MEMORANDUM

To: African Union
From: Aliyah Weiss
Date: November 2, 2024

Subject: Addressing the 2Africa Cable Crisis + Strategic Considerations for the African Union

Introduction: In the face of the unfolding 2Africa cable crisis, this memo outlines critical strategic considerations for the African Union to navigate the challenges posed. This includes Ghana, Nigeria, and South Africa's response to the FuzzyBear ransom demands as well as what action to take towards the Chinese government in light of the espionage allegations. It also will include whether to block access to Meta services in AU member nations and how. Lastly, what to do about the mysterious devices on 2Africa cable in certain countries, and whether to continue using the system.

1. **Response Plan for FuzzyBear Ransom Demands:**

Option 1: Pay Ransom

- Advantages: Fast solution, possibly avoids data leak
- Disadvantages: Expensive, encourages more ransom attacks, doesn't guarantee data protection

Paying the ransom is the fast solution if we want to sweep this under the rug. However, there is a chance FuzzyBear takes the money and still leaks the data anyways. It is an expensive risk to take, and will subsequently encourage them to request another ransom, creating an ongoing cycle of financial burden and potential data exposure that may undermine trust in our cybersecurity measures.

Option 2: Decline Ransom

- Advantages: Demonstrates resilience, discourages another ransom demand
- Disadvantages: Risk of data exposure, backlash from affected populations

Declining to pay the ransom is a bold decision that will show resilience and likely discourage FuzzyBear from requesting another ransom. They know the likelihood of being paid is low when it's already being avoided with such a large threat. However, the chances of them going through with the leak are high. The disadvantaged here are dealing with the damage of the leak, as well as disapproval from the communities affected, necessitating a proactive and transparent communication strategy to mitigate the impact.

Option 3: Negotiations and Diplomacy

- Advantages: Possibly reduce ransom

- Disadvantages: Unpredictable response from FuzzyBear and/or other countries, doesn't guarantee data security, time consuming

Engaging in negotiations and diplomacy may offer an opportunity to reduce the ransom, providing a potential middle ground. However, the response from FuzzyBear and other involved parties is unpredictable, introducing uncertainty into the resolution process. This option does not guarantee data security and is inherently time-consuming, requiring careful consideration of the potential risks and benefits before pursuing diplomatic avenues.

Suggested Action:

The best choice is to pursue option 2, declining to pay the ransom to FuzzyBear. Declining demonstrates a level of resilience and will discourage FuzzyBear from future ransom demands. It does leave a large risk of data exposure, however proactive measures can be taken to mitigate the aftermath of the potential leak. This includes openly communicating with the affected populations (Meta users), maintaining transparency, and implementing enhanced security. Anyone affected should be rewarded with a settlement similar to the Equifax breach in 2017, or the previous Meta (Facebook) data breach in 2019. These solutions allow us to focus on preserving public trust and long-term security while navigating the FuzzyBear leaks.

2. **Response to Chinese Government Espionage Allegations:**

Option 1: Formal Accusation and Sanctions

- Advantages: Conveys a strong message and can provoke international support
- Disadvantages: Escalates tensions, can lead to economic repercussions

Formally accusing the Chinese government of causing the leaks is an incredibly strong stance to take. This can be positive, as it will lead to many of China's adversaries, such as the US/UK, to join allyship with Africa. However, China's response is unpredictable. Ultimately, they most likely will not admit to it, and could instead punish Africa. Dismantling the cables they have funded would lead to internet black outs and severe punishments to the African communities affected. If they don't respond as extremely, tensions would still be high, potentially impacting diplomatic relations and economic partnerships.

Option 2: Diplomatic Channels and Investigation

- Advantages: Maintains diplomatic relationships, maintains stability
- Disadvantages: Unpredictable responses, time consuming, might not yield proof

Opting for diplomatic channels and investigation offers a measured approach to address the espionage allegations against the Chinese government. Diplomatic relationships and stability can be maintained by engaging in dialogue and cooperative investigation. This option allows for a thorough examination of the evidence, ensuring a comprehensive understanding of the situation before placing public blame. However, the responses from the Chinese government are unpredictable, and the process is inherently time-consuming. Despite potential challenges, this

option fosters an environment of collaboration and dialogue, aiming for a more nuanced and evidence-based resolution to the allegations.

Option 3: Public Denouncement

- Advantages: Avoids confrontation with China, maintains stability
- Disadvantages: Can appear weak, loss of trust from affected nations

Choosing to publicly denounce the situation without taking direct action against China presents a cautious strategy to avoid further escalation. Diplomatic relations and stability can be maintained by refraining from formal accusations. However, this approach may be perceived as weak, potentially diminishing credibility and trust among the affected nations. Addressing concerns in a transparent manner will allow the affected nations to understand the details of the scenario while still avoiding direct confrontation. This fosters an environment of open communication and mitigates potential diplomatic fallout.

Suggested Action:

The best choice is to pursue option 2, leveraging diplomatic channels and thorough investigations to approach Chinese government espionage allegations. This approach allows for careful examination of the evidence without impacting diplomatic relationships with China, as well as keeping regional stability. Despite it being a time consuming response, it seeks to gather concrete proof before taking action. This avoids any unnecessary conflict and allows communities to remain calm. Furthering allegations to accusations can be dividing and isolating Africa if it goes poorly. By fostering an environment of cooperation and understanding, a resolution can be reached that addresses the immediate concerns and establishes a foundation for future diplomatic collaborations.

3. **Blocking Meta Services in AU Member Nations:**

Option 1: Complete Restriction

- Advantages: Limits misinformation, panic, and is a quick resolution
- Disadvantages: Impacts entire country communication lines, can lead to public unrest

Opting for complete restriction by blocking access to Meta during this critical period offers a swift and decisive solution to limit the spread of misinformation and potential panic. However, such a measure significantly impacts the entire country's communication infrastructure, potentially leading to public unrest. While it effectively curtails the dissemination of unverified information, the repercussions of isolating citizens from global communication channels must be carefully weighed against the benefits.

Option 2: Partial Restriction

- Advantages: Controls information flow, mitigates some misinformation harm
- Disadvantages: Can be circumvented, can be perceived as censorship

Implementing partial restrictions on Meta services presents a balanced approach, allowing for controlled information flow to mitigate the harm caused by misinformation. While it provides a measure of control, this option has drawbacks, including the potential for users to circumvent restrictions and the risk of being perceived as engaging in censorship. Finding the right balance between mitigating misinformation and preserving open communication is essential for effective crisis management.

Option 3: No Restrictions

- Advantages: Avoids any consequences regarding information censorship
- Disadvantages: Potential harm to national security regarding misinformation

Choosing not to impose restrictions on Meta services avoids immediate consequences related to information censorship. However, this option poses potential risks to national security, as misinformation may spread during this period. Balancing the need for open communication with preventing the harmful effects of misinformation requires careful consideration and strategic communication efforts to mitigate the impact on public perception and national security.

Suggested Action:

The best choice is to pursue option 2, partial restrictions of Meta content. This approach strikes a balance between controlling the flow of information to mitigate the harm caused by misinformation and avoiding the extreme consequences associated with complete restrictions. By adopting a measured strategy, there is an acknowledgement of the importance of maintaining open communication channels while addressing the immediate concerns related to potential misinformation during this period. It is important, however, to complement these restrictions with a transparent communication strategy that keeps the public informed about the reasoning behind these measures, fostering a sense of understanding and cooperation to navigate the challenges posed by the crisis effectively.

4. **Continuing Usage of 2Africa Cable and Mysterious Devices**

Option 1: Investigate Technology while Encrypting Data

- Advantages: Identifies potential threats and informs future security measures
- Disadvantages: Time consuming and may yield no results, risk of data not being protected

Delving into the technology on the cables presents a comprehensive approach to addressing the mysterious devices. However, the investigation's time-consuming nature raises concerns, and the potential for yielding no results adds complexity. The ambiguous nature of these devices, whether they appear as unknown, deceptive spyware, or harmless elements, poses challenges to conclusive findings. In scenarios where the devices are indeed spyware, an ongoing investigation means continued cable usage, allowing potential data theft to persist. In this case, there should be

more encryption technology for all affected devices using the cables. If possible, the suspicious devices should try to be removed if proved to have no serious effect on usage.

Option 2: Suspension of Cable Usage

- Advantages: Avoids any data compromises and ensures safety
- Disadvantages: Disrupts internet connectivity, economic impacts

Opting for the suspension of cable usage is a decisive measure to ensure the safety of data and eliminate potential threats. However, this comes at the cost of disrupting internet connectivity, creating economic impacts in the regions connected by the 2Africa cable. While it guarantees the prevention of data compromises, the economic repercussions must be carefully weighed against the security benefits, necessitating a strategic and well-communicated approach to manage the impacts on affected communities.

Option 3: Continue Usage with Enhanced Security

- Advantages: Maintains connectivity and addresses security concerns
- Disadvantages: May not fully eliminate threats allowing risks to persist

Continuing the usage of the cable with enhanced security measures is a realistic approach that balances the need for connectivity with addressing security concerns. While maintaining internet connectivity, this option acknowledges potential risks persisting despite heightened security. The challenge lies in the effectiveness of these enhancements, as they may not fully eliminate the threats posed by the mysterious devices. A comprehensive evaluation of the enhanced security measures is crucial to ensure that the benefits outweigh the potential risks and that the 2Africa cable continues to serve its intended purpose securely.

<u>Suggested Action:</u>

The best choice is to pursue Option 1, which is to investigate the technology. While acknowledging the potential time-consuming nature and the uncertainty of yielding results, a thorough investigation into the mysterious devices is essential for identifying potential threats and informing future security measures. This approach provides an opportunity to comprehensively understand the nature and purpose of the devices, allowing for a more targeted and effective response. Simultaneously, encrypting continuing data traveling through the wires is a powerful tool to attempt protecting future data from being leaked. This method addresses immediate concerns while laying the groundwork for a secure and resilient cable system in the long term.

Conclusion:

The recommended approach for the African Union in responding to the 2Africa cable crisis involves strategic decisions on multiple fronts. Declining FuzzyBear's ransom demands showcases resilience, supplemented by proactive communication and security measures to manage potential fallout. Diplomacy and thorough investigation into Chinese government

espionage allegations aim to maintain regional stability and avoid unnecessary conflict. Implementing partial restrictions on Meta content maintains a balance between controlling misinformation and preserving open communication. The investigation into mysterious devices on the 2Africa cable emphasizes a comprehensive understanding for informed security measures, as well as extra protection with better encryption technology. This holistic strategy aims to address immediate challenges while laying the groundwork for a resilient digital infrastructure, requiring collaborative efforts and transparent communication for success.