FUW CENTRE FOR RESEARCH JOURNAL OF MANAGEMENT & SOCIAL SCIENCES (FUWCRJMSS)

The Interrelationship between Cyber security, Propaganda, and Hybrid Warfare in Nigerian Politics

[1]Bweseh Benjamin Musa., [2]Cinjel, Nandes Dickson & [3]Hannah Itopa, Emmanuel

[1]Department of Banking and Finance, Federal University Wukari
[2&3]Department of Public Administration, Federal University Wukari
Corresponding Email: Bwesehbenjaminmusa@gmail.com

Abstract

The article investigates how cybersecurity, propaganda and hybrid warfare interact to affect the nation's political stability and governance; revealing how cyber operations are used to propagate misinformation, compromise key infrastructure, public opinion, and trust in democratic institutions leveraging present cybersecurity framework of the Nigerian government. The interconnectedness of propaganda, hybrid warfare, and cybersecurity in Nigerian politics focusing on the cybersecurity architecture that Nigeria currently has in place, and the effects that hybrid warfare techniques have. The Study offers policy proposals to strengthen Nigeria's resilience and protect its political stability and governance in the digital era, drawing on international case studies. To strengthen Nigerian defences against these complex threats, policy proposals are offered, highlighting the necessity of cutting-edge cybersecurity solutions, strong legislative frameworks, public awareness campaigns, and international cooperation. Nigeria can effectively safeguard its political stability and maintain efficient administration in the face of threats from hybrid warfare, cyberattacks, and disinformation by taking a comprehensive strategy.

Keywords: Interrelationship, Cyber Security, Propaganda, Hybrid Warfare , Nigerian Politics

Introduction

Flourishing digital technologies have led to a change in the character of political disputes and warfare, bringing with them advanced cyber techniques, hybrid warfare tactics, and propaganda operations. This shift has significant ramifications for all countries, including Nigeria, which is attempting to manage the complexity of these interconnected issues within its political context.

In Nigeria, cybersecurity breaches, sophisticated propaganda campaigns, and hybrid warfare tactics increasingly influence political dynamics, eroding public trust, destabilizing institutions, and complicating governance. Nigeria's digital revolution has revealed risks in addition to encouraging innovation and economic success that widespread the use of social media and digital technologies which has given cybercriminals additional places to carry out their nefarious deeds.

Critical infrastructure cyberattacks causes major disruptions and misinformation efforts aimed at swaying public opinion and eroding trust in democratic processes sometimes accompany these cyber threats. (Tekedia, 2021)

Propaganda has become a potent instrument for influencing political outcomes, especially when distributed via social media. The 2019 general elections in Nigeria saw a sharp increase in the spread of false and fake

information, which influenced voter attitudes and actions, and foreign organizations are connected to coordinated disinformation campaigns aimed at influencing Nigerian politics, demonstrating that the employment of propaganda is not just limited to domestic actors (Suleiman, 2023)

Nigeria faces a difficult challenge from hybrid warfare, which combines traditional military techniques with cyber operations and propaganda which uses information operations and cyberattacks to sow disarray and instability to accomplish strategic goals without resorting to direct military combat. The effects of hybrid warfare are visible in several global conflicts, such as the crisis in Ukraine, where propaganda and cyberattacks have been employed to considerable success (Nigerian Bulletin, 2024).

Resolving the interplay among hybrid warfare, propaganda, and cybersecurity calls for a thorough and multidimensional strategy. To defend vital infrastructure, requires strengthening cybersecurity safeguards, creating strong legislative frameworks to combat cybercrime and disinformation, and raising public awareness to increase resistance to propaganda. To properly tackle these global dangers, international cooperation and intelligence sharing are also necessary, hence, the intersection of hybrid warfare, cybersecurity, and propaganda constitutes a crucial frontier in contemporary political struggle. In Nigeria, maintaining political stability, strengthening national security, and preserving democratic processes all depend on resolving these interconnected issues, therefore, this research aims to add to this important conversation by illuminating the relationship between these events and their political ramifications in Nigeria.

Objectives of the Study

This research aims to investigate the intricate relationships between Propaganda, Hybrid warfare, and Cybersecurity (PHC) in the framework of Nigerian politics. Specifically, it is tailored toward:

i. Examining the current state, role and impact of Propaganda, prevalence of Hybrid warfare tactics and cybersecurity in Nigeria;
ii. Provides a comprehensive understanding of how PHC interact to influence political dynamics in Nigeria;
iii. Offers insights into the challenges and opportunities for strengthening Nigeria's political and security landscape in the digital age.

Landscape on Cyber Security, Propaganda, Hybrid warfare and Nigerian Politics.

Cybersecurity is the defence against cyberattacks of internet-connected devices, including data, software, and hardware which is also essential in the political sphere because it protects the credibility of voting procedures, government functions, and vital infrastructure. Cyber-threats have the power to compromise political stability, jeopardise national security,

and erode public trust which can take many forms, from hacking and data breaches to disinformation campaigns and cyber espionage. As a country that is working to strengthen its democratic systems and improve its digital infrastructure, Nigeria must make sure that its cybersecurity measures are strong (CISA, 2020).

Political warfare has used propaganda, or the purposeful spread of information often biased or deceptive to sway public opinion and behavior, as a key tactic for millennia. Propaganda has changed dramatically throughout time, from the deployment of posters and pamphlets in the early political campaigns to the sophisticated use of social media platforms in modern politics. Propaganda has been essential in Nigeria in forming political narratives, affecting election results, and galvanizing public support, comprehending the workings and effects of propaganda is crucial to appreciating its significance in Nigerian politics (U.S. Department of Defense, 2018).

A comprehensive approach to conflict is represented by hybrid warfare, which combines cyberwarfare, irregular warfare, and conventional warfare with other influencing techniques including economic pressure and propaganda. Instead of using traditional open warfare which makes use of the entire range of state and non-state actors to accomplish strategic goals. Nigeria offers a conducive environment for hybrid warfare strategies due to its heterogeneous socio-political structure and unique security issues in the region. Nigeria's political stability and national security are seriously threatened by the interaction of cyber and informational methods with traditional and unconventional tactics (Mueller, 2019).

Cyber activities are having an increasing impact on Nigeria's political landscape whose activities range from the dissemination of fake news and misinformation on social media platforms to hacking attacks that target election and governmental systems whereas foreign and domestic propaganda has grown to be a potent instrument for influencing voter behavior and forming political discourse and Nigeria's security issues such as the northeastern insurgency, the Niger Delta conflicts, and inter-communal conflicts create an environment conducive to the use of hybrid warfare techniques.

Cybersecurity in Electoral Processes and Politics

Within the political context, cybersecurity refers to safeguarding government operations, election procedures, and vital infrastructure from cyberattacks that could jeopardize political stability and democratic institutions. Norris (2019) indicated that cyberattacks aimed at election systems can take many different forms, such as voter database hacking, interference with electronic voting devices, and the spread of misinformation campaigns to sway voter opinion. Allegations of foreign meddling through cyber means during the 2016 U.S. presidential election are a

well-known example of how they created serious concerns about electoral integrity.

Similar questions concerning the cybersecurity of Nigeria's election procedures have been raised due to the difficulties of the Independent National Electoral Commission (INEC) has had guarding against cyberattacks, strong cybersecurity measures are required to ensure the integrity of elections (Abubakar, 2020). The possibility of cyber intervention in elections emphasizes how crucial it is to put thorough cybersecurity measures in place to protect democratic processes. The growing frequency and sophistication of cyberattacks directed at political entities emphasizes the need of cybersecurity in governmental activities. One example of how cyber threats might affect political campaigns and electoral outcomes is the hacking of the Democratic National Committee (DNC) in the 2016 U.S. presidential election (Mueller, 2019). In a similar vein, cyber threats targeting the credibility of election processes and the dissemination of false information have been directed towards European nations (European Union Agency for Cybersecurity, 2020).

Nigeria's election commission, official websites, and vital infrastructure have all been the subject of many cyberattacks (Abubakar, 2020). These events demonstrate how urgently strong cybersecurity safeguards are needed to safeguard political processes and preserve public confidence in democratic institutions.

Cyber Threats to Governmental Operations

Because government activities depend more and more on digital infrastructure, they are vulnerable to cyberattacks. Cyberattacks on government networks may result in the loss of private data, interruption of public services, and jeopardisation of national security. One prominent instance of the far-reaching effects of cyber vulnerabilities in governmental operations is the 2015 Office of Personnel Management (OPM) data breach in the United States, where hackers gained access to the personal information of millions of federal employees (Fruhlinger, 2019).

The government of Nigeria has also been the subject of cyberattacks aimed against its digital infrastructure. These attacks erode public confidence in government institutions while also endangering the secrecy and integrity of official data. To safeguard government operations and preserve public trust in the state's capacity to protect national interests, effective cybersecurity measures are vital (Olowu, 2021).

Cybersecurity in Nigerian Politics

Nigerian politics' cybersecurity situation now displays both continued difficulties and advancements. Nigeria's National Cybersecurity Policy and Strategy (NCPS) 2021 is one of the most notable achievements in the country's cybersecurity framework establishment. The goal of this policy is to counteract the growing threat of cyberattacks and use digital technology

to boost national security and spur economic growth (Tekedia, 2021).

Nigeria yet has a long way to go in the fight against cybercrime. Cybercriminals attack people, companies, and governmental institutions in this hotspot nation. Suleiman (2023) notes that this has led to substantial financial losses as well as a rise in mistrust of digital networks. Furthermore, the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015, which governs most of the legal framework, is frequently criticised for being insufficiently comprehensive in addressing the dynamic nature of cyber threats (Suleiman, 2023).

The landscape of cybersecurity has also been changed by political initiatives. For example, the controversial cybersecurity charge that was supposed to finance cybersecurity projects was recently put on hold by President Bola Tinubu. Widespread criticism and worries about the program's potential financial impact on Nigerians led to this suspension (Nigerian Bulletin, 2024).

Nigeria is working to strengthen its cybersecurity capabilities by raising awareness, educating the public, and developing a workforce with the necessary skills. Roles like information security managers, network security engineers, and cybersecurity analysts are among the many expanding opportunities in the cybersecurity industry. Furthermore, Nigerian businesspeople possess the ability to launch cybersecurity companies to meet the growing need for services like incident response and penetration testing (Suleiman, 2023).

Inter-relationship between Disinformation, Cyber Propaganda & Modern Politics in Nigeria

Disinformation campaigns aim to discredit political opponents, change public opinion, and cause social unrest by using cybersecurity flaws to spread false or misleading information (Benkler, Faris, & Roberts, 2018). In political situations around the world, the use of botnets, phony accounts, and other cyber-tools to spread misinformation has become a major problem.

Social media sites are frequently inundated with misleading information during elections with the intention of confusing and manipulating voters. A strong cybersecurity framework is required to detect and mitigate the rapid dissemination of misinformation via digital channels (Nwachukwu, 2020). To reduce the influence of cyber-propaganda on political processes, policies must take into account the interaction between cybersecurity and disinformation.

Through governmental efforts like the National Cybersecurity governmental and Strategy (NCPS), the Nigerian government has taken action to address cybersecurity concerns. Nigeria's critical infrastructure and cyberspace are safeguarded by the NCPS, which also emphasises the need for public-private sector cooperation to improve cybersecurity resilience (National Security Adviser, 2021). These policies must be implemented effectively to

reduce cyber dangers and protect political processes.

Studies have demonstrated that propaganda has a major impact on public opinion and voting behavior. Digital propaganda can influence public opinion and impact political decisions, as seen by the use of targeted social media efforts during the Brexit referendum and the 2016 U.S. presidential election (Benkler, Faris, & Roberts, 2018). The ability of social media platforms to quickly spread misleading information is a serious obstacle to the preservation of reasoned and informed public conversation.

During election seasons, social media is very frequently used in Nigeria to disseminate rumours and sway public opinion (Nwachukwu, 2020). Comprehending the workings and effects of propaganda is essential to formulating counterstrategies and safeguarding the integrity of democratic processes.

Impact of Hybrid Warfare on Political Dynamics

After Russia annexed Crimea in 2014, the idea of hybrid warfare gained traction as a means of achieving strategic objectives without issuing a formal declaration of war by combining cyberattacks, military force, and propaganda (Galeotti, 2016). Since then, several state and non-state actors have embraced this strategy to achieve political goals affordably and transparently.

The potential of hybrid warfare to upend political stability and threaten state sovereignty emphasizes its significance in contemporary politics. Insurgent organizations and other non-state actors have used hybrid warfare strategies in Nigeria to subvert government authority and further their own goals (Olowu, 2021). The combination of irregular warfare tactics, propaganda, and cyberattacks in these conflicts emphasises the necessity for all-encompassing solutions to confront hybrid threats.

Hybrid warfare techniques can take advantage of cybersecurity flaws and magnify the effects of propaganda, while cyberattacks can help propagate false narratives by breaching information systems. For instance, Russian actors used a mix of disinformation campaigns and cyberattacks during the 2016 U.S. presidential election to stoke division and affect voter behaviour (Mueller, 2019). This concerted effort is an example of how propaganda, hybrid warfare, and cybersecurity may be combined to further political goals.

The interaction of these factors has been seen in Nigeria in several conflicts and political crises. The use of hybrid warfare by insurgent organizations, misinformation campaigns to sway public opinion, and cyberattacks to sabotage election processes highlight the complex nature of contemporary political conflicts (Abubakar, 2020). To tackle these obstacles, a comprehensive strategy incorporating counter-propaganda

tactics, cybersecurity precautions, and efficient responses to hybrid threats is needed.

If left unchecked, cybersecurity risks have the potential to taint election outcomes and cause political instability. Second, propaganda has the power to polarise society, influence public opinion, and inspire violence—especially in the digital era. Addressing its issues requires an understanding of its workings and effects. Third, Nigeria's complicated security environment, which is characterized by the existence of insurgent organizations and regional conflicts, leaves it open to the use of hybrid warfare strategies that could further destabilize the nation.

Theories of Propaganda, Hybrid warfare, and Cybersecurity in political warfare

This literature review explores key theories that elucidate the role and impact of cybersecurity in political warfare, including deterrence theory, information warfare theory, and cyber power theory.

Deterrence Theory

The idea of deterrence, which was first applied to the strategic use of nuclear weapons during the Cold War, has been modified for application in the cyberspace. The fundamental idea behind cybersecurity deterrence theory is to stop cyberattacks by threatening serious repercussions or retaliation (Libicki, 2009). The difficulties in determining who is responsible, the wide range of players involved, and the fluctuating intensity of cyberattacks, researchers have argued over the efficacy of deterrence in cyberspace (Nye, 2011).

Deterrence is nevertheless a key principle for comprehending state behaviour in the cyberspace, despite these difficulties. As an illustration, the U.S. Department of Defense's Cyber Strategy places a strong emphasis on deterrence by building offensive cyber capabilities and informing adversaries of the possible repercussions (U.S. Department of Defence, 2018).

Information Warfare Theory

The strategic application of information and communication technology to accomplish military and political goals is examined by information warfare theory. Accordingly Arquilla and Ronfeldt (1996), this idea covers a wide range of actions, such as cyber espionage, cyberattacks, and psychological operations meant to affect public opinion and decision-making. Information warfare emphasizes the dual function of cybersecurity in safeguarding and taking advantage of information systems by using information as both a weapon and a target.

The idea of the information domain as a separate battleground where wars are fought by the manipulation and control of information is fundamental to information warfare. This field is crucial to contemporary political warfare, since cyber operations are

employed to disseminate misinformation, obstruct enemy communications, and get intelligence (Ventre, 2016). Information warfare theory is applied to modern conflicts, as demonstrated by Russia's employment of cyber techniques during the annexation of Crimea and its meddling in numerous elections around the world (Galeotti, 2016).

Power Theory

Cyber power theory examines the strategic significance of cyber capabilities in the projecting of national power (Nye, 2011). According to this view, cyber power has social, political, and economic facets in addition to traditional military might. The ability of a country to use cyberspace for offensive or defensive operations to accomplish strategic goals is known as cyber power. Cyberpower can be classified as "hard" or "soft" according to Nye's concept. While soft cyber power focuses on influence and attraction, such as forming cyber alliances and influencing global standards, hard cyber power entails coercive measures, such as cyberattacks and cyberespionage. A country's overall cyber power and its capacity to use cyber capabilities in political warfare are determined by the balance of these factors. China's cyber strategy, which is sometimes called "cyber sovereignty," is based on the principle of cyber power. Through cyber operations targeted at geopolitical influence and economic espionage, China aims to project power abroad while simultaneously controlling its home cyberspace (Segal, 2017). This strategy emphasises how diverse cyberpower is in political conflict.

Sociotechnical Systems Theory

In cybersecurity, the interaction between social and technical components is highlighted by socio-technical systems theory. According to this idea, successful cybersecurity in political warfare necessitates knowledge of how organizational structures, technology systems, and human actors interact (Johnson & Goetz, 2007). To build robust cyber systems, the sociotechnical approach emphasizes how crucial it is to match organizational and social norms with technology defences. For instance, the effectiveness of cyber operations frequently depends on taking advantage of human weaknesses, such as phishing assaults that target specific members of an organization (Mitnick & Simon, 2011). To reduce these risks, sociotechnical systems theory supports all-encompassing approaches to cybersecurity that incorporate technical controls with organisational policy, training, and education.

Cyber Conflict Theory

The study of cyber conflict theory looks at the dynamics of disputes that take place in and through cyberspace. This theory focuses on the strategic interactions between state and non-state actors while analysing the nature, causes, and effects of cyber wars (Valeriano & Maness, 2015). Understanding how cyber operations fit into larger conflict strategies and the

circumstances in which they escalate or de-escalate is the aim of cyber conflict theory. Lindsay (2013), research conducted using this approach has revealed several elements that effect cyber conflict, such as the impact of international standards, the importance of asymmetries in cyber capabilities, and the difficulties associated with attribution. The idea also discusses how cyberwarfare may affect global peace and security as well as how cyberattacks may lead to larger-scale military conflicts.

Propaganda in Modern Nigerian politics

To stop propaganda from spreading throughout Nigerian politics, cybersecurity is essential. Due to Nigeria's growing digital penetration, political campaigns and, regrettably, the spread of false information and propaganda have made cyberspace a vital venue. This is a thorough explanation of how cybersecurity is used to control and lessen propaganda in Nigerian politics:

Propaganda models in Modern Politics

Various models of propaganda have been developed to understand its mechanisms and impact. Two key models are the Propaganda Model by Herman and Chomsky and the Agitation Propaganda Model.

i. Propaganda Model by Herman and Chomsky

a. Filters of Information

According to Herman and Chomsky, media output is screened using a variety of criteria, such as ownership, advertising, sourcing, flak, and prejudices against terrorism and communism. These filters aid in comprehending how the media represents the interests of influential groups over those of the general people.

b. Manufacturing Consent

According to the paradigm, elite policies are frequently legitimized by the mass media in democracies by shaping public opinion and emphasizing certain issues while downplaying others.

ii. Agitation Propaganda Model

The Agitation Propaganda model centers on the function of propaganda in galvanizing public opinion in support of a cause, frequently using emotive appeals and disinformation to instill a sense of crisis or urgency. It places a strong emphasis on using narratives, symbols, and slogans that appeal to the ideals and feelings of the intended audience and inspire people to take action.

Application of Propaganda models in Nigerian Politics

i. Media Ownership and Control

Nigerian media ownership is concentrated in the hands of a small number of extremely powerful people and organizations, much like Herman and Chomsky's concept. These proprietors frequently have political ties, which affect the bias and content of the media. Media outlets controlled by political supporters or politicians themselves are used as weapons during

election seasons to promote narratives that support their positions and disparage those that do not.

ii. Cyber Propaganda

The emergence of digital media has led to the considerable use of cyber propaganda in Nigerian politics. Politically charged content as well as misinformation are disseminated through social media sites. To sway public opinion and affect election results, strategies like bot amplification, troll farms, and fake news websites are used.

iii. Hybrid Warfare

In Nigerian politics, hybrid warfare combines cyberwarfare, propaganda, and traditional military strategies. Cyberattacks are used by political players and state operatives to sabotage opposition communication networks, steal confidential data, and start defamation campaigns. Narratives that obscure or justify these activities are created through propaganda, which frequently presents them as essential steps for maintaining stability or national security.

iv. Public Mobilization

Political campaigns in Nigeria are run using agitation propaganda. To mobilise support, populist rhetoric, emotional appeals, and feelings towards particular racial and religious groups are used. Posters, songs, and speeches are examples of propaganda items that are designed to stir up strong emotions and get people voting.

The antecedent of Propaganda and Misinformation in Nigerian Politics

a. **Use of Social Media**: In Nigeria, social media platforms have developed into effective instruments for political communication; these platforms are used, nevertheless to disseminate propaganda and misleading information which has the power to sway public opinion and affect election results. Many complaints surfaced during the 2019 elections about the propagation of false material on social media intended to discredit political opponents (Tekedia, 2021).

b. **Cybersecurity Measures to Counter Propaganda**: To stop the spread of misinformation, the Nigerian government and commercial sectors have realized that strong cybersecurity measures are necessary. This entails keeping an eye out for false information and fake news on social media and other digital platforms. Artificial intelligence (AI) and machine learning are two examples of tools and technologies that are being utilized more and more to identify and flag problematic content.

c. **Legislative Efforts**: Aiming to stop the dissemination of misleading material online, the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 has provisions. However, since the current legal framework is frequently viewed as insufficient to address the intricacies of digital misinformation, more targeted rules and regulations targeting misinformation SOand propaganda are required (Suleiman, 2023)

d. **Public Awareness Campaigns**: An additional crucial component of

cybersecurity in Nigerian politics is educating the populace about the perils of false information. The media, civil society organizations, and the government are among the stakeholders that have been involved in educating the public about how to spot and stay away from fake news. These efforts aim to increase citizens' digital literacy so they can evaluate internet material critically (Suleiman, 2023).

e. **International Collaboration**: Nigeria has been strengthening its cybersecurity architecture through cooperation with foreign partners. To exchange best practices and technology for thwarting digital disinformation involves collaborations with multinational IT businesses and international cybersecurity organizations. According to Nigerian Bulletin (2024), these kinds of partnerships are essential for combating the international character of propaganda and cyber threats.

f. **Cybersecurity in Election Monitoring**: One of the main goals of cybersecurity initiatives is to guarantee the integrity of voting procedures. Cybersecurity tools are used by independent organisations and election monitoring authorities to protect voter data and stop election results from being manipulated. These initiatives lessen the influence of misinformation and preserve public confidence in the voting process (Nigerian Bulletin, 2024).

Challenges of Propaganda and Misinformation in Nigerian Politics

i. **Technological Gaps**: Nigeria faces challenges related to technological infrastructure and the availability of skilled cybersecurity professionals.
ii. **Regulatory Gaps**: Existing laws need to be updated and new regulations introduced to effectively combat digital misinformation.
iii. **Economic Constraints**: Economic pressures can limit the resources available for comprehensive cybersecurity measures(Suleiman, 2023).

Opportunities in Propaganda and Misinformation in Nigerian Politics

i. **Growth of Cybersecurity Sector**: The increasing need for cybersecurity creates opportunities for job creation and the growth of cybersecurity firms.
ii. **Digital Literacy Initiatives**: Expanding digital literacy programs can empower citizens to combat misinformation.
iii. **Enhanced International Cooperation**: Leveraging international partnerships can help Nigeria adopt advanced technologies and strategies to address propaganda and cyber threats

Interrelation between Cybersecurity, Propaganda, and Hybrid Warfare

i. **Cybersecurity as a Shield against Propaganda in Hybrid Warfare**: In hybrid warfare, adversaries use cyber operations to infiltrate systems, steal sensitive data, and

spread propaganda. Robust cybersecurity measures are crucial to defend against these cyber threats and prevent the manipulation of public opinion and electoral outcomes. For example, protecting electoral systems from hacking helps maintain the integrity of elections and counters the impact of digital propaganda.

ii. **Propagation of Misinformation through Cyber Channels**: Cyber channels, particularly social media, are exploited to disseminate misinformation and propaganda. Cybersecurity strategies must include monitoring and counteracting fake news and disinformation campaigns. The spread of false information can destabilize societies, create panic, and undermine trust in institutions, which are key objectives in hybrid warfare.

iii. **Cyber Attacks as a Component of Hybrid Warfare**: Cyber-attacks are a core component of hybrid warfare. They can disrupt communication systems, financial institutions, and other critical infrastructure, amplifying the impact of propaganda campaigns. For example, a cyberattacks on a power grid combined with a propaganda campaign can create chaos and erode public trust in the government's ability to provide basic services.

iv. **Information Warfare**: Information warfare, a critical aspect of hybrid warfare, involves using cyber operations and propaganda to control the information environment. By hacking into media outlets or manipulating social media algorithms, adversaries can control the narrative and influence public perception. Cybersecurity efforts must therefore include safeguarding information integrity and ensuring accurate information prevails over manipulated content.

Strategic Implications of Propaganda and Misinformation in modern Politics

i. **Holistic Security Approach**: Addressing the interrelation between cybersecurity, propaganda, and hybrid warfare requires a holistic security approach. This includes not only technical defenses against cyberattacks but also measures to counter disinformation and strengthen societal resilience against propaganda.

ii. **International Collaboration**: Combating hybrid threats necessitates international collaboration. Nations must work together to share intelligence, develop common strategies, and enhance collective cybersecurity capabilities. This includes cooperation between governments, private sector entities, and international organizations.

iii. **Public Awareness and Education**: Raising public awareness about the nature of cyber threats, propaganda, and hybrid warfare is critical. Education campaigns can help citizens recognize and resist disinformation, thereby reducing the effectiveness

of propaganda and hybrid warfare tactics.

Impact of Propaganda and Misinformation on Nigerian Political Stability and Governance

i. **Erosion of Trust in Institutions**: Cyberattacks and propaganda campaigns can erode public trust in government institutions. For example, when electoral systems are compromised through hacking or when misinformation spreads about electoral fraud, citizens may lose confidence in the legitimacy of their political leaders and the electoral process.

ii. **Polarization and Social Unrest**: Propaganda and disinformation can polarize societies by amplifying existing divisions and creating new ones. By spreading false or misleading information, adversaries can incite social unrest and violence, leading to political instability. This has been evident in several countries where misinformation campaigns have exacerbated ethnic, religious, or political tensions.

iii. **Manipulation of Public Opinion**: The use of digital platforms for propaganda allows actors to manipulate public opinion on a large scale. This manipulation can skew political discourse, influence election outcomes, and undermine democratic principles. For instance, targeted misinformation campaigns can sway voter behavior by spreading false narratives about candidates or policies.

iv. **Destabilization through Hybrid Warfare**: Hybrid warfare strategies, which combine cyberattacks with traditional military tactics and propaganda, can destabilize nations. By targeting critical infrastructure, such as power grids or communication networks, cyberattacks can cause widespread disruption and panic. When coupled with propaganda, these attacks can weaken the government's ability to respond effectively and maintain order.

v. **Challenges to Policy Making**: The spread of misinformation and cyber threats can complicate policy-making processes. Governments may find it challenging to develop and implement effective policies when they are constantly defending against cyberattacks and combating false information. This can lead to ineffective governance and policy paralysis.

vi. **Increased Need for Cybersecurity Measures**: To protect political stability and governance, governments must invest in robust cybersecurity measures. This includes developing comprehensive cybersecurity policies, enhancing law enforcement capabilities, and fostering public-private partnerships to address cyber threats and disinformation.

vii. **Resource Allocation**: Governments may need to allocate significant resources to counteract the effects of cyberattacks and propaganda. This includes funding for cybersecurity infrastructure, public awareness campaigns, and

international cooperation efforts. Such resource allocation can strain public finances and divert attention from other critical areas of governance.

viii. **International Relations**: The use of cyber tactics and propaganda in hybrid warfare can strain international relations. Countries accused of engaging in such practices may face sanctions, diplomatic isolation, or retaliatory measures. Conversely, nations under threat may seek international support to enhance their cybersecurity and combat disinformation, leading to new alliances and partnerships

Case Studies of Propaganda, Cyber-Security in modern Politics

i. **Russian Interference in U.S. Elections**: Russia's alleged interference in the 2016 U.S. elections exemplifies hybrid warfare tactics. Cyber operations were used to hack into political party emails, while propaganda was spread through social media to influence public opinion and create discord.

ii. **Ukraine Conflict**: The conflict in Ukraine is another prominent example, where Russia has used a combination of cyberattacks, military force, and propaganda to achieve its strategic objectives. Cyberattacks on Ukrainian infrastructure and the dissemination of misleading information have been central to this hybrid warfare strategy.

iii. **Russian Interference in Western Elections**: Russia's alleged interference in the 2016 U.S. presidential election and other Western elections illustrates how cyberattacks and propaganda can undermine political stability and governance. These actions have led to significant political fallout, including investigations, sanctions, and increased polarization within affected countries.

iv. **Ukraine Conflict**: The ongoing conflict in Ukraine showcases the impact of hybrid warfare on political stability and governance. Russia's use of cyberattacks, coupled with military aggression and propaganda, has created a protracted crisis that continues to challenge Ukraine's political stability and governance structures

Policy Recommendations

i. **Enhance Cybersecurity Infrastructure**

- **Invest in Advanced Cybersecurity Technologies**: The government should invest in advanced cybersecurity technologies such as AI and machine learning to detect and mitigate cyber threats and misinformation campaigns.
- **Establish a National Cybersecurity Agency**: Create a dedicated agency responsible for coordinating national cybersecurity efforts, including monitoring and responding to cyber threats and managing cyber crises.
- **Regular Audits and Updates**: Conduct regular security audits and updates of critical

infrastructure to ensure they are protected against the latest cyber threats.

ii. **Strengthen Legal and Regulatory Frameworks**
   - **Update Cybercrime Laws**: Revise and update the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 to address emerging threats and incorporate specific provisions for combating misinformation and propaganda.
   - **Implement Data Protection Regulations**: Enforce data protection regulations to safeguard citizens' personal information and reduce the risk of data breaches that could be exploited for propaganda.
   - **Establish Penalties for Misinformation**: Introduce legal penalties for individuals and organizations that intentionally spread misinformation and propaganda, including fines and imprisonment.

iii. **Promote Public Awareness and Digital Literacy**
   - **Digital Literacy Campaigns**: Launch nationwide digital literacy campaigns to educate the public on identifying and avoiding misinformation. This includes training on verifying information sources and recognizing fake news.
   - **Collaboration with Media**: Work with media organizations to promote fact-checking and responsible reporting. Encourage media outlets to highlight misinformation and provide accurate information to the public.
   - **Educational Programs**: Integrate digital literacy and cybersecurity education into school curricula to prepare future generations to navigate the digital landscape safely.

iv. **Enhance Collaboration and Intelligence Sharing**
   - **Public-Private Partnerships**: Foster collaboration between the government, private sector, and academia to share intelligence on cyber threats and develop innovative solutions for combating hybrid warfare.
   - **International Cooperation**: Engage in international cooperation and partnerships to share best practices, receive technical assistance, and participate in joint cybersecurity initiatives.
   - **Regional Security Alliances**: Strengthen regional security alliances to coordinate responses to hybrid threats and enhance collective cybersecurity capabilities.

v. **Develop a Comprehensive Counter-Propaganda Strategy**
   - **Establish a Counter-Propaganda Unit**: Create a dedicated unit within the national cybersecurity agency to monitor and counteract propaganda and misinformation campaigns.

- **Real-Time Monitoring**: Implement real-time monitoring of social media and other digital platforms to detect and respond to misinformation quickly.
- **Proactive Communication**: Develop a proactive communication strategy to provide accurate and timely information to the public, countering false narratives and reducing the impact of misinformation.

vi. **Support Research and Development**
- **Fund Cybersecurity Research**: Allocate funds for research and development in cybersecurity technologies, focusing on innovative solutions to detect and prevent cyber threats and misinformation.
- **Academic Collaboration**: Encourage collaboration between academic institutions and industry to research the interrelation between cybersecurity, propaganda, and hybrid warfare, and develop effective countermeasures.
- **Innovation Hubs**: Establish innovation hubs and incubators to support startups and entrepreneurs working on cybersecurity solutions.

Implementation and Oversight

i. **Interagency Coordination**: Ensure coordination between various government agencies involved in cybersecurity, information, and national security to implement these policies effectively.

ii. **Regular Assessments**: Conduct regular assessments and reviews of the implemented policies to identify areas for improvement and adjust strategies as necessary.

iii. **Transparency and Accountability**: Maintain transparency in the implementation of these policies and hold relevant agencies accountable for their performance in enhancing cybersecurity and combating misinformation.

Summary of Findings

This article examines the intricate interrelation between cybersecurity, propaganda, and hybrid warfare. The analysis reveals several critical findings:

i. **Increased Digital Penetration and Vulnerability**: Nigeria's growing digital infrastructure and widespread use of social media have created new vulnerabilities. These platforms are frequently exploited for cyber operations and the dissemination of propaganda, making cybersecurity an urgent priority.

ii. **Role of Social Media in Propaganda**: Social media plays a pivotal role in the propagation of misinformation and propaganda. During political campaigns and elections, false information is often spread to manipulate public opinion, discredit opponents, and create social discord. The 2019 Nigerian elections highlighted the

extensive use of social media for these purposes.

iii. **Challenges in Cybersecurity Framework**: Nigeria's existing cybersecurity framework, including the National Cybersecurity Policy and Strategy (NCPS) 2021 and the Cybercrime Act of 2015, provides a foundational structure but is insufficient to address the sophisticated nature of current cyber threats. There is a need for more robust and comprehensive cybersecurity measures.

iv. **Impact of Hybrid Warfare**: Hybrid warfare, which combines conventional military tactics with cyber operations and propaganda, poses a significant threat to Nigeria's political stability. Cyberattacks on critical infrastructure, coupled with targeted misinformation campaigns, can destabilize the nation by creating chaos and eroding public trust in government institutions.

v. **Global Lessons and Relevance**: International examples, such as Russian interference in U.S. elections and the Ukraine conflict, illustrate the global relevance of these threats. These case studies provide valuable lessons for Nigeria, emphasizing the need for vigilance and proactive measures to counter hybrid warfare strategies.

vi. **Need for Comprehensive Policy Measures**: The findings underscore the necessity for Nigeria to adopt a multi-faceted strategy to combat these interconnected threats. Recommendations include investing in advanced cybersecurity technologies, updating legal frameworks, promoting digital literacy, fostering public-private partnerships, and enhancing international cooperation.

Conclusion

Nigeria's current cybersecurity framework, though evolving, requires substantial enhancement to address these multifaceted threats effectively. The National Cybersecurity Policy and Strategy (NCPS) 2021 and the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 provide a foundation, but gaps remain in legal provisions, technological capabilities, and public awareness.

The role of social media as a platform for propaganda is particularly concerning. The dissemination of misinformation can sway public opinion, disrupt electoral processes, and incite social unrest. Lessons from international case studies, such as Russian interference in Western elections and the Ukraine conflict, demonstrate the global relevance of these threats and underscore the need for a proactive and comprehensive approach.

To safeguard political stability and improve governance, Nigeria must adopt a multi-faceted strategy. Key policy recommendations include investing in advanced cybersecurity technologies, updating and enforcing robust legal frameworks, promoting digital literacy, fostering public-private partnerships, and enhancing

international cooperation. By implementing these measures, Nigeria can strengthen its resilience against cyber threats, mitigate the impact of propaganda, and effectively counter hybrid warfare tactics.

By enhancing cybersecurity measures, educating the public, and fostering international collaboration, Nigeria can protect its democratic processes, maintain public trust, and ensure stable and effective governance in the digital age.

Future Research Directions

i. **Advanced Cybersecurity Technologies and Applications**: Future research should focus on the development and application of advanced cybersecurity technologies such as artificial intelligence (AI), machine learning, and block-chain. These technologies can enhance threat detection, automate response processes, and secure critical infrastructure. Investigating how these technologies can be tailored to Nigeria's specific context and integrated into existing frameworks is essential.

ii. **Impact of Social Media Algorithms on Propaganda**: Understanding the role of social media algorithms in the spread of misinformation and propaganda is crucial. Research should examine how algorithms amplify certain types of content and explore methods to mitigate the spread of false information. This includes studying the effectiveness of algorithmic adjustments, user education, and platform policies in reducing the impact of propaganda.

iii. **Effectiveness of Legal and Regulatory Measures**: Evaluating the effectiveness of current legal and regulatory measures in combating cyber threats and misinformation is necessary. Future research could analyze the implementation and impact of the Cybercrime Act of 2015 and other relevant laws, identifying gaps and proposing enhancements. Comparative studies with other countries' legal frameworks could provide insights into best practices.

iv. **Public Perception and Behavioral Responses**: Investigating how the Nigerian public perceives cyber threats, propaganda, and hybrid warfare, and how these perceptions influence behavior, is important. This includes studying the effectiveness of public awareness campaigns and digital literacy programs in changing behavior and enhancing resilience against misinformation.

Hybrid warfare, propaganda, and cybersecurity in contemporary politics are essential to the tactics used by state and non-state actors to subvert democratic institutions, upset political equilibrium, and accomplish political goals. Comprehending their interaction and influence is essential for formulating efficient solutions to the

changing terrain of threats. These dynamics should be further investigated in future studies to shed light on new dangers and preventative measures.

References

Abubakar, I. (2020). Cybersecurity and the Integrity of the Electoral Process in Nigeria. Journal of Cybersecurity Studies, 4(1), 45-63.

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election, Journal of Economic Perspectives.

Arquilla, J., & Ronfeldt, D. (1996). The Advent of Netwar (Revisited). RAND Corporation.

Ayeni, T. (2019). Cyber Propaganda and Its Impact on the Nigerian Electoral Process, Journal of Information Warfare.

Benkler, Y., Faris, R., & Roberts, H. (2018). Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press.

Chiluwa, I., & Ifukor, P. (2015). War against Our Children, Stance and Evaluation in #BringBackOurGirls Campaign Discourse on Twitter and Facebook, Discourse & Society

CISA. (2020). Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov

European Commission. (2016). General Data Protection Regulation (GDPR). Retrieved from https://ec.europa.eu

European Union Agency for Cybersecurity. (2020). Cybersecurity in the EU: New Threats, New Trends. Retrieved from https://www.enisa.europa.eu

Fruhlinger, J. (2019). The OPM hack explained: Bad security practices meet China's Captain America. CSO Online. Retrieved from https://www.csoonline.com

Galeotti, M. (2016). Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right. Journal of Strategic Studies, 39(1), 1-24.

Herman, E. S., & Chomsky, N. (1988). Manufacturing Consent, the Political Economy of the Mass Media. Pantheon Books.

Johnson, M. E., & Goetz, E. (2007). Embedding Information Security into the Organization. IEEE Security & Privacy, 5(3), 16-24.

Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365-404.

Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.

Mueller, R. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. U.S. Department of Justice.

National Security Adviser. (2021). National Cybersecurity Policy and Strategy. Federal Republic

of Nigeria. Retrieved from https://www.nsa.gov.ng

Nigerian Bulletin (2024). Nigeria Breathes Easier as Tinubu Orders Immediate Suspension of Cybersecurity Levy Implementation.

Norris, P. (2019). Strengthening Electoral Integrity: The Pragmatic Case for International Assistance*. Cambridge University Press.

Nwachukwu, C. (2020). Disinformation in Nigerian Politics: The Role of Social Media. African Journal of Political Science, 15(2), 89-105.

Nye, J. S. (2011). The Future of Power. Public Affairs.

Olowu, D. (2021). Cybersecurity in Nigerian Governmental Operations: Challenges and Solutions. African Security Review, 30(1), 76-92.

Onapajo, H. (2014). Politics for God: Religion, Politics, and Conflict in Democratic Nigeria, Journal of African Elections.

Schiffrin, A. (2017). Media Capture and the Threat to Democracy. Columbia University Press.

Segal, A. (2017). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.

Suleiman (2023). Navigating the current state of the cybersecurity in Nigeria. Opportunities and and Challenges in 2023.

Tekedia (2021). The Updated Nigeria's National Cybersecurity Policy and Strategy.Available on https://www.tekedia.com/the-updated-nigerias-national-cybersecurity-policy-and-strategy/

U.S. Department of Defense. (2018). Department of Defense Cyber Strategy. Retrieved from https://www.defense.gov

Umejei, E. (2020). Media Ownership in Africa in the Digital Age: Continuity and Change. Palgrave Macmillan.

Valeriano, B., & Maness, R. C. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press.

Ventre, D. (2016). Cyber Conflict: Competing National Perspectives. Wiley