COMBATING MISINFORMATION DISINFORMATION IN NATIONAL ELECTIONS

Legal and Technical Frameworks Requirements

Desmond Israel ESQ. CISSP, CIPM, CCT, CC

Founder/Lead Consultant

Information Security Architects Ltd, Ghana

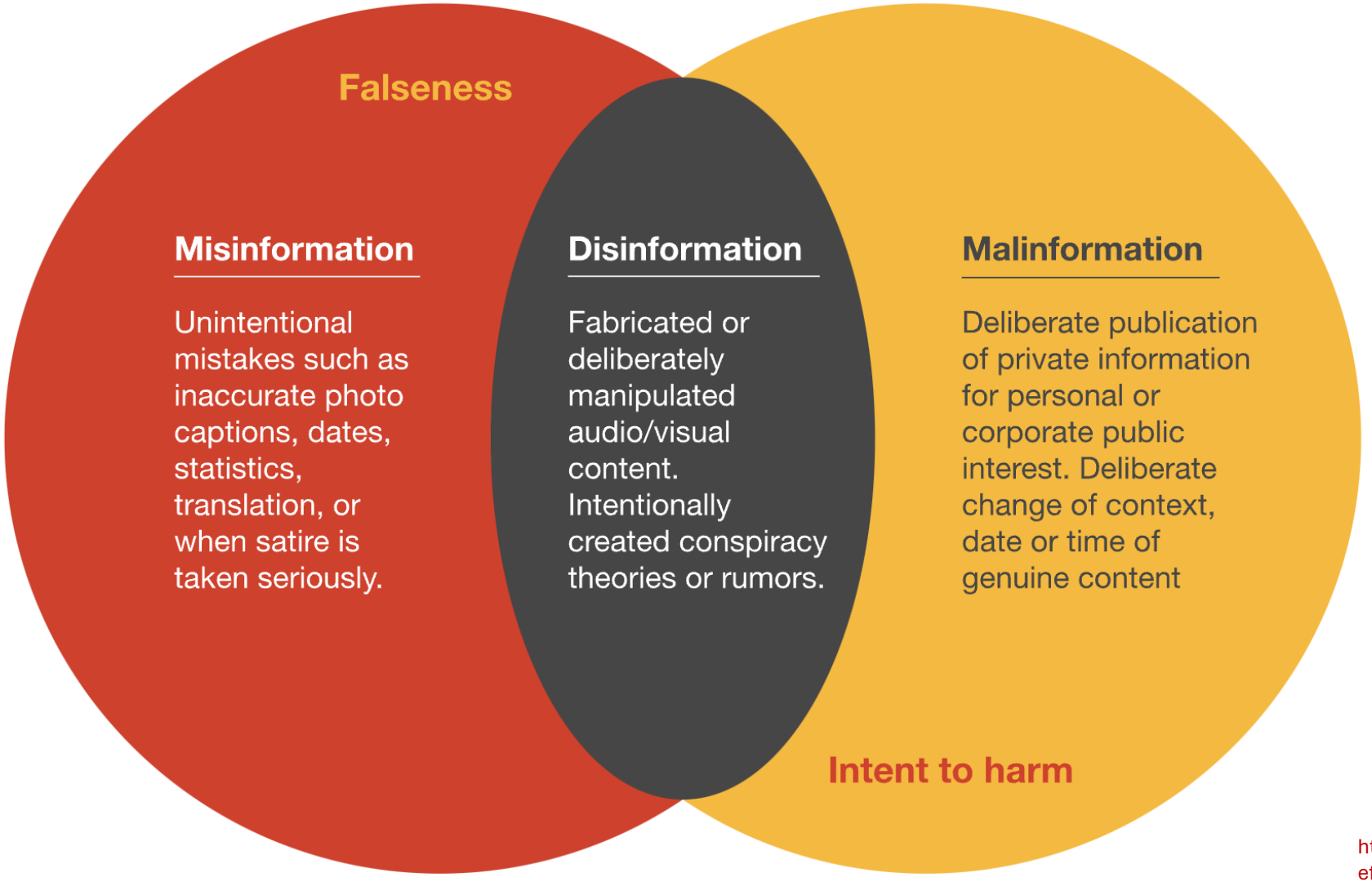
SIGNPOST

- Context
- Global Case Studies
- Legal Requirements
- Technical Requirements
- Combat Feed Tunnel
- Call to Action

CONTEXT

1

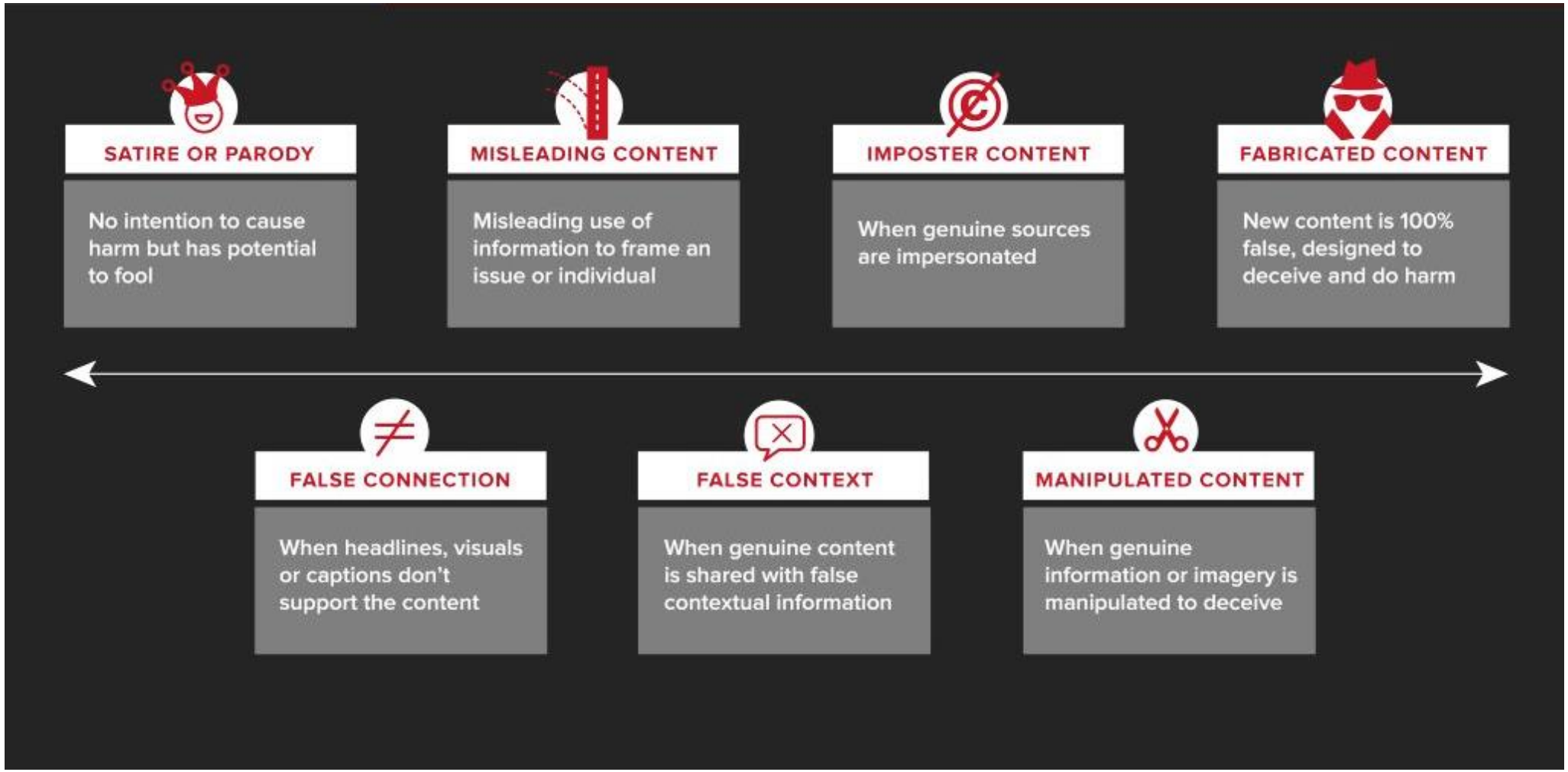
CONTEXT: The Era of Information Disorder



Source: FirstDraft, The essential guide to understanding the information disorder, 2019.

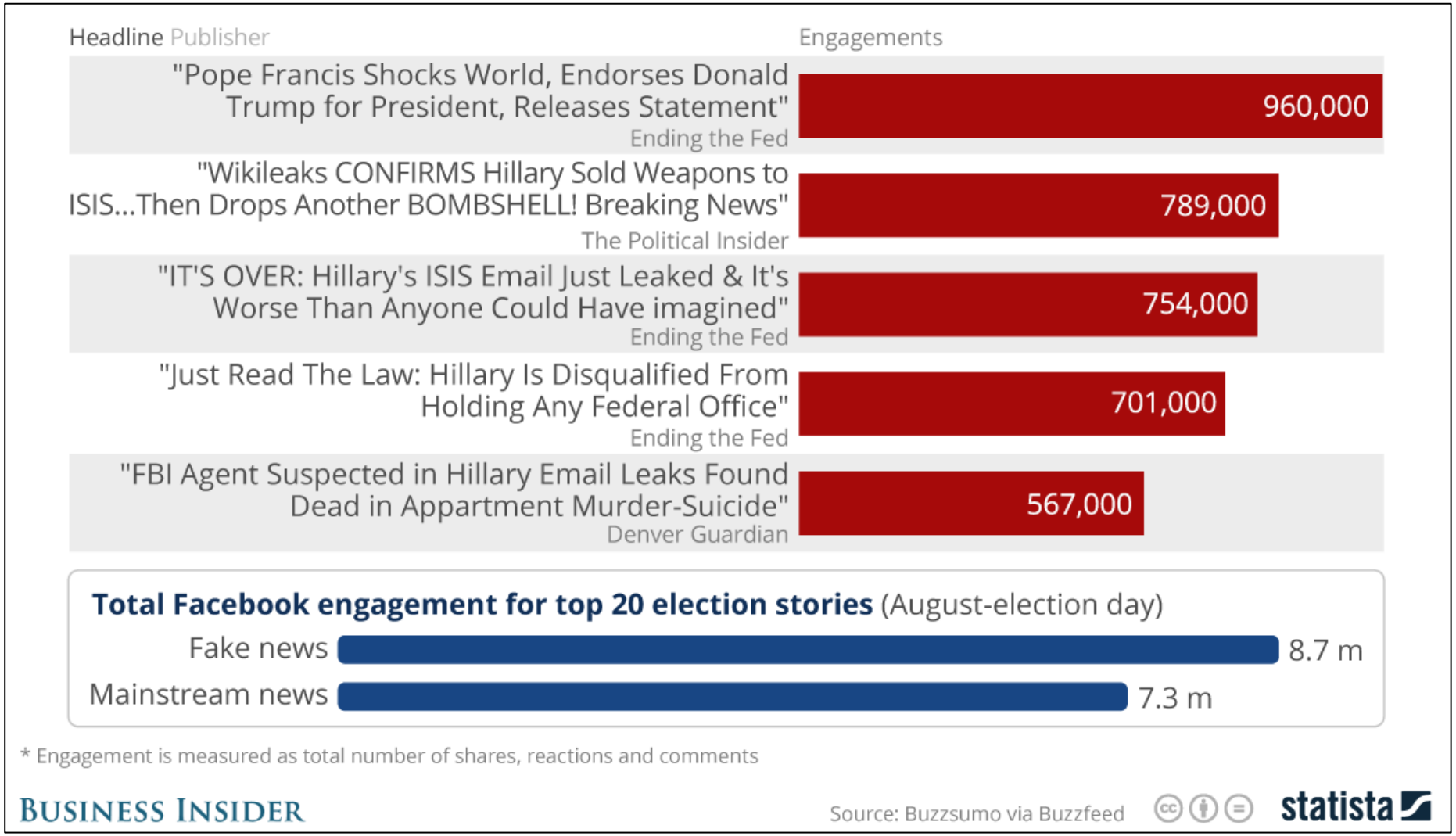
https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html

CONTEXT: Identifying the disorder



https://libguides.uvic.ca/fakenews/types

CONTEXT: Top 5 Fake US Election Stories



https://guides.lib.berkeley.edu/fake-news

GLOBAL CASE STUDIES

2

Global Case Studies: Europe's 2017 Election Interference

Mar

Netherland Public Election

Overview: The 2017 Dutch election came at a time of increasing populism in Europe, with the far-right Party for Freedom (PVV) and its leader Geert Wilders gaining significant attention.

May

France [Macron's Campaign]

Overview: The French Presidential election saw a significant disinformation campaign **aimed at undermining the candidacy of Emmanuel Macron**, the eventual victor. Russian actors have been linked to both online disinformation and cyberattacks targeting Macron's campaign.

Jun

UK Snap Elections

Overview: The UK snap election occurred in the wake of the Brexit vote, a politically volatile time for the country. Russia has been accused of attempting to **influence British political discourse, especially regarding Brexit-related narratives.**

Sep

Germany: Federal Elections

Overview: The German Federal elections saw attempts to spread disinformation, primarily targeting **Chancellor Angela Merkel and her Christian Democratic Union (CDU) party**. Russian interference aimed to exploit the refugee crisis and Merkel's pro-refugee policies to foment political division.

Global Case Studies: Europe's 2017 Election Interference

Russian Election Disinformation Tactics Table

	Country	Overview	Tactics	Tools	Objectives
1	UK (June 2017) Snap Elections	UK elections influenced by Brexit debates, Russian attempts to exacerbate societal divisions.	Social media manipulation, divisive content amplification.	Social media bots, troll farms.	Sow discord around Brexit, weaken Theresa May's leadership.
2	Netherlands (March 2017)	Populist rise in Netherlands with Geert Wilders, Russian efforts to polarize on immigration.	Polarization on immigration, fake news targeting Wilders' opponents.	Troll accounts, bots, factitious news.	Push far-right narratives, undermine trust in centrist candidates.
3	France (May 2017) Macron Campaign	Targeted disinformation and hacking against Macron's campaign, promoting far-right Le Pen.	Macron leaks, fake news on social media, amplification of far-right messaging.	Hacking (APT28), RT, Sputnik, social media manipulation.	Weaken Macron, boost Le Pen, undermine EU support.
4	Germany (Sept 2017) Federal Elections	Anti-Merkel disinformation focusing on refugee crisis, aiming to weaken her stance on Russia.	Amplification of refugee crisis, anti-immigrant narratives, fake news.	RT Deutsch, Sputnik, fake migrant crime stories.	Weaken Merkel, undermine refugee policies, destabilize pro-EU stance.

LEGAL REQUIREMENTS

3

Legal Requirements

LEGISLATIVE FRAMEWORK

Legislation should **criminalize the deliberate dissemination of false information** with the intent to disrupt elections.

DATA PROTECTION

It is important to ensure that any efforts to track and counter disinformation **respect existing data protection laws**.

LEGAL ACCOUNTABILITY

Ensure that platforms are held legally accountable for not promptly removing disinformation during elections. This includes regulations to **enforce transparency in political advertising.**

Legal Requirements

Law/Framework	Scope	Mechanisms	Examples/Notes
Electronic Communications Act, 2008 (Act 775 as amended) (Section 76)	Governs the transmission and publication of information through electronic communication systems, including social media.	The National Communications Authority (NCA) can impose fines or revoke licenses of offenders.	Section 76 criminalizes the intentional transmission of false communications, leading to harm.
Criminal Offences Act (S. 208)	Criminalizes the publication of false news that can cause fear and alarm to the public.	Police and the Attorney General can prosecute individuals for false publications.	Individuals can be fined or face imprisonment for publishing fake news that leads to public unrest.
Right to Information Act, 2019 (Act 989)	Regulates the dissemination of information by public institutions, promoting transparency.	The Information Commission enforces the release of accurate public information.	Not directly related to fake news, but enhances access to verified public data to counter disinformation.

Electronic Transactions Act, 2008 (Act 772)

Cybersecurity Act, 2020 (Act 1038)

TECHNICAL REQUIREMENTS

4

Technical Requirements

Monitoring and Detection Tools

Leverage systems like Media Sonar, CrowdTangle, and Hoaxy to track social media trends and identify disinformation in real-time. These tools **monitor specific keywords, URLs, hashtags, and conversations** across social platforms.

Incident Response Coordination

A rapid response team (like CERT or the equivalent) is essential for addressing disinformation crises. **Create clear protocols for communication and action.**

Threat Intelligence Sharing

Governments, social media platforms, and civil society need to collaborate in real-time. Platforms like Facebook's **ThreatExchange allow entities to share intelligence on disinformation actors or tactics**.

Cyber Forensics

Use digital forensics tools such as EnCase or X-Ways Forensics to trace the origin of disinformation campaigns. These tools allow forensic experts to **track metadata, timestamps, and IP addresses.**

COMBAT FEED TUNNEL

5

Combat Feed Tunnel (CFT) - Approach

Identify the Claim:
Determine the specific claim or piece of content that needs verification.

1

Collect Data:
Use the tools mentioned above to gather all available information related to the claim.

2

Analyze the Data:
Assess the credibility of the sources, looking for any inconsistencies or signs of tampering.

3

Corroborate with Trusted Sources:
Compare findings with established facts from trusted organizations or official statements.

4

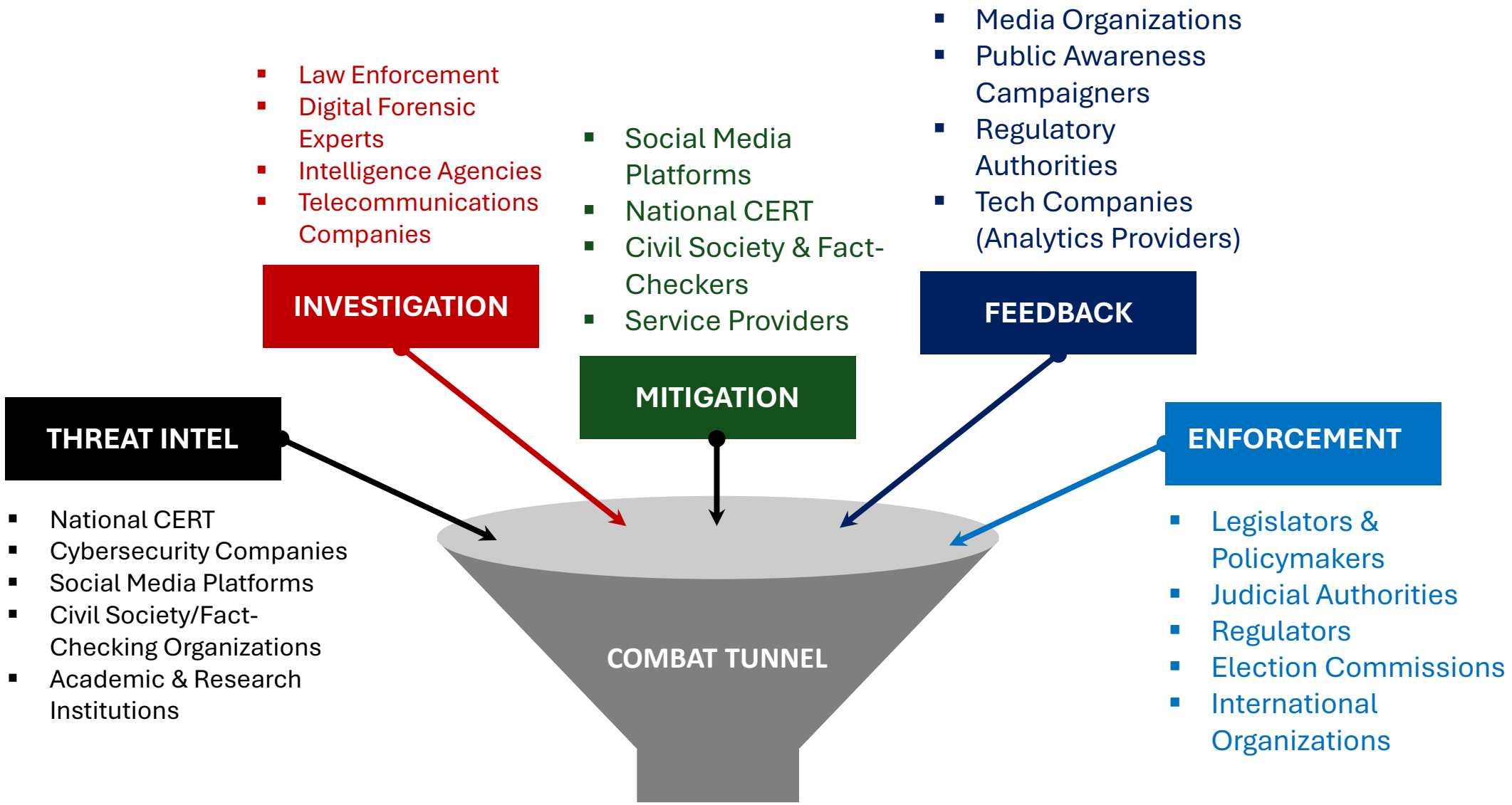
Map the Spread:
Determine how the misinformation has spread through social networks to understand its impact and reach.

5

Report Findings:
Share the results of the investigation with the public to counteract the spread of the misinformation.

6

Combat Feed Tunnel (CFT) - Players



Combat Feed Tunnel (CFT) - Roles

Theart Intel Feed	Investigation Feed	Mitigation Feed	Feedback	Enforcement Feed
Start with inputs from national CERT, social media platforms, and cybersecurity companies, utilizing threat intel tools. Continuous monitoring by fact-checkers and research bodies.	Reports from law enforcement, forensic experts, and telecom companies. Legal teams investigate the origin and spread of disinformation.	Coordination between platforms and CERT to execute mitigation measures such as content takedowns and blocking. Public awareness efforts to inform the public of disinformation threats.	Public and private organizations (e.g., media, regulators) providing real-time data on the effectiveness of mitigation. Deploy tools and analytics providing performance feedback.	Legislative and judicial follow-up to ensure compliance and prosecute disinformation actors. International and national organizations enforcing cross-border actions where necessary.

Combat Feed Tunnel (CFT) – Sleuthing Tools

Advanced Search Operators: Utilize platform-specific search functions on social networks like Twitter and Facebook. Keywords, hashtags, and phrases, when combined with advanced search operators, can pinpoint the first mentions of a claim.
Reverse Image Searching: Tools like Google Images or TinEye allow investigators to find where an image first appeared online. This is crucial when images are used out of context to support false narratives.
Geolocation Verification: Platforms such as Google Earth and Bellingcat's geolocation tools help verify the location depicted in social media posts, which is often misrepresented in viral misinformation.
Social Network Analysis Tools: Software like Gephi or NodeXL can map out the spread of information across networks, identifying key influencers and nodes that may be responsible for the initial spread.
Metadata Analysis Tools: EXIF data viewers can extract metadata from images and videos, which can reveal the original creation date and potentially the location, debunking misinformation about events' timelines.
Fact-Checking Websites: Websites like Snopes, FactCheck.org, and Hoax-Slayer provide references for debunking popular myths and misinformation.
Archival Services: The Wayback Machine or Archive.is can show the history of a web page or claim, demonstrating how it may have changed over time.
Bot Detection Tools: Tools like Botometer can assess whether a social media account has bot-like characteristics, often used to amplify misinformation.
Content Verification Browser Extensions: Extensions like InVID can help in verifying the authenticity of videos, checking for signs of manipulation.
Crowdsourcing Platforms: Platforms like Reddit's r/RBI (Reddit Bureau of Investigation) allow users to crowdsource OSINT investigations, pooling together diverse skill sets to uncover the origins of misinformation.

https://www.linkedin.com/pulse/using-osint-trace-origins-viral-misinformation-goldenowlosint-roczf/

CALL TO ACTION

6

Call to Action

"In the face of escalating misinformation and disinformation, safeguarding our democratic institutions requires collective vigilance, technical innovation, and unwavering legal enforcement.

Let us unite across sectors—government, civil society, technology, and law—to build a digitally resilient democracy where truth prevails, and trust is restored.

The time to act is now, for inaction is not an option when the very foundation of our democratic processes is at stake."

THANK YOU

D E S M O N D I S R A E L E S Q .

LLM (Natsec/Cybersec) | LLB | BSc (Mgt. with Computing) | BL | Advanced Diploma (IT)

CISSP | CIPM | CCT | CC | Verified Certificate (Cyberwar, Security and Intelligence)

Lawyer and Data Privacy/Information Security Practitioner

Founder & Lead Consultant, Information Security Architects Ltd (***Rapid7 & CodeHunter Partner***)

Adjunct Lecturer, Ghana Institute of Management and Public Administration (GIMPA) School of Law

Consulting Partner, Legal Afrique Unlimited

Technology Policy Researcher / Former Fellow (Center for AI and Digital Policy)

Research Consultant (Child Online Africa)

Memberships: GBA, ISC2, IAPP, IIPGH, ISOC-SIG

desmond.israel@gmail.com | Linkedin.com/in/desmondisrael | @desmond_israel