WEAPONIZATION OF INFORMATION IN THE ERA OF INSECURITY

Presented by
Professor Wole Michael OLATOKUN
Department of Data & Information Science
University of Ibadan, Nigeria
Email: woleabbeyolatokun@yahoo.co.uk

Lead Paper delivered at the Maiden Virtual Conference on Social Media, Fake news, Misinformation and Information Disorder in the era of Insecurity on Monday 23 May, 2022 at the Kwara State University, Malete, Kwara State, Nigeria

Outline of the presentation

- Introduction
- The Information age
- Industrial Revolution throughout history
- Key drivers of 4IR
- Conceptual definitions
  - Information
  - Weaponize
  - Weaponised Information
  - Cognitive hacking
  - Fake news
  - Social media
  - Insecurity
- Causes of insecurity in Nigeria
- Social media and insecurity
- Information dissemination on social media
- When does information on social media becomes weaponized?
- Cases of information weaponization
- Responses to information weaponization
- Conclusions

Introduction

The **Information Age** (also known as the **Computer Age**, **Digital Age**, or **New Media Age**) is a historical period that began in the mid-20th century, characterized by a rapid epochal shift from traditional industry established by the Industrial Revolution to an economy primarily based upon information technology.

INDUSTRIAL REVOLUTION THROUGHOUT HISTORY

- **First Industrial Revolution.** It occurred at the end of the 18th century, in 1784, when steam was harnessed for mechanical production.
- **Second Industrial Revolution.** In 1870, mass production powered by electricity was first introduced. The assembly line was invented and the industrial sector speeded up exponentially.
- **Third Industrial Revolution.** In 1969, advances in computing led to machine programming, which opened the door to progressive automation.
- Around 2014, Schwab, the German economist foresaw what was to come: "We are at the beginning of a revolution that is fundamentally changing the way we live, work, and relate to one another". **In its scale, scope and complexity, what I consider to be the Fourth Industrial Revolution is unlike anything humankind has experienced before.** And this is for three reasons about which the experts agree: Its speed, scope and unprecedented impact.

Key drivers of the 4IR

- Explosive Data and Information leading to Bigdata
- Artificial Intelligence &Experts Systems
- Machine Learning
- Robotics
- Internet of Things
- Augmented and Virtual reality
- Exponential technology
- 3D and 4D Printing

Conceptual Definitions

INFORMATION: Information is data presented in a readily comprehensible form to which meaning has been attributed within the context of its use.

- Information is disseminated with the aid of media or channels such as word of mouth, television, radio, newspaper, magazine, books, journals and the internet.
- Information disseminated on the internet are done with the aid of social media tools and platforms.
- In this webinar, social media is the focus. Social media refers to "interactive digital media, which incorporate two-way communication & involve some form of computing" (Logan, 2016).

Conceptual Definitions

WEAPONIZE: adapt for use as a weapon.

WHAT IS WEAPONIZED INFORMATION?

Weaponized information is a message or content piece that is designed to affect the recipient's perception about something or someone in a way that is not warranted. The term implies a target and the intention to cause harm.

The term ‘the weaponisation of information’ is often used to describe this highly instrumental use of the media, including social media, to further particular interests.

Weaponized information consists of:

- intentional falsehoods, known as **disinformation**.
- **It can be true but taken out of context,** like a comment carefully selected from a longer statement so that it does not reflect what the speaker said.
- **It may be a mixture of truth and lies,** so that the known facts lend credence to the untruths.
- The information **may be true but its significance overblown or the timing of release calculated** to cause the most harm possible.

COGNITIVE HACKING

Cognitive hacking is a cyberattack that seeks to manipulate the perception of people by exploiting their psychological make up

FAKE NEWS

- Comprises fabricated information geared towards legitimating falsehood to achieve political gains.
- Studies in fake news in Nigeria cut across examining challenges in curtailing the spread of misinformation and disinformation in social media during elections (Assay, 2019)
- Pragmatic use of Facebook as a propaganda to deceive electorates (Olajimbiti, 2019).

INSECURITY

Beland (2005) defined insecurity as the state of fear or anxiety or lack of protection or inadequate freedom from danger. It is a state of one's life not being safe as a result of some threats or negative factors.

The Causes of Insecurity in Nigeria

1. **Boko-Haram Crisis**
2. **Socio-Economic Condition**
3. **The Poor Attitude of Government to Crime Control**
4. **Collaboration with Criminals**
5. **Weak Security System**
6. **Loss of Socio-Cultural and Communal Value System**
7. **Porous or compromised Borders**
8. **High level of unemployment/poverty**
9. **Ethnicity**
10. **The Menace of Fulani Herdsmen Activities in Nigeria**

Information dissemination on Social Media

- Social media refers to the means of interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks.
- Social media is about conversations, community, connecting with the audience and building relationships.
- Today, when we talk about information, what comes to mind is the social media which serves as a channel to convey information.

Popular Social Media Tools and Platforms

- **Blogs:** A platform for casual dialogue and discussions on a specific topic or opinion.
- **Facebook:** The world's largest social network, with more than 2.93 billion monthly active users (as at first quarter 2022). Users create a personal profile, add other users as friends, and exchange messages, including status updates. Brands create pages and Facebook users can "like" brands' pages.
- **Whatsapp**: WhatsApp has **2 billion** active users worldwide. WhatsApp is ranked as the most used mobile messenger app in the world. More than 100 billion messages are sent each day on WhatsApp.
- **Twitter:** A social networking/micro-blogging platform that allows groups and individuals to stay connected through the exchange of short status messages (140 character limit).
- **YouTube/Vimeo:** Video hosting and watching websites.
- **Flickr:** An image and video hosting website and online community. Photos can be shared on Facebook and Twitter and other social networking sites.
- **Instagram:** A free photo and video sharing app that allows users to apply digital filters, frames and special effects to their photos and then share them on a variety of social networking sites.
- **LinkedIn:** A place where groups of professionals with similar areas of interest can share information and participate in a conversations.

Nigeria Social Media Poll Report (2019)

- About 120 million Nigerians (61%) have access to the internet
- The proportion of people using each social networking platform includes -Facebook (86 percent), WhatsApp (84 percent), Instagram (19 percent), Twitter (11 percent), and Snapchat (2 percent) (NOIPolls, 2019).
- Out of these, about 19% and 8% of Twitter and WhatsApp users respectively spend upwards of 10 hours daily on the average on the social media sites
- Social media thus becomes vital tools in the hands of political influencers (Ahmad et al., 2019), online recruiters, marketers, advertisers, and others who target social media users for one thing or another.

When does information on social media becomes weaponised?

- Social media being a **great source of information** can be used as a positive or a negative perspective.
- **You can change the mindset of people in a positive sense or negative sense**
- You want to project the image of an aspirant in an election. You adopt any of the social media tools to assess the view of the electorates by using materials that favours the aspirant. People would start thinking positive towards the aspirant
- If you want to start a **campaign** about anything social media is a great weapon to convey the message.

When does information on social media becomes weaponised?

When…

- Used for communication with an intent to cause damage.
- Societies are being turned to war through incitement.
- Platforms are turned into vehicles to advance a particular political agenda
- Used to promote a false or misleading narrative as factual which is very often very detrimental to certain groups or even a Nation as a whole.
- When terrorists hijack platforms to achieve their goals –Around 90% of organized terrorism is on the Internet. Terrorist groups spread their messages through sites like YouTube, Twitter, Facebook and recruit people via them.

When does information on social media becomes weaponized?

When…

- ❑ Hackers use social media to pose serious threat to others
- ❑ Social media is used to incite people to cause communal violence
- ❑ Social media is used to attack other people's religions.
- ❑ Used to pose threat to national security as it disturbs communal harmony.
- ❑ Used to catalyse revolution or political instability or civil unrest e.g. Endsars
- ❑ Used for propaganda masquerading as news
- ❑ Used for cyberbullying &cyberstalking

What are the actual weapons used?

Misinformation: incorrect information spread by people without the intent to deceive. It is actually incorrect or misleading information presented as a fact.

Disinformation: incorrect information spread by people intentionally in order to deceive or manipulate others. It is a form of propaganda.

Malinformation: is genuine information that is shared to cause/inflict harm on a person, organization or country.

Hate Speech: any form of expression (speech, text, images) which "demeans or attacks a person or people as members of a group with shared characteristics such as race, gender, religion, sexual orientation or disability"

Dangerous Speech: speech that has a special capacity to catalyze or amplify violence by one group against another.

How does weaponization works?

1. **Information operations (IO):** Coordinated disinformation campaigns are designed to disrupt decision making, erode social cohesion and delegitimize adversaries in the midst of interstate conflict.
2. **Political manipulation (PM):** Disinformation campaigns can also be used to systematically manipulate political discourse within a state, influencing news reporting, silencing dissent, undermining the integrity of democratic governance and electoral systems, and strengthening the hand of authoritarian regimes
3. **Digital hate speech (DHS):** Social media platforms amplify and disseminate hate speech in fragile contexts, creating opportunities for individuals and organized groups to prey on existing fears and grievances.
4. **Radicalization:** The ability to communicate across distances and share usergenerated, multimedia content inexpensively and in real time have made social media a channel of choice for some violent extremists and militant organizations, as a means of recruitment, manipulation and coordination.
5. **Propaganda:** A predominant purpose for which social media platforms are utilised is the distribution of propaganda. All other aspects of online strategy depend on this, in that it provides meaning and context to all other forms of content
6. **Recruitment:** In addition to propaganda distribution for broader communicative and intimidation purposes, social media is used to communicate with potential recruits. An estimated 30,000 foreign fighters have entered Syria and Iraq since 2011 due to ISIS recruitment drive.

The 7 stages of online propaganda

- recognition of the target (research on the audience),
- armament (preparation of the narratives and fake news, creation of background stories to make the disinformation credible and creation of alternative versions tailored to the different audiences),
- massive dissemination (by all available means, social and traditional media),
- activation of specific relays (military groups on social networks),
- growth (purchase of advertisements, bots, trolls),
- maintenance (by varying the stories, responding to objections),
- laundering (traces of the original actor disappear once the goal is achieved, diversion of attention and suppression of online posts and even accounts).

Cases of information weaponisation

1. **Jihadist groups:** the case of ISIS Al Qaeda had already recognized the opportunities to carry out terrorist operations in the virtual sphere.

In 2005, Ayman al-Zawahiri said, "**we are in a battle and more than half of this battle is in the media. In this media battle we are in the race for the hearts and minds of our Umma [the Muslim community]**."

Ten years later, the Geneva Center for Security Policy estimated that ISIS' campaign on social media had attracted more than 18,000 foreign soldiers from more than 90 countries.

2. Ethnic and/or religious communities: Nigeria

- The incessant farmers/herders conflicts escalated in states like Plateau and Benue in Northcentral Nigeria with increased access to social media.
- On 13 November 2018, the British Broadcasting Corporation (BBC) published an investigative report on how fake news circulated on Facebook has been fuelling the farmers/herders violent clashes in Plateau State, Nigeria.
- The BBC report referred to some images on social media falsely attributed to the violence in Plateau State which resulted in reprisal killings.
- The gory pictures trending on social media which were falsely attributed to inter-communal violence exacerbated high tensions in the country.

Examples from the BBC Report

- The BBC report cited other examples of fake news like the "**gruesome image of a woman face down in a pool of blood with a gaping shoulder wound purported to be from recent attacks which retweeted hundreds of times on Twitter**. The picture turned out to have first appeared online in 2011 in a story about domestic violence in Nigeria.

- An **image showing about six persons killed in the attacks** on closer inspection, revealed that the picture did not originate in Nigeria. It was actually the scene of a 2015 traffic accident in the Dominican Republic" (BBC, 2018).

- Another case highlighted by the BBC was when "**major Nigerian news outlets ran a story claiming that Danladi Ciroma, a leader of the Miyetti Allah Cattle Breeders Association (MACBAN), said the attacks in Plateau were revenge for the loss of 300 cows. Mr Ciroma was reported to have said that since these cows were not found, noone should expect peace in the areas.** His comments drew widespread anger and swift condemnation, he has however denied ever making the statement" (BBC, 2018).

The next slide contains disturbing images. Viewers discretion advised please

HumAngle
How Misinformation Aggravates Farmers-Herders Conflict In Nigeria - HumAngle Media

FIJ NG
EXCLUSIVE: How Local Militants Colluded with Fulani Killer Herdsmen to Kill Up to 200 Villagers in Benue

OTHER USES OF SOCIAL MEDIA AS A WEAPON

1. Cloning of Nigeria's President
2. ENDSARS Protests
3. Deborah Blasphemy case
4. Russia's purported interference in America's 2016 & 2020 elections
5. Russian-Ukraine war

Tools used for weaponization

- **Bots:** These are automated or semi-automated actors, like bots or netbots. This tactic involves fake Twitter or Facebook accounts that allow for the rapid diffusion of fake news through biased retweets and likes.
- **Trolls:** there are internet trolls: individuals who spread information, saturate certain websites with comments, and/or harass others.
- **Leaks:** leaks may form part of an information manipulation campaign, such as is evidenced by the American presidential election (2016 DNC Leaks) and French presidential election (2017 Macron Leaks), They can be used to discredit a target, who may be either a victim of hacking, or a third party.
- **The falsification of documents:** One of the most common methods—though crude and relatively easy to detect—is the falsification of documents: images, articles in newspapers, internet sites
- **Electoral interference:** Electoral interference can target systems (electronic voting, voting lists, party databases), which consequently affects the population's confidence in the results, or the voters themselves in order to influence their vote.

Curtailing Weaponization

1. **Prevention:** Reducing the incidence of weaponization with activities that include influencing policies and regulations of governments, multinational bodies, industry associations & technology companies

2. **Monitoring, detection and assessment of threats:** Bringing together a wide variety of stakeholders, from intelligence organizations to civil society organizations, to identify threats and their potential impact

3. **Building resilience:** Helping fragile populations resist the worst impacts of the weaponization of social media, with digital media literacy training, online and offline awareness-building and education, and strategies to build social cohesion.

4. **Mitigation:** Minimizing harm once weaponized information has already spread. E.g. including warning and response components into monitoring systems, establishing crisis and response plans, and countering online hate speech and radical or violent extremist narratives.

Responses to Information weaponization

- **Some common questions:**
- Is it better to respond to an information weaponization attack or to simply ignore it?
- If the choice is to respond, is it sufficient to correct it or should the opportunity be used to promote an alternative message?
- Answers to these questions are a combination of ignorance and both defensive and offensive measures.

RESPONSE 1: IGNORING WEAPONIZED INFORMATION ATTACK?

- Ignoring the attack is tempting, if it is believed that the information will die on its own.
- The rhythm of the media is such that few events outlive the daily flow of information, and public opinion tends to forget quickly.
- Refuting is repeating and may help to keep the story alive.
- **"Strategic silence"** may therefore, in some cases, be the preferred option.
- The risk is allowing such false and potentially dangerous ideas to sink into the minds of the population.
- If they are not contradicted from the outset, these ideas may continue to grow with time.
- Ignorance as a strategy should therefore only be reserved for minor and inoffensive forms of weaponized information.

RESPONSE 2: REACTING DEFENSIVELY?

- Reacting defensively by correcting false information has the advantage of not allowing the ideas to spread and be left unchallenged, by quickly cutting them short.
- The task however requires time and human resources— to monitor social networks, detect manipulation attempts, formulate a response, disseminate it, and analyze its reception.
- There is also a risk that it might have the opposite effect, as the response could spark a debate, and even involuntarily give new wind to the trolls.

RESPONSE 3: DEFENSIVE AND OFFENSIVE STRATEGIES?

- The most efficient solution would therefore combine a defensive strategy with an offensive one
- This is by providing new information that will help to take back control over the discussion.
- Unfortunately, this requires even more time and resources

Recommendations

- **Enactment of relevant laws** against disinformation, misinformation, hate speech and dangerous speech.
- **Awareness and education:** support for research through partnerships with universities, massive awareness-raising campaigns, including through mail distribution, training of civil servants, journalists and companies, media literacy (basics of programming, develop capacity to distinguish between reliable and unreliable information; media literacy, cybersecurity and defense education, etc)
- **Media Outreach:** The four main government measures relating to the media consist of **registration**, **prohibition, regulation** and **denunciation**. Ministry of Information, Ministry of Communications, Nigeria Communication Commission, National Information Technology Development Agency all have roles to play

Recommendations

Civil Society: Fact-checking (the AFP Fact Check, the BBC's "Reality Check," Google "CrossCheck,") the power of fact-checking lies principally in its potential to embarrass those who disseminate false information,

Research: Universities would need to embark on extensive collaborative research in this area.

Journalists: Verifying the authenticity of information before publishing them

Everybody: Be a voice that helps stop the spread of disinformation. Raise awareness within your digital circle of family, friends, and associates about its dangers. If you notice that someone is sharing false information, speak up. Alert the person and their audience that the "news" item they posted or shared is false. Tell them about the tips and resources in this guide so they will know how to identify fake information and help combat it.

Conclusions: Anticipating the future

- Information weaponizers are creative and quick to adapt;
- Technology and the media evolve rapidly; and it is easy for new actors to arrive on the stage.
- For these reasons, we should expect information weaponization to expand and involve an ever-increasing number of actors.
- Had someone said ten years ago that the recently created social networks (Facebook in 2004, Twitter in 2008, Instagram did not exist yet) would play such a tremendous role in the lives of billions of people and be implicated in a massive information problem threatening the world, hardly anyone would have believed them.

Conclusions: Anticipating the future

- Artificial intelligence will make bots more human and, therefore, harder to detect.
- Photo, audio and video editing software, for example, will render it possible in the near future to make anyone say anything. This makes the detection of false information even more difficult.
- "Deepfake videos," in which people's faces are digitally modified in order to make them do or say anything that one wants, are already very believable.
- An even greater danger, far more subtle than the creation of a fake video, arises from the slight alteration of only a part of an audio or video clip, such as a recording of a speech.
- Another challenge lies in the possible creation of a great number of variations of that speech—e.g. the circulation of twenty different versions of a single speech, so as to hide the authentic version in the confusion.
- Knowledge in social psychology, big data and artificial intelligence—would continue to be used to create a weapon of mass division.

Distinguished audience:

Never let the future disturb you. You will meet it, if you have to, with the same weapons of reason which today arm you against the present.

— Marcus Aurelius

THANKS FOR LISTENING

WEAPONIZATION OF INFORMATION IN THE ERA OF INSECURITY

Presented by
Professor Wole Michael OLATOKUN
Department of Data & Information Science
University of Ibadan, Nigeria
Email: woleabbeyolatokun@yahoo.co.uk

Lead Paper delivered at the Maiden Virtual Conference on Social Media, Fake news, Misinformation and Information Disorder in the era of Insecurity on Monday 23 May, 2022 at the Kwara State University, Malete, Kwara State, Nigeria