Weaponizing Connectivity: The Role of Social Media and Cyberspace in Modern Subversion

Daphne Damons
Laurel Shield Consultancy, Pretoria, South Africa

info@lauralshield.co.za

Abstract: The proliferation of social media has revolutionized modern warfare, transformed the nature of conflict and redefined the rules of engagement (Arquilla & Ronfeldt, 1993). The rapid evolution of social media platforms, with their speed and anonymity, has created complex tools with far-reaching impacts on global security and stability (Kaplan & Haenlein, 2010). The threat landscape has evolved significantly, shifting from traditional warfare to cyber operations short of war, which have significant implications for state power and global security. Thus, the traditional notion of warfare has undergone significant transformation with the advent of cyber operations and social media. As noted by Valeriano and Maness (2015). "Cyber warfare is a new and evolving form of conflict that is changing the way states interact with each other". Cyber operations short of war refer to the use of cyber-attacks, propaganda, and disinformation to influence the actions of other states or non-state actors without resorting to conventional military force. Hence, nations can exert their influence and act without resorting to conventional military force. This new reality has given rise to a theater of hybrid threats, which demands innovative strategies for counteraction (Giannopoulos, G., et al 2020). This article examines the weaponisation of connectivity, exploring how social media platforms and cyberspace are being leveraged as tools of modern subversion. Drawing on existing literature (Gladwell, 2010 & Morozov, 2011) and recent global events, this research investigates how state and non-state actors are exploiting social media to further their strategic interests (Loader & Mercea, 2011) as well as providing a framework for countermeasures making use of examples. The implications of these actions for global security and stability are also examined (Nye, 2011). By shedding light on this underexplored topic, this article aims to contribute to a deeper understanding of how roll connectivity is weaponized to use social media and cyberspace in modern subversion.

Keywords: Subversion, Cyber operations, Countermeasures, Social media, Conflict short of war

1. Introduction

Thomas Alsop (2023) highlighted the rapid adoption of Global Navigation Satellite System (GNSS) devices, which reached 6.5 billion units globally in 2021 and are forecasted to rise to 10.6 billion by 2031. This rapid and transformative technological evolution is characterized by unparalleled connectivity and innovation. This widespread adoption of GNSS technology has enabled the creation of complex surveillance systems that can track individuals' movements and activities. This extensive connectivity has created fertile ground for subversion, with social media emerging as a powerful instrument for propaganda and political warfare. Data collection through GNSS technology can be analyzed to identify patterns and trends in individuals' behavior, which can be used to inform surveillance and intelligence operations. The proliferation of social media significantly reduces the resources needed for information operations making it a cost-effective method to influence public opinion and destabilize societies.

In 2013, Edward Snowden, an employee at the Central Intelligence Agency (CIA) disclosed how the United States government through the National Security Agency (NSA) used the Internet to gain strategic advantage over nation-states (Paganini, 2013). Snowden reported that the NSA had led over 61,000 hacking operations worldwide, including many in Hong Kong and mainland China (BBC,2014). Indicating that the rules of warfare have moved from conventional? warfare to conflict short of war (Maschmeyer, 2022). This disclosure provides a clear indication that nation-states are making use of the connectivity of communication networks to gain strategic advantage over their adversaries, thus exposing the existence of a global surveillance infrastructure that enables the collection and analyses of vast amounts of data on individuals' activities. This is an indication that connectivity can be weaponized using social media platforms in modern subversion. Van Niekerk and Maharaj (2013) define social media as a subcategory of Web2.0 technologies, which include all connected social networks, weblogs and wiki's. The concept of social media platforms is centered on user generated content, online collaboration, and information sharing. For example, China's 50 Cent Party is an online group of online commentators who are paid to post pro-government content on social media platforms. King et al. (2017) in their study found that the 50 Cent Party was used to spread propaganda and misinformation on social media platforms during the 2024 Hong Kong protests?

Michel Foucault's (1926-1984) theory on power and surveillance provides a valuable framework for understanding Edward Snowden's whistleblowing and its implications for nation states/and mass surveillance. Snowden's revelations about mass government surveillance programs highlight the dynamics of modern power

structures which Foucault addresses in his work. The China 50 Cent Party's spread of misinformation as a form of power exercise, where the party seeks to shape public opinion and maintain control over the narrative provides an illustration of the dynamics of modern power structures . Foucault's theory on surveillance and discipline highlights the ways in which institutions and governments use surveillance to control and regulate behavior. This perspective assists in understanding how surveillance operates in the context of whistleblowing and misinformation. By examining the power dynamics, surveillance, and disciplinary power at play, we gain an deeper understanding of how power operates in the modern world.

McCombs and Shaw's AST (1972) theory on agenda–setting explains how media influences public opinion by setting the agenda for what issues are considered important. An example of this can be inferred in the actions of the Mozambican government's decision during the surge of violence after the elections to block social media access as a form of censorship and control over the flow of information which is directly linked to an agenda-setting theory, highlighting the media's power to shape public opinion. *The 2022 power grid sabotage was a cyberwarfare operation launched by Russia, especially the Sandworm group, to disrupt Ukraine's power grid, this was a perfect example of agenda-setting to influence and distort information*.

Power Dynamics and Agenda setting overlaps as both theories recognize the importance of power dynamics and the shaping of public opinion. In the context of social media disinformation and cyber operations, both theories can help us understand how power operates through the manipulation and the shaping of public opinion. The subversion of social media platforms involves the manipulation of these platforms to spread disinformation, propaganda, and malware.

This paper will examine the linkages between Snowden's revelation into connectivity and the implications of cyberwarfare in relation to manipulation of social media platforms.

2. Definition of Traditional and Modern Subversion and its Relevance

Subversion is the systematic attempt to overthrow or undermine a government or political system by moles working secretly from within (Merriam-Webster Dictionary). Traditional subversion is aimed at undermining social structures where "moles" are used to penetrate societies, groups, or organizations. A "mole" in this context is defined as "a person or thing that takes an active role or produces a specified, outcome". The effect of Subversion is indirect and covert (Maschmeyer~~,~~ 2023).

Modern subversion refers to sociotechnical structures of Information Communication~~s~~ Technologies (ICTs) embedded in modern technologies, to enable cyber operations. Even though the pursued structures differ, they both rely on subversive techniques of exploitation (Maschmeyer, 2023). The different search engines, social media platforms, and online news organizations, play an increasingly significant role in election integrity, civic discourse and group identity formation, which have physical impacts on peace and social cohesion (Maschmeyer, 2023). Social media platforms collect and analyze vast amounts of data on individuals' activities, which can be used to inform surveillance and intelligence operations.

Social media platforms and cyberspace have become key battlegrounds for modern subversion. These platforms can be used to spread disinformation, propaganda, and malware, thus inherently undermining social cohesion and political stability. Nations employ subversion through online mobilization~~:~~ Social media and online platforms can be used to mobilize people around a particular cause or ideology, potentially leading to social unrest, protests, or even violence.

3. Weaponizing Connectivity to Gain State Power

The extensive connectivity enabled by GNSS technology and social media platforms has created new opportunities for surveillance, subversion, and manipulation. The widespread adoption of social media platforms has enabled the conduct of information operations?, which can be used to manipulate public opinion and influence behavior.

The 2024, Mozambique elections is a good example of the significant role social media played and in recent?, Mozambique elections to assist the government to curb the surge of violent protest. Access Now reported that: "according to the BBC, Venâncio Mondlane – who lost the presidential election to Daniel Chapo of the ruling Frelimo Party, who was declared the winner on October 24 with 71% of the vote – insists he is the real winner and has been posting social media videos urging supporters to protest the results". These social media posts have caused violence and unrest, highlighting the potential for social media to be used as a tool for subversion and manipulation. Due to the surge in violent protest actions, the Mozambiquan government was forced to

block social media (Access Now, 2024). This action aided the government to gain control over their citizens that used social media platforms to mobilize protest actions.

Getimane D, et al, 2024, in their study, examined which social media platforms were used in Mozambique. The social media platforms were used to reach the supporters, this subversive agent had manifold effects on the societies in Mozambique. Highlighting Foucault's concept of power and knowledge to understand how cyber operations, including those conducted by states, shape and reinforce existing power dynamics. States can take possession of and control knowledge, particularly in the form of sensitive information and data as indicated in the case of Mozambique.

The 2022 power grid sabotage was a cyberwarfare operation launched by Russia, especially the Sandworm Group, to disrupt Ukraine's power grid. Mandiant year reported that during the power grid operation, a novel technique with little groundwork was used to subvert the power grid. The report indicated that "living off the land" techniques, were utilized during the attack. Namely, it is foregoing malware and using only existing functionality. Mandiant (2022) lead cybersleuth Dan Black has hailed this operation as the harbinger of a "new era" in cyber conflict. This incident highlights the vulnerability of critical infrastructure to cyber-attacks, which can be facilitated by increasing connectivity. The growing interconnectedness of critical infrastructure systems, such as power grids, creates new vulnerabilities that can be exploited by malicious actors (Farrel, Finnemore, 2023). The sabotage incidents demonstrate the potential for cyber-physical attacks, which can have devastating consequences for critical infrastructure and the individuals that rely on it. Social media platforms can play a significate role in the dissemination of distorted information and the shaping of public opinion during crises situation such as power grid sabotage. Disinformation and propaganda could be spread via social media platforms which can exacerbate the consequences of a crises undermining trust of a institution or nation state.

3.1 Weaponizing Connectivity: Context of the Snowden Revelations

Wyat (2019) places emphasis on the importance of information in developing strategies and influencing decision-making processes. The NSA's collaboration with international intelligence partners and its use of keyloggers to capture passwords and other real-time information demonstrates a classic example of subversion in cyber operations (Alhinnawi et al., 2015). This can be noticed during Snowden's revelations exposing the CIA's use of technology to influence and steer nations' decision-making processes.

3.2 Weaponization via Information Operations

Information operations — defined as "the integrated employment … of information-related capabilities in The theater of war with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries" — is a central component of Russia's Information Warfare strategy, Giannopoulos, G, et al (2020). In such situations, conflict is not declared overtly, and most activities are carried out below the threshold of conventional means. Thus, a nation's cyber power is evaluated by its ability to use digital technologies to achieve national and international objectives, particularly in defense and offense (Alhinnawi et al., 2015) as disclosed by Snowden.

This highlights the strategic dimension of cyber power in state power. The Snowden revelations highlighted the strategic importance of information in influencing decision-making processes and the role of technology in achieving national objectives. Cyber power is a critical component of state power, and nations are increasingly leveraging digital technologies to achieve strategic gains. Thus, the use of state power was evident in the Mozambique incident where the government blocked access to social media platforms, creating an opportunity for the government to shape the narrative and influence decision-making. In the case of the 2022 power sabotage, it influences decision-making by creating a sense of urgency and crises. This may lead to hasty decision-making that may not be in the best interest of the government or its citizens.

Traditional subversion has shifted into cyberspace, taking the form of cyberwar mechanisms of exploitation. Social media platforms have become a key battleground for information warfare, with governments and non-state actors using these platforms to exert influence and shape public opinion.

4. Review Process

The review process will focus on the act of cyberwarfare using social media platforms through spread of malware, opening fake profiles, social media spoofing and the like. Nation states and threat actors exploit vulnerabilities in technological systems and social media platforms' algorithms and design, making it essential to address these vulnerabilities. Hybrid threat actors are on the rise, creating complex, multi-layered threats

which combine cyber-attacks with disinformation campaigns, that require comprehensive countermeasures. Propaganda and misinformation are spread through the following means:

- Bot farms, that is automated accounts.
- Human operated accounts known as troll farms;
- Social media spoofing, which is fake social media accounts that mimic legitimate accounts;
- Phishing attacks are used to compromise the use of social media accounts through the distribution of malicious software (malware).
- AI-generated content are used as “Deep fakes”, to create fake video’s audio and images.
- Hybrid actors use hashtag hijacking, high jacking popular hashtags to spread disinformation as means of subversion:

Social media are monitored to identify and disrupt opposition movements as revealed by Snowden. The information gathered through monitored conversations can identify and disrupt opposition movements. It can also shape public opinions and influence policy debates. Government has a responsibility to educate citizens in the importance of media literacy and critical thinking skills, to effectively counter disinformation and propaganda.

5. Observations and Implications

The intersection of social media, cyberspace, and subversion has transformed the nature of modern warfare, enabling states and non-state actors to exert significant influence and intersect global stability. Subversion of social media is a significant threat to democracy, national security and individual privacy. Foucault’s theory on power and knowledge highlights the ways in which power operate through networks and relationships, which is relevant to understanding the subversion of social media platforms. On the other hand, Mc Combs theory on agenda - setting highlights the way media shapes public opinion. The use of bots, trolls and malware on social media is widespread and it is used to spread disinformation, propaganda and malware.

Governments are grappling with the emerging challenges posed by digitally enabled cyber operations, including the spread of disinformation and the use of deepfakes. The role of social media in modern subversion highlights the need for a comprehensive understanding of the complex relationships between governments, technology, and citizens' rights. Democracy is at risk and social media platforms can be used to influence public opinion and influence election outcomes.

The Snowden revelations support the growing body of research that traditional subversion has shifted into cyberspace, taking the form of cyberwar mechanisms of exploitation (Maschmeyer, 2023). This new era of warfare blurs traditional conflict boundaries, leveraging cyberspace's scale, speed, and secrecy to achieve strategic gains in conflict short of war (Maschmeyer, 2023). It puts the spotlight on the extent of government surveillance and the role of technology companies in facilitating surveillance operations. For example, in Mozambique, the decision to block social media access can be seen as a form of control and censorship. Nevertheless, the Mozambique government made a tough decision to block the social media platforms, to stop the public disorder and gain back stability in the country. This case is complex and showcases the need to study the relationship between governments, technology, and citizens' rights.

The intersection of social media, cyberspace, and subversion has transformed the nature of modern warfare, enabling states and non-state actors to exert significant influence and intersect global stability. Paterson, T., & Hanley, L.(2020) highlight how citizens questioned the election outcomes and sighted foreign interference in the electoral process outcomes. They attribute this interference in the democracy of nations to the continued failure of governments to grasp their ability to combat this emerging threat of the spread of disinformation and how to counter it. Digital tools such as ‘deepfakes’ are used to spread disinformation (Paterson, T., & Hanley, L, 2020) on social media platforms. Governments need to establish counter measures to ensure democracies are protected against the emerging challenges that digitally enable cyber operations to pose to its citizens.

As the use of Automated bots and human agents, amplify certain narratives, and create the illusion of grassroots support for a particular cause or ideology. Jonathan Ong & Jason Cabañes (2018) stated that “No technology has been weaponized as such an unpecedented global scale as social media”. The use of social media is very complex and ever-evolving (Maschmeyer,2023). Governments therefore need to keep abreast of the current events in a nation and drive the narrative to ensure that the democracy of a nation is upheld. The KGB, the Russian Intelligence Service has mastered the art of using social media platforms as tactics to exploit the Western media freedom of speech, to establish “agents of influence within media houses” (Maschmeyer,2023). In 2014,

Russian-backed separatists in Ukraine launched a disinformation campaign on social media, claiming that Ukrainian forces were committing atrocities against civilians. This campaign aimed to discredit the Ukrainian government and justify Russian intervention (NATO StratCom COE,2015).

Trollrensics (2024) a Dutch consulting firm revealed that "a vast coordinated network of accounts influenced public discourse on social networks in Germany and France ahead of the European elections [in June 2024]." According to the report, the Dutch delegation of the Socialists and Democrats group in the European Parliament, was instructed to open social media accounts to spread misinformation on anti-vax, anti-LGBT, and pro-Russian speech. The combination of an intensive information campaign, cyber warfare are considered as a test – case for Russia executing a new form of warfare where hybrid, asymmetric warfare, combining highly trained Special Operation Forces, play a key role (NATO StratCom COE,2015) .

6. Countering Hybrid Threats: A Policy Framework for Monitoring, Detection, and Assessment

A comprehensive policy framework is needed to monitor, detect, and assess potential threats, particularly in the context of hybrid warfare. Giannopoulos, G., et al, 2020 give guidance to suitable policy framework highlighting. Goverments need to invest in critical thinking and media literacy to assist individuals to make informed decisions. Seeking influence is not new, and trying to gain strategic advantage through subversion (Giannopoulos, G., et al, 2020) is advancing. The Snowden revelations in 2013 exposed the extensive surveillance capabilities of governments and intelligence agencies worldwide. However, the conventional reason (Giannopoulos, G., et al, 2020) is broken as the threat landscape has evolved from traditional war to cyber operations short of war. These disclosures highlighted the need for a comprehensive policy framework. Hybrid threats, which combine conventional and unconventional tactics, have become increasingly prevalent in modern conflict. These threats can emanate from state or non-state actors and may involve cyber-attacks, disinformation campaigns, or other forms of asymmetric warfare (Giannopoulos, G., et al, 2020). The threat landscape has evolved significantly, shifting from traditional warfare to cyber operations short of war.

This new reality has given rise to a theater of hybrid threats, which demands innovative strategies for counteraction. At the core of these strategies lies a framework comprising monitoring, detection, and assessment. This approach is underscored by research from Giannopoulos, G., et al (2020) and a study by Mercy Corps, emphasizing the importance of collaborative efforts and community engagement. Examples of Hybrid attacks are Cyber-attacks on critical infrastructure, such as power grids or financial systems.

6.1 Monitoring: A Collaborative Effort

Effective monitoring can no longer be achieved in isolation. Governments must collaborate with a wide range of organizations, including intelligence structures, civil societies, and community groups (Mercy Corps, 2019). This multi-stakeholder approach facilitates the sharing of information and resources, enhancing the ability to identify and counter hybrid threats. Community participation is a critical component of monitoring efforts

The Sentinel project's Una Hakika program in the Kenya's Tana Delta, for example, fights rumors that contribute to inter-ethnic violence. This program allows community participation to report, verify, and contribute to the development of strategies to address misinformation (Mercy Corps, 2019), spread through the various social media platforms programs like Una Hakika help to prevent inter-ethnic violence and promote social cohesion

6.2 Detection: Leveraging Technology and Human Intelligence

Detection is a crucial phase in the counter-hybrid threat framework. It involves leveraging technology, such as artificial intelligence and machine learning, to identify patterns and anomalies in data. Human intelligence, derived from community reports and social media monitoring, also plays a vital role in detection efforts.

6.3 Assessment: Evaluating the Severity of Hybrid Threats

Assessment is the final phase of the framework, where the severity of identified hybrid threats is evaluated. This involves analyzing the potential impact of the threat, as well as the intentions and capabilities of the actors involved. A comprehensive assessment enables decision-makers to develop targeted responses to counter the hybrid threat. Through applying this framework, nation-states contribute to building resilience, mitigating cyber operations, and enabling governments to develop regulatory frameworks to counter cyber operations efforts.

6.4 Building Resilience

Governments need to provide basic digital media literacy training, and education in online and offline awareness building. To provide a buffer against the weaponization of social media. For example, Sri Lanka has developed a digital story narrative. This platform is used to build storytelling skills as a means to balance opposing online speech, assisting citizens to become more accountable consumers of online information.

7. Mitigation

Governments need to have *can consider* scenario planning to minimize harm once weaponized information has already spread. For example, addressing online hate speech and establishing crisis and response plans. An example is the Kenya project Dangerous Speech Project's Nipe Uwell, which provided public information on perilous speech as well as instruments to report and eliminate such speech online during the height of election conflicts. Further research is needed to develop advanced analytical techniques for anomaly detection and pattern recognition. Examining the effectiveness of different countermeasures, such as fact-checking initiatives or social media platform regulation.

The revelations of the Snowden gave nations an understanding of government surveillance and the role of technology in shaping power dynamics. Thus, indicating how the use of GNSS technology for surveillance and tracking and its implications for individual privacy and autonomy. Thus, the need for a comprehensive framework to monitor, detect, and assess potential threats, particularly in the context of hybrid warfare. By leveraging this framework, governments and organizations can better counter hybrid threats and protect their interests. Ongoing research in this area can inform the development of more effective strategies for countering hybrid threats and enhance global security.

8. Recommendations for Future Research and Policy Interventions

Based on the articles reviewed by its event that more research is needed on how connectivity is used to spread disinformation to gain strategic advantage over nations. Research could investigate the impact of GNSS technology on individual privacy and autonomy and examine the ways in which governments and institutions use GNSS technology to exercise control over populations. Providing platforms for agenda setting to change the narrative in order to gain state power. Thus research should focus on examining the role of social platforms in shaping public opinion and influencing policy debates, Nations need to provide policy direction on countering disinformation narratives.

9. Conclusion

The various case studies in this article are clear indicators that Social Media Vulnerabilities are being exploited. Influencers and bot networks have the potential to shape public opinion and amplify disinformation campaigns. Psychological Manipulation Techniques are being used in disinformation campaigns to evoke emotional responses and influence decision-making. Hybrid Threat Actors' Tactics are combined in cyber-attacks with disinformation campaigns to create complex, multi-layered threats. The use of these tools indicate that media literacy and critical thinking skills to counter disinformation and propaganda effectively need to be developed. Several interventions can be considered: The Government needs to label suspicious content, allowing users to make informed decisions about what they share and engage with. Social media can require users to disclose the sources of the information they share, enabling users to determine the credibility of the content. Social media platforms can provide fact-checking trolls to help users to evaluate the accuracy of the information they share. Social media platforms can amplify disinformation and propaganda, allowing it to reach a wider audience and potentially influence public opinion. Influence on Decision-Making: social media can shape decision-making processes by creating emotional responses, influencing perceptions, and manipulating public opinion.

References

Alhinnawi, B. & Incze, Gáspár & Syed, Ekhtiar & Edel, D. & Priom, M.. (2015). The snowden revelations and their effects on european it--related decisions and decision--making processes. Proceedings of the 2015/16 Course on Enterprise Governance and Digital Transformation Accessed https://www.infosecinstitute.com/resources/general-security/how-edward-snowden-protected-information-and-his-life/

Alhinnawi, H., et al. (2015). The Impact of Snowden's Revelations on Cybersecurity. Journal of Information Security, 6(2), 147-155.

BBC, (2014) Edward Snowden: Leaks that exposed US spy program, accessed https://www.bbc.com/news/world-us-canada-23123964 Published, 17 January 2014

Cyberwarfare: Strategies, Threats, and Global Geopolitical Challenges Cyberwarfare: Strategies, Threats, and Global Geopolitical Challenges, https://blog.tixeo.com/en/cyberwarfare-strategies-threats-and-global-geopolitical-challenges/

Getimane, Domingos & Taula, Rui & Gonçalves, Bruno. (2024). Impact of news consumption on social media during the 2024 electoral campaign in Mozambique. Insight - News Media. 7. 668. 10.18282/inm668.

Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305

Johnson, T.A.. (2015). Cyber intelligence, cyber conflicts, and cyber warfare. 10.1201/b18335.

King, G, Pan, J & Roberst, M.E. (2017). How the Chines government fabricates distraction, not engaged argument. American Political review, 111(3)484 -501

Maschmeyer, L. (2022) 'A new and better quiet option? Strategies of subversion and cyber conflict', Journal of Strategic Studies, 46(3), pp. 570–594. Doi: 10.1080/01402390.2022.2104253.

Maschmeyer, L. (2023). Cyberwar and Strategic Subversion. Journal of Strategic Studies, 46(1), 34-51.

Maschmeyer, L. (2023). Subversion, cyber operations, and reverse structural power in world politics. European Journal of International Relations, 29(1), 79-103. Https://doi.org/10.1177/13540661221117051

Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes.' Australian Journal of International Affairs, 74(4), 439–454. Https://doi.org/10.1080/10357718.2020.1734772

Pierluigi P (2013) How Edward Snowden protected information … and his life Https://www.business-humanrights.org/en/latest-news/mozambique-government-shuts-down-access-to-social-media-messaging-sites-to-deal-with-post-election-protests/

Riga | 2015 ;ANALYSIS OF RUSSIA'S INFORMATION CAMPAIGN AGAINST UKRAINE; Examining non-military aspects of the crisis in Ukraine from a strategic communications perspective accessed russian_information_campaign_public_12012016fin

Wyat, S. (2019). The Importance of Information in Modern Warfare. Military Review, 99(3), 23-30.