ashton Kutcher's brownface.

Ashton Kutcher as Raj YouTube/Popchips

This PSP billboard wasn't widely published.



Intel released an ad they knew was racist.



intel
Leap ahead

MULTIPLY COMPUTING PERFORMANCE
AND MAXIMIZE THE POWER OF YOUR EMPLOYEES.

INTEL® CORE™2 DUO PROCESSOR. 40% MORE PERFORMANCE FOR BUSINESS.
Boasting 40% more performance with improved energy efficiency,* 64-bit capable Intel Core 2 Duo desktop processor delivers unparalleled multi-tasking capability. Now you can boost productivity and efficiency by running multiple computing-intensive applications at once. Learn more about why great business computing starts with Intel inside. **Visit intel.com/dualcore**

*Performance measured Intel® Core™2 Duo desktop processors compared to Intel® Pentium® D Processor 805 on SPECint_base2000 and SPECint_rate_base2000 (2 copies). Actual performance may vary. Visit intel.com/performance ©2007 Intel Corporation. Intel, the Intel logo, Intel. Leap ahead., Intel. Leap ahead. Logo, Intel Core and Core Inside are trademarks of Intel Corporation in the United States and other countries.

CONSPIRACY THEORY

- EXPLOITING
- The desire for understanding and certainty
- The desire for control and security
- The desire to maintain a positive self-image

MEDICAL DIAGNOSIS, STATISTICS AND MISCOMMUNICATION

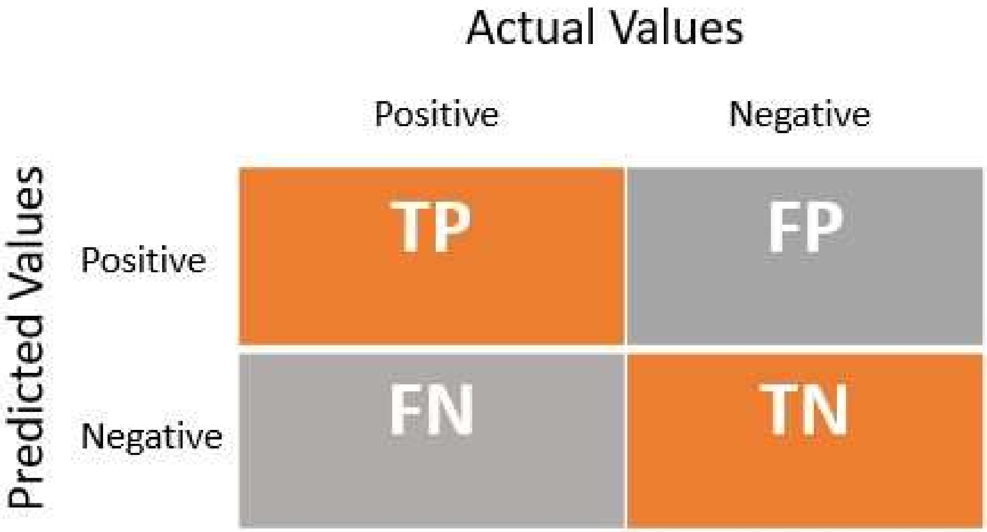
- *Sensitivity* and *specificity* describe the accuracy of a test which reports the presence or absence of a condition.

  If individuals who have the condition are considered "positive" and those who don't are considered "negative", then

  sensitivity is a measure of how well a test can identify true positives and specificity is a measure of how well a test can identify true negatives.

- a positive result in a test with high sensitivity is not necessarily useful for "ruling in" disease. Suppose a 'bogus' test kit is designed to always give a positive reading. When used on diseased patients, all patients test positive, giving the test 100% sensitivity. However, sensitivity does not take into account false positives. The bogus test also returns positive on all healthy patients, giving it a false positive rate of 100%, rendering it useless for detecting or "ruling in" the disease.

CLASSIFICATION PROBLEM: RELATION BETWEEN SENSITIVITY, SPECIFICITY AND ACCURACY



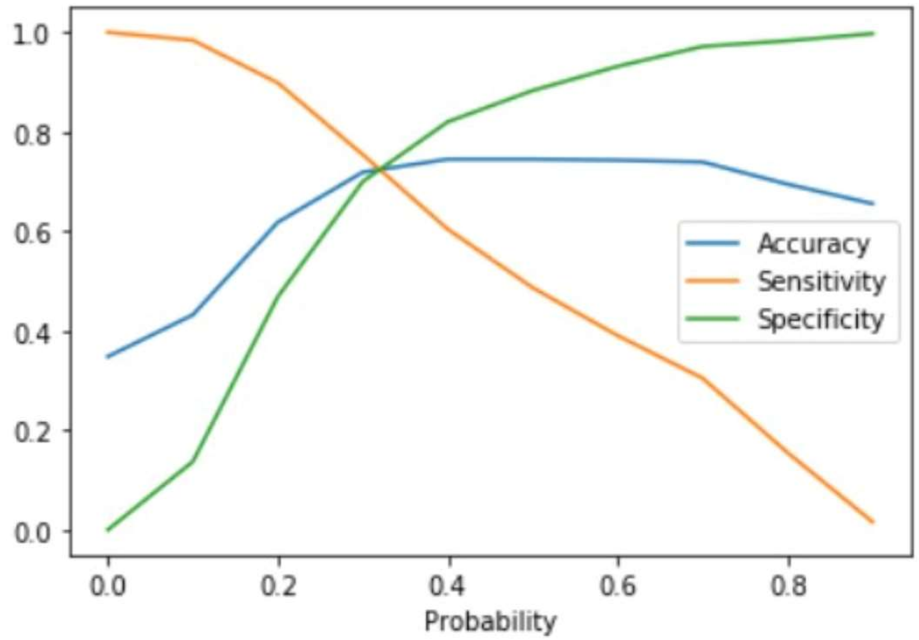
Predicted Values \ Actual Values	Positive	Negative
Positive	TP	FP
Negative	FN	TN

Figure 1

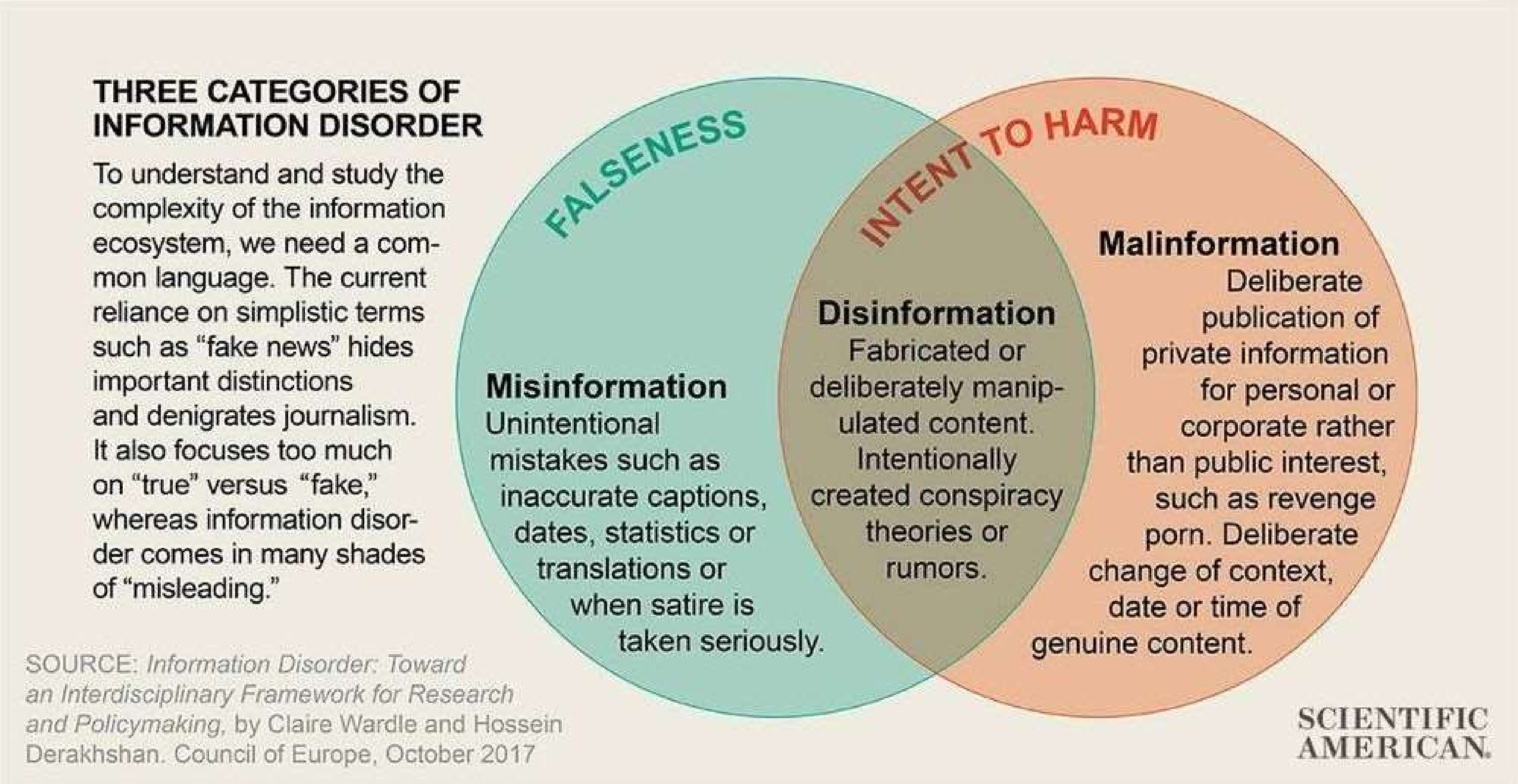
TP = True Positive
TN = True Negative
FP = False Positive
FN = False Negative

RELATIONSHIP BETWEEN ACCURACY AND SENSITIVITY AND SPECIFICITY

- Accuracy $= \dfrac{TP+\ TN}{TP+FP+FN+TN}$
- Sensitivity $= \dfrac{TP}{TP+FN}$
- Specificity $= \dfrac{TN}{TN+FP}$



INFORMATION DISORDER



THREE CATEGORIES OF INFORMATION DISORDER

To understand and study the complexity of the information ecosystem, we need a common language. The current reliance on simplistic terms such as "fake news" hides important distinctions and denigrates journalism. It also focuses too much on "true" versus "fake," whereas information disorder comes in many shades of "misleading."

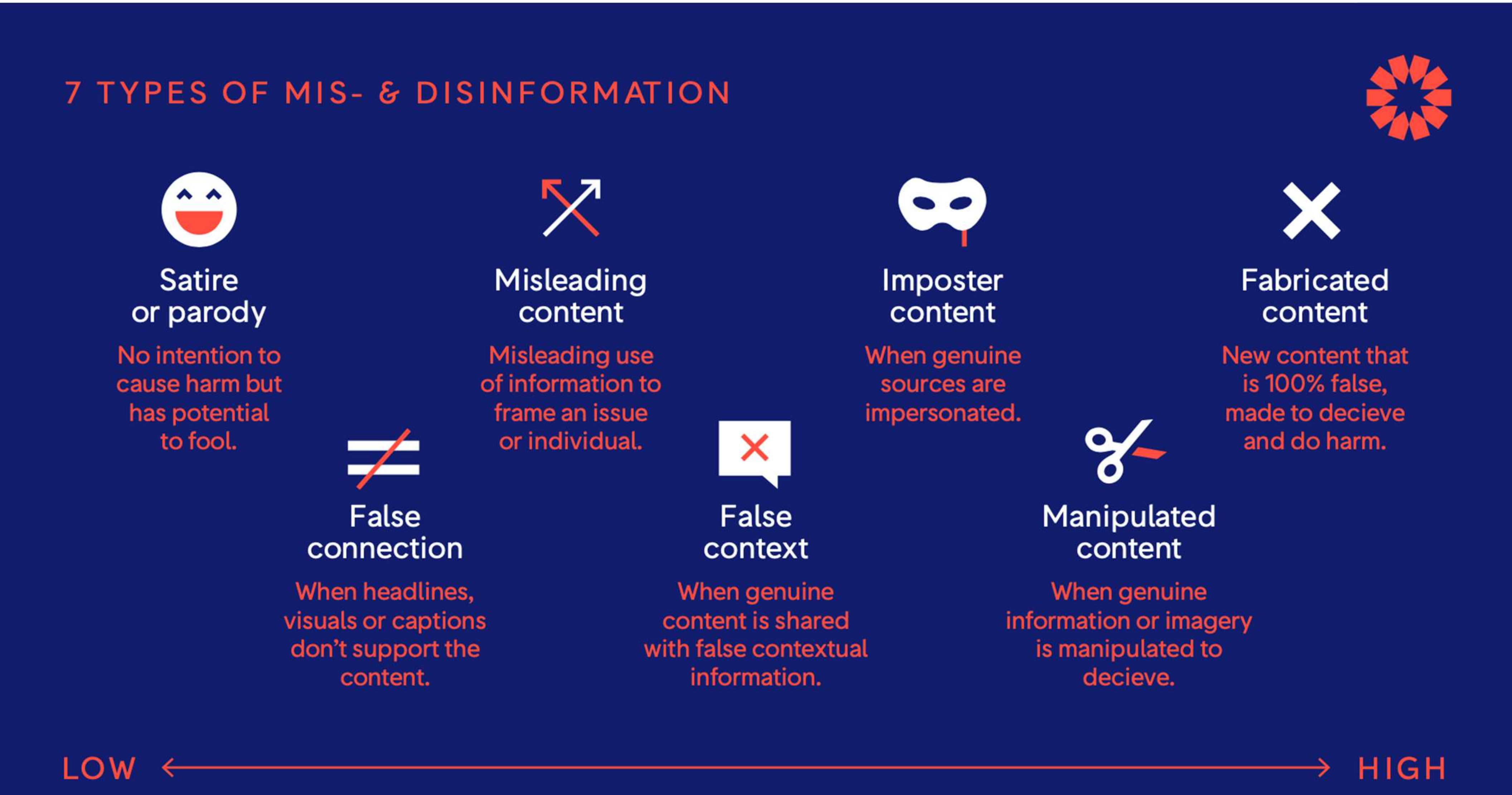
Misinformation Unintentional mistakes such as inaccurate captions, dates, statistics or translations or when satire is taken seriously.

Disinformation Fabricated or deliberately manipulated content. Intentionally created conspiracy theories or rumors.

Malinformation Deliberate publication of private information for personal or corporate rather than public interest, such as revenge porn. Deliberate change of context, date or time of genuine content.

SOURCE: *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*, by Claire Wardle and Hossein Derakhshan. Council of Europe, October 2017

SCIENTIFIC AMERICAN.



7 TYPES OF MIS- & DISINFORMATION

Satire or parody
No intention to cause harm but has potential to fool.

False connection
When headlines, visuals or captions don't support the content.

Misleading content
Misleading use of information to frame an issue or individual.

False context
When genuine content is shared with false contextual information.

Imposter content
When genuine sources are impersonated.

Manipulated content
When genuine information or imagery is manipulated to decieve.

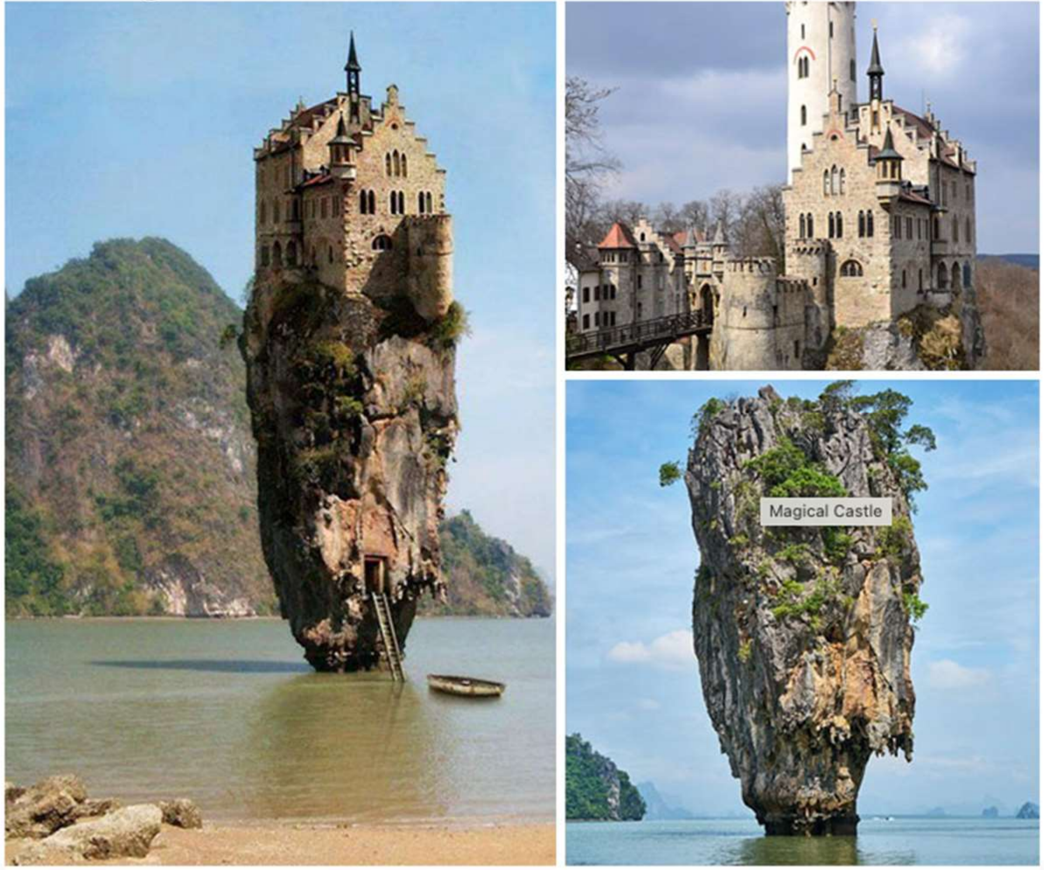
Fabricated content
New content that is 100% false, made to decieve and do harm.

LOW ⟷ HIGH

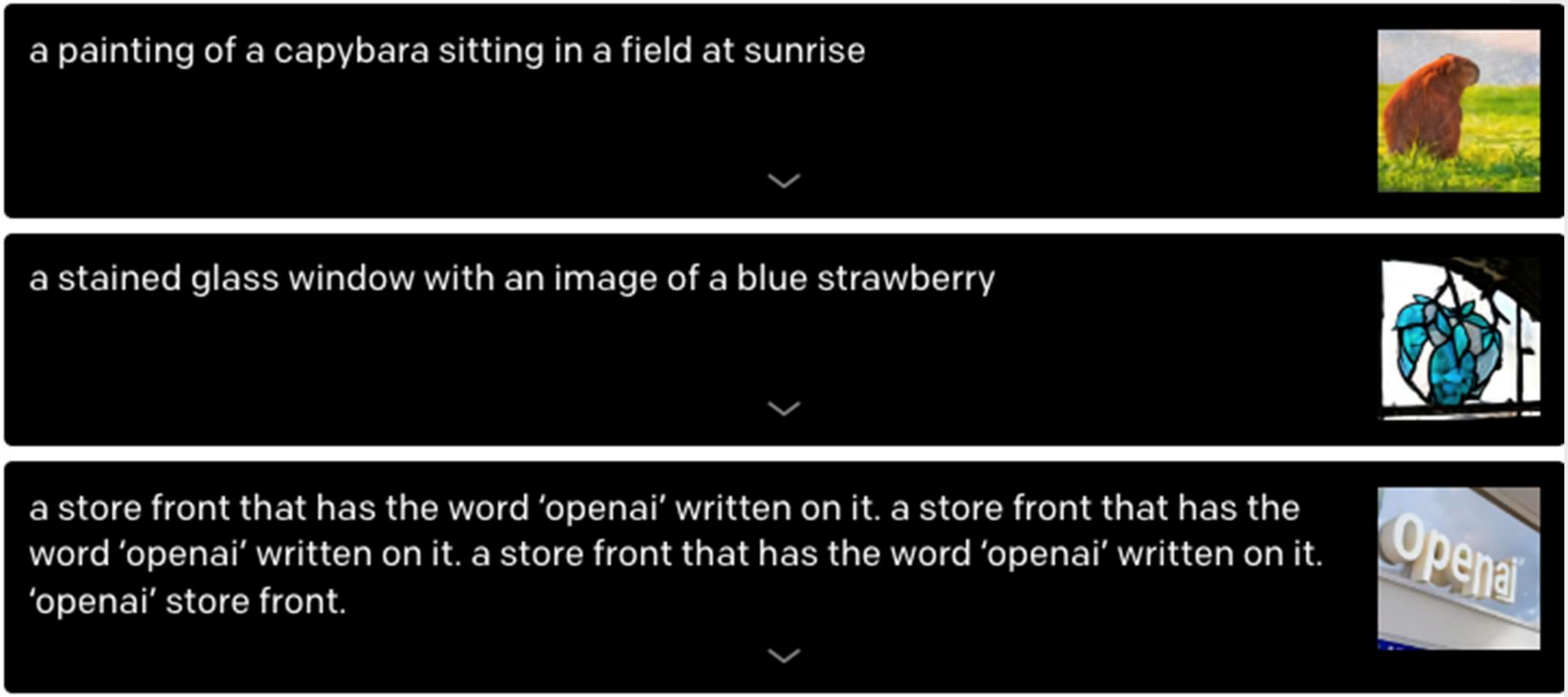
https://firstdraftnews.org/long-form-article/understanding-information-disorder/

PICTURES, VIDEO AND AUDIO

#5 Magical Castle



PICTURES, VIDEO AND AUDIO: DALL·E



a painting of a capybara sitting in a field at sunrise

a stained glass window with an image of a blue strawberry

a store front that has the word ‘openai’ written on it. a store front that has the word ‘openai’ written on it. a store front that has the word ‘openai’ written on it. ‘openai’ store front.

CISA AND ELECTIONS

- Securing our nation's election infrastructure requires true partnership. CISA has been working with state and local election oficials to be sure they have access to the resources, tools, capabilities, and information they need to build resilience against all threats. CISA worked with all 50 states, the District of Columbia, and the U.S. territories to secure the 2022 election. This work included hundreds of election infrastructure security assessments and cybersecurity vulnerability scanning in hundreds of jurisdictions.

https://www.cisa.gov/sites/default/files/publications/CISA-YearInReview_v1_508.pdf

https://www.cisecurity.org/ei-isac

TRUST AND GOVERNMENT WEB SITES

- Election websites can use the .gov top-level domain (TLD) for free.
- .gov is only available to federal, state, and local government entities verified by the U.S. Cybersecurity and Infrastructure Security Agency (CISA).
- The Center for Democracy and Technology found that, of the 7,010 websites that they included for analysis (websites of county- and municipality-level election officials), only 1,747 (25%) used .gov.
- Of the 7,010 county or municipalitywebsites that CDT analyzed, 6,260 (89%) supported HTTPS.

CDT EXAMPLE” POOR DOMAIN CHOICE FOR ELECTION WEBSITE

- As an example, the official election website in Harris County, TX (home to nearly 5 million residents), is harrisvotes.com. A bad actor could register, say, harriselections.com and use it to spread false information about voting options, to collect private voter information, or to publish false results.
- Look no further than Champaign County for ignoring use of .gov domain
- https://champaigncountyclerk.com/elections

“CHAMPAIGN COUNTY, Ill. (WCIA) — The Champaign County Clerk’s office had to work around few issues that came up on election night.

The website went down, but it was back up and running as of 7:30 a.m. Wednesday, after being down for around 12 hours.”

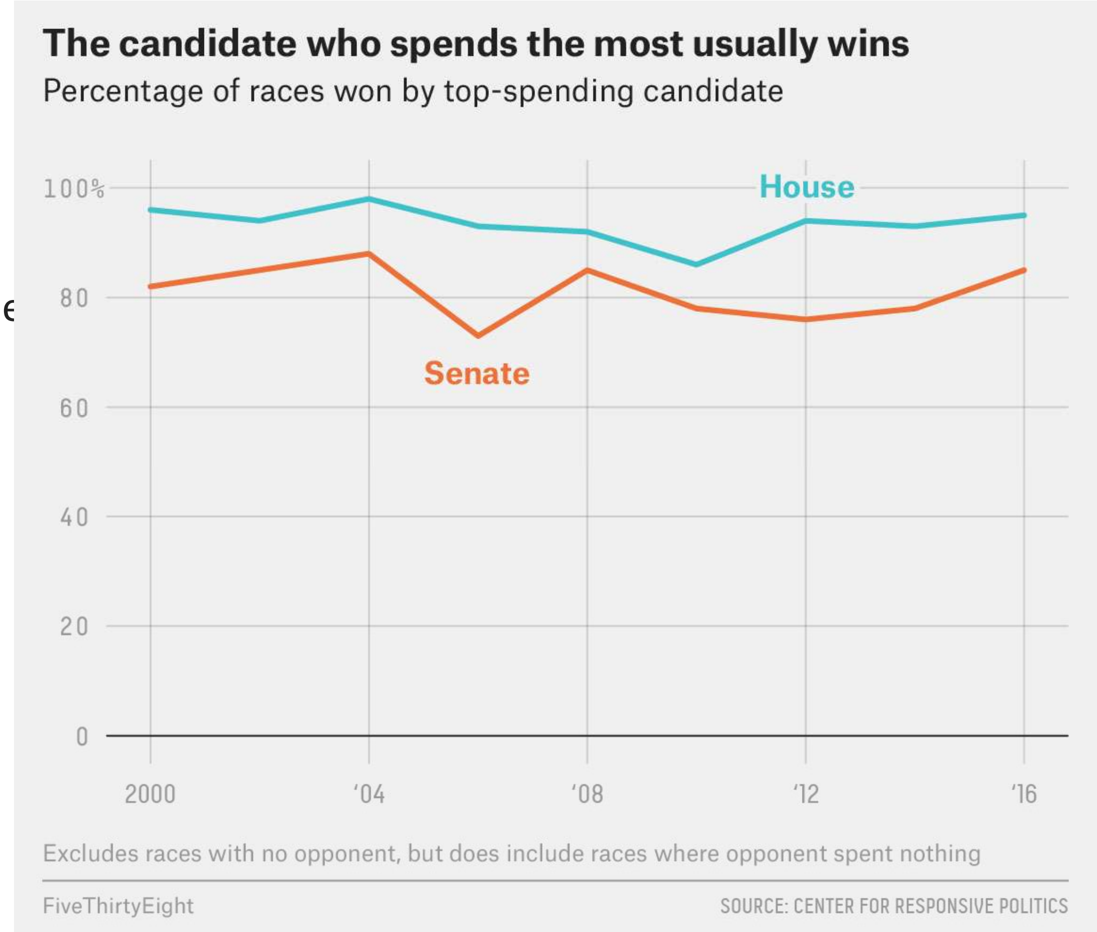
https://www.wcia.com/news/your-local-election-hq/champaign-county-clerks-website-unofficial-election-results-back-online/

2. DEMOCRACY

Election Security
Voting process
Voting machines
Voting systems
Government

ELECTIONS ARE BIG MONEY

- The



The candidate who spends the most usually wins

Percentage of races won by top-spending candidate

Excludes races with no opponent, but does include races where opponent spent nothing

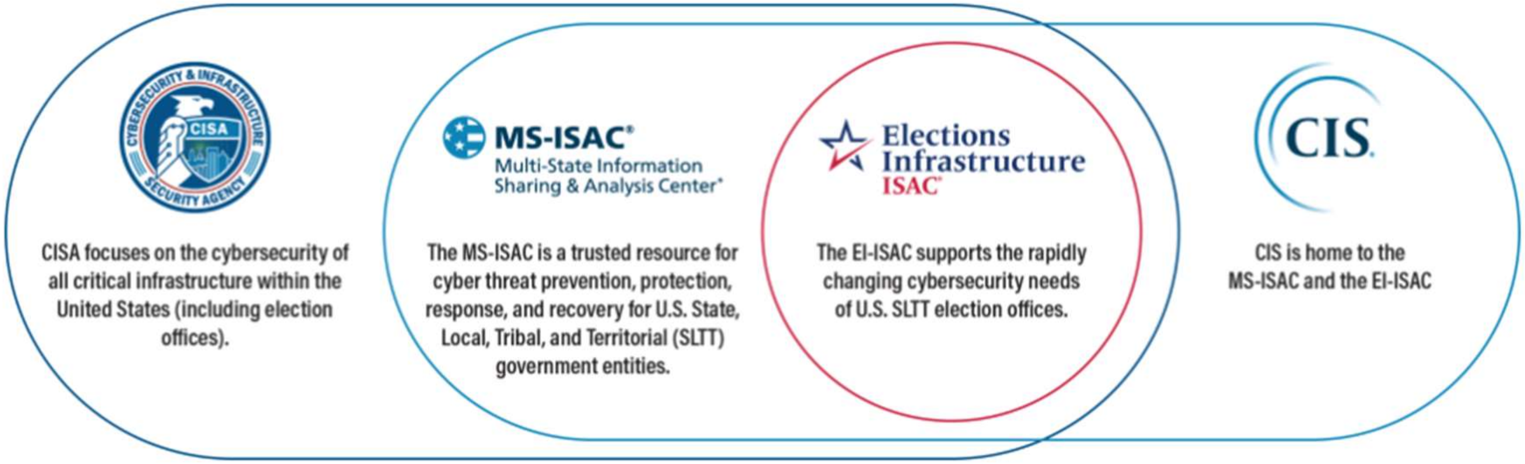
FiveThirtyEight

SOURCE: CENTER FOR RESPONSIVE POLITICS

https://fivethirtyeight.com/features/money-and-elections-a-complicated-love-story/

**Advertising —
even negative advertising
— isn't very effective**

GOVERNMENT SUPPORT FOR ELECTION CYBERSECURITY


CISA
MS-ISAC
Multi-State Information Sharing & Analysis Center
Elections Infrastructure ISAC
CIS

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CIS is home to the MS-ISAC and the EI-ISAC

MAJOR CYBERSECURITY CONCERNS IN VOTING

- **Voter information:** Cyber threat actors may try to compromise or manipulate electronic poll books and voter registration databases in attempt to cause confusion or delay voting.
- **Websites:** Cyber threat actors often target state and local websites with DDoS, phishing, and defacement.
- **Email systems:** Cyber threat actors use phishing as the preferred vector with which to target state and local email systems.
- **Networks:** Cyber threat actors commonly use vectors, such as phishing or malware, in their attempts to infiltrate state and local networks that election offices rely on for regular business functions

https://www.cisa.gov/cybersecurity-toolkit-protect-elections

UNDERSTAND PHISHING ATTACKS.

- Phishing attacks use

1. email,
2. text messaging,
3. social media,
4. and/or malicious websites
5. to solicit personal information or to trick individuals into downloading malicious software.

- Cyber threat actors often use elections and political events to capture attention and lure recipients into clicking a link or downloading a file that contains malicious code.
- Election officials are often required to open email attachments, which could contain malicious payloads, to facilitate election administration processes (e.g., absentee ballot applications).

PROTECT AGAINST PHISHING ATTACKS

Product Link	**Description**
Election Security Risk in Focus: Phishing	CISA’s free training on phishing details phishing types, detection, and impacts with an emphasis on election infrastructure-related risks and available resources.
Cisco OpenDNS Home	OpenDNS blocks phishing websites that try to steal a user/organization identity and login information by pretending to be a legitimate website.
Cloudflare DNS resolver with malware filter	Cloudflare DNS resolver with malware filter is a private and fast DNS resolver that prevents user/organization devices from accessing known malware threats. For example, if an employee opens and clicks on a phishing email link, the link in the email won’t work. This prevents attackers from compromising sensitive internal information.

PROTECT AGAINST PHISHING ATTACKS

Product Link	Description
Quad9	Quad9's DNS platform is designed to prevent computers and devices from connecting to malware or phishing sites.
Google Advanced Protection Program	The Google Advanced Protection Program safeguards users with high visibility and sensitive information from targeted online attacks. New protections are automatically added to defend against today's wide range of threats.
Google Web Risk	Google Web Risk is a User Protection Service from Google Cloud designed to reduce the risk of threats targeting user-generated content. Google Web Risk lets organizations compare URLs in their environment against a repository of more than one million unsafe URLs.
Secureworks PhishInSuits	The Secureworks Adversary Group and Counter Threat Unit research team developed the PhishInSuits tool to conduct security assessments and test control frameworks against scenarios such as business email compromise (BEC) attacks. The tool combines this variation of illicit consent attack with text message (SMS)-based phishing (smishing) to emulate BEC campaigns and includes automated data-exfiltration capabilities.

DETECT PHISHING ATTEMPTS.

Product Link	Description
Google Safe Browsing	This toolset identifies known phishing and malware across the web and helps notify users and website owners of potential harm. It is integrated into many major products and provides tools to webmasters.
CrowdStrike Hybrid Analysis	This tool is a free malware analysis service that detects and analyzes unknown threats using a unique Hybrid Analysis technology. Users can submit suspicious URLs and receive aggregated malicious verdicts as well as the contents at said URL. Hybrid Analysis is also a file sandbox and free alternative to other public malware repositories for file/threat hunting.
Google VirusTotal	VirusTotal inspects items with more than 70 antivirus scanners and URL/domain blocklisting services, in addition to a variety of other tools, to extract signals from the studied content. Users can select a file from a computer via the browser and send it to VirusTotal. Submissions may be scripted in any programming language using the HTTP-based public application programming interface (API).

POLITICAL LOBBYING WITH CHATGPT

- artificial intelligence replacing humans in the democratic processes -- not through voting, but through lobbying (Bruce Schneier)
- automatically compose comments submitted in regulatory processes.
- write letters to the editor for publication in local newspapers.
- comment on news articles, blog entries and social media posts millions of times every day.
- mimic the work that the Russian Internet Research Agency did in its attempt to influence our 2016 elections, but without the agency’s reported multimillion-dollar budget and hundreds of employees.
- AI could provide techniques for precision targeting of lobbying:
- target undecided representatives sitting on committees controlling the policy of interest and then
- focus resources on members of the majority party when a bill moves toward a floor vote

UNDERSTAND RANSOMWARE ATTACKS

- Ransomware is malicious software designed to deny access to computer systems or data.
- In a ransomware attack, the ransomware actor

1. Encrypts systems and/or data, rendering them inaccessible to owners and users.
2. In some cases, data is also taken (exfiltrated) from the user's computer or network.
3. The actor demands payment to decrypt the systems and/or data.
4. However, paying this ransom does not guarantee the user will regain access to their systems and/or data; these assets can be permanently lost or leaked.

- For elections, a ransomware attack could leak or deny access to voter registration data, unofficial results reporting, and other sensitive information. It could also inhibit access to important election systems during critical operational periods, such as registration and candidate filing deadlines.

PROTECT AGAINST RANSOMWARE ATTACKS.

Product Link	Description
CISA Free Ransomware Services	CISA offers free services and training to protect organizations against ransomware.
Microsoft controlled folder access/ransomware protection in Windows	Controlled folder access in Windows helps protect against threats like ransomware by safeguarding folders, files, and memory areas on the device from unauthorized changes by unfriendly applications.
Microsoft Windows Backup and Restore	This tool sets up automatic backups of Windows 10 and 11 operating systems to an external drive or network location.

PROTECT AGAINST RANSOMWARE ATTACKS.

Product Link	**Description**
Zscaler’s Ransomware Risk Assessment	This service assesses an organization’s ability to counteract a ransomware infection and its spread, as well as an organization’s ability to resume operations after an infection. This web-based tool scans defenses against ransomware-specific intrusion, lateral movement, and exfiltration methods. It is safe to use and runs within the browser.
Cisco Immunet Antivirus	Immunet is a malware and antivirus protection system for Windows that utilizes cloud computing to provide enhanced community-based security.
Google Drive for desktop	This tool backs up files on Windows or Mac computers. Note: It does not allow users to restore their system; it only saves copies of files.

PROTECT AGAINST RANSOMWARE ATTACKS.

Product Link	**Description**
Google Chrome OS and Chromebooks	Chrome OS is a cloud-first platform that provides protection against ransomware by default through built-in proactive security measures such as safe browsing practices, blocking executables, and automatic data and file backups.
Microsoft Defender Antivirus in Windows	Built into Windows 10 and 11 and in versions of Windows Server, this tool is used to protect and detect endpoint threats, including file-based and fileless malware.
Cisco ClamAV	ClamAV is an open-source (general public license [GPL]) antivirus engine used in a variety of situations, including email and web scanning and endpoint security. It provides many utilities for users, including a flexible and scalable multithreaded daemon, a command-line scanner, and an advanced tool for automatic database updates.

DETECT RANSOMWARE ATTACKS.

Product Link	**Description**
Google Security Command Center	This tool helps users strengthen their security posture by evaluating their security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and mitigating and remediating risks.
Microsoft Safety Scanner	Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers. It can run scans to find malware and try to reverse changes made by identified threats.
AWS GitHub Security Assessment Tool	An AWS tool to help users create a point in time assessment of their AWS account using Prowler and Scout as well as optional AWS developed ransomware checks.

DETECT RANSOMWARE ATTACKS.

Product Link	Description
Cisco Snort	This network intrusion detection and prevention system conducts traffic analysis and packet logging on Internet Protocol (IP) networks. Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior. Snort uses a flexible rule-based language to describe traffic that it should collect or pass, and a modular detection engine. The related free Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort alerts.
Mandiant Red Team and Investigative Tools	These tools are designed to confirm and investigate suspected security compromises.

UNDERSTAND DDOS ATTACKS.

- DDoS attacks on election infrastructure can hinder access to voting information.
- A DDoS attack occurs when malicious cyber actors flood a public-facing, internet-accessible server with requests, rendering the targeted server slow or inaccessible.
- This prevents users from accessing online resources, such as web pages and online accounts, and may disrupt an organization’s activities for a period of time, potentially hindering voters’ ability to access voting information or unofficial election results.

PROTECT AGAINST DDOS ATTACKS.

Product Link	Description
Cloudflare DDoS Protection	Cloudflare's Athenian Project provides provides unmetered and unlimited DDoS protection through their Autonomous DDoS Protection Edge, which automatically detects and mitigates DDoS attacks. The Autonomous Edge includes multiple dynamic mitigation rules exposed as Cloudflare DDoS Attack Protection Managed Rule sets, which provide comprehensive protection against a variety of DDoS attacks across L3/4 and L7 of the OSI model. This tool mitigates against DDoS attacks without incurring latency or interfering with legitimate users. To learn more on DDoS protection and to get started with the Athenian Project, visit the Cloudflare Athenian Project page.

PROTECT AGAINST DDOS ATTACKS.

Product Link	Description
Cloudflare DNS	Cloudflare provides fast and secure managed Domain Name System (DNS) as a built-in service on its network. When users/organizations use Cloudflare DNS, all DNS queries for user/organization domains are answered by Cloudflare’s global Anycast network. The Anycast network allows Cloudflare to mitigate DDoS attacks directed at any site using Cloudflare name servers. In addition, Cloudflare DNS comes with Domain Name System Security Extensions (DNSSEC) protocol, which creates a secure domain name system by adding cryptographic signatures to existing DNS records. By checking its associated signature, users/organizations can verify that a requested DNS record comes from its authoritative name server and wasn’t altered en route, as opposed to a fake record injected in a man-in-the-middle attack.

PROTECT AGAINST DDOS ATTACKS.

Product Link	Description
Cloudflare HTTPS Encryption (Secure Socket Layer [SSL]/Transport Layer Security [TLS])	This tool offers free SSL certificates to keep user data secure, verify ownership of the website, prevent attackers from creating a fake version of the site, and gain user trust. By encrypting any data that goes between a user and a web server, SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. SSL also stops certain kinds of cyberattacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data.

PROTECT AGAINST DDOS ATTACKS.

Product Link	Description
Google reCAPTCHA	reCAPTCHA uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on a user's website.
Google Jigsaw Project Shield	Project Shield is a free service that defends news, human rights, and election-monitoring sites from DDoS attacks.
Lumu Technologies Lumu Free	Lumu Free offers continuous monitoring across the network by leveraging multiple sources of metadata (DNS, proxy, firewall). Organizations can uncover contact with malicious infrastructure, enabling threat mitigation and attack prevention. Malicious incidents can be labeled to ensure prioritization according to an organization's risk tolerance.
Let's Encrypt	This tool provides a free digital certificate to enable HTTPS (SSL/TLS) for websites. While Let's Encrypt provides a free way to enable HTTPS, its lack of enterprise support may require internal support from jurisdictions.

DETECT A DDOS ATTACK.

Product Link	Description
Cloudflare Web Analytics Cloudflare Logs	Cloudflare’s built-in analytics give users/organizations deeper insights into their traffic patterns, threats observed (and blocked), and other information found in the dashboard. High-level analytic dashboards provide overviews of traffic and security posture, including traffic and firewall events, DNS query traffic, and the geographical distribution of DNS queries over time. Cloudflare provides access to detailed logs of HTTP requests for domain. Logs are typically used for debugging, identifying configuration adjustments, and creating analytics, especially when combined with other data sources such as application server logs. Logs are helpful when investigating incidents such as website outages.
Cloudflare Rate Limiting	Cloudflare Rate Limiting automatically identifies and mitigates excessive request rates for specific URLs or for an entire domain. Request rates are calculated locally for individual Cloudflare data centers. The most common uses for Rate Limiting are DDoS and brute-force attack protection, and to limit access to forum searches, API calls, or resources that involve database-intensive operations at user/organization origin.

OTHER TOOLS

Microsoft AccountGuard adds an extra layer of protection against Nation-State sponsored attackers to elections organizations.
Crossfeed is a tool that continuously enumerates and monitors an organization's public-facing attack surface in order to discover assets and flag potential security flaws.
Azure for Elections is a set of security and resiliency assessments & enhanced support for elections-critical workloads running in the Azure cloud - Cloud Cybersecurity Assessments - Resiliency assessments for high load - Prioritized rapid support response during Election Week
The Cloudflare Anycast Content Delivery Network quickly routes incoming traffic to the nearest data center with the capacity to process the request efficiently, handling surges in web traffic due to registration deadlines and election result updates.
The Cloudflare Web Application Firewall (WAF) protects the integrity of information on the user/organization election website from common vulnerabilities, such as Structured Query Language (SQL) injection attacks, cross-site scripting, and cross-site forgery requests.
GRR Rapid Response is an incident response framework focused on remote live forensics. The goal of GRR is to support forensics and investigations in a fast, scalable manner to allow analysts to quickly triage attacks and perform analysis remotely.

ELECTION SECURITY RUMOR VS. REALITY

- https://www.cisa.gov/rumorcontrol
- While important commonalities exist across and within states, each state, local, and territorial election jurisdiction administers its elections under a unique legal and procedural framework using varying systems and infrastructure. The differences and complexity introduced by this decentralization can lead to uncertainty in the minds of voters; uncertainty that can be exploited by malicious actors. Complementing election officials' voter education and civic literacy efforts, this page seeks to inform voters and help them build resilience against mis-, dis- and mal-information (MDM) narratives about election infrastructure.

VOTING MACHINES

Regular Ballots

- Votes must be auditable.
- voter knows that the marks they made on their ballot express their real intent.
- Punch card
- Mechanical lever voting
- Optical scan voting machines, where you fill in a bubble on the ballot next to the candidate names.
- Direct-recording electronic voting machines - completely impossible to audit.

Absentee Ballots

- high-speed scanners that scan 800 ballots per minute
- automatic envelope openers
- signature-verification software – rejecting a signature that’s valid is more likely than rejecting a forged signature
- Post-office nop longer stamps all envelopes so post-marked deadlines are not reliable

CANVASS

- Checking and cross-checking votes
- Spread sheet: votes per voting machine versus candidate per office and votes per precinct

- Canvass is sent to a state and then applied in the same way across counties

EXPLAIN POSITIVE USES OF FAKE NEWS

- Fake news, or intentionally misleading information presented as real news, is generally considered a harmful and negative phenomenon. However, there are some potential positive uses of fake news that could have a beneficial impact in certain contexts. Here are a few examples:

1. Educational purposes: In some cases, fake news can be used as a teaching tool to help people become more discerning and critical consumers of news. By creating fake news stories and asking people to evaluate them for accuracy and bias, educators can help individuals develop the skills needed to identify misinformation and propaganda.
2. Satire and parody: Fake news can be used for comedic or satirical purposes, such as the satirical news show "The Daily Show" or the satirical website "The Onion." This type of fake news can be used to critique or satirize political or social issues, and can be a valuable form of political commentary.
3. Psychological research: In some cases, fake news can be used as part of psychological research studies to understand how people process and react to misinformation. This research can help to inform efforts to combat the spread of fake news and improve media literacy.
4. Security and intelligence operations: In some instances, fake news can be used as part of security or intelligence operations to deceive adversaries or disrupt their activities. For example, intelligence agencies may create fake news stories to mislead foreign governments or terrorist groups.

- It is important to note that the potential positive uses of fake news are limited and are outweighed by the potential harm caused by its spread. The intentional creation and dissemination of fake news is a serious problem that can cause significant harm to individuals, societies, and democracies. It is important to be vigilant in identifying and combatting the spread of fake news.

Thank you !!