2nd July 2024.

Ref No:2024/07/0202

Press Statement

The Potential of a Cyberattack on Ghana's 7th December Elections

The Africa Center for Digital Transformation (ACDT) wishes to address the public and all stakeholders on the potential cyber threats that may impact the integrity and security of Ghana's upcoming December 7th elections. As digital transformation continues to permeate all aspects of Ghanaian society, including electoral processes, the risk of cyber-attacks has become a critical concern that requires urgent attention and comprehensive strategies.

The hype surrounding cyber-attacks is often relegated to the realm of fiction in larger public conversations, and seems to paint a picture of some shadowy, omnipotent force that can flip votes, deny services, and bring the most advanced infrastructural devices of the world to a grinding halt.

The Africa Center for Digital Transformation (ACDT) is aware of the importance of December 7th elections and its significance on the country's development and that of the African continent. It is within this context that we take the issue of cyber-attacks seriously and consider it of national importance.

Ghana is barely five (5) months away from electing a new President and Members of Parliament. Whilst the public attention has been on ensuring a peaceful, free and fair election, improving the cyber defense readiness and raising cyber vigilance in countering cyber threats, both directly and indirectly, will be a strong force multiplier for the public and private sector, election stakeholders, and the general public. Cyber attacks during elections in West Africa have been agrowing concern, with several notable incidents reported in recent years:

1. Nigeria

In 2015 and 2019 Elections: During these elections, there were reports of cyber attacks aimed at the Independent National Electoral Commission (INEC). The attacks included attempts to hack into the commission's database and spread disinformation online. While some systems were compromised, INEC stated that these attacks did not affect the overall election results.

2. **Sierra Leone:**

In 2018 Elections: Sierra Leone experienced cyber attacks targeting the National Electoral Commission (NEC). These attacks aimed to disrupt the electoral process and manipulate public perception. The government took measures to enhance cybersecurity and maintain the integrity of the election.

3. **Ghana**:

Ghana faced cyber attacks on its Electoral Commission's website during the 2016 elections. In the 2020 elections, there were numerous cyber threats targeting the electoral process, prompting enhanced cybersecurity measures.
During 2016 Elections: Ghana's Electoral Commission (EC) website was attacked, leading to temporary shutdowns. The EC acknowledged the attack but stated that it did not affect the integrity of the election results .
Also in 2020 Elections: Ghana experienced a significant number of cyber threats targeting the electoral process. These included attempts to hack the EC's systems and other government websites. The National Communications Authority (NCA) and the Cybersecurity Authority worked to mitigate these threats, ensuring the elections proceeded without major disruptions
n on the potential cyber threats that may impact the integrity and security of Ghana's upcoming December 7th elections. As digital transformation continues to permeate all aspects of Ghanaian society, including electoral processes, the risk of cyber-attacks has become a critical concern that requires urgent attention and comprehensive strategies.

4. **Liberia**:

In 2017 Elections: During the presidential elections, Liberia experienced cyber attacks aimed at disrupting the election process. These included attempts to hack into the electoral commission's systems and spread disinformation. The government worked with international partners to address these threats andensure a fair election.

5. **Senegal**:

In 2019 Elections: Cybersecurity experts noted attempts to interfere with Senegal's electoral process through cyber attacks. These included phishing attacks, hacking attempts on the electoral commission, and disinformation campaigns.

These incidents underline the importance of robust cybersecurity measures to protect the integrity of the electoral processes in West Africa.

To the various political parties in Ghana, Win or lose, a breach of election systems may trigger collateral effects on public institutions, commercial victoryof political parties, and influence domestic interests and foreign policy relationships. In the face of heightened national security and business concerns,we provide research-backed statements to boost stakeholder awareness of the opportunities and risks of a 7th December cyber culture.

The 2020 elections saw the collection of voters' information, such as biometrics, photographs, digital ID numbers, and residential addresses, both contact and digital, become imperative. Privacy and data protection issues must be prioritized.

The question begging loud is how prepared we are to win the fight against cyberattacks on the electoral integrity of the 2024 elections.

Proactive Measures and Recommendations:

To mitigate these potential risks, ACDT recommends the following proactive measures:

1. **Strengthening Cybersecurity Infrastructure:** Investing in robustcybersecurity measures to protect electoral systems from cyber threats. This includes regular security audits, penetration testing, and ensuring the use ofupdated and secure software.
2. **Capacity Building and Training:** Providing comprehensive training for electoral officials and IT personnel on best practices in cybersecurity. This ensures that they are well-equipped to detect and respond to potential threats promptly.
3. **Public Awareness Campaigns:** Educating the public on recognizing and avoiding misinformation, and promoting digital literacy to help citizens identify credible information sources.
4. **Collaboration with International Bodies:** Engaging with international cybersecurity organizations and election monitoring bodies to adopt best practices and benefit from their expertise and resources.
5. **Incident Response Planning**: Developing and regularly updating incident response plans to quickly address and mitigate any cyber incidents that may occur.

The ACDT is committed to supporting the Ghanaian government, the Electoral Commission, and all stakeholders in ensuring that the December 7th elections are conducted in a secure, transparent, and credible manner. We urge all involved parties to prioritize cybersecurity as an integral part of the electoral process and work collaboratively to protect Ghana's democracy from cyber threats.

AFRICA CENTER FOR DIGITAL TRANSFORMATION (ACDT)
C/O P. O. BOX 4466
CANTONMENTS - ACCRA

Kwesi Atuahene
Executive Director
Tel: +233 266080904

For further information or inquiries, please contact on WhatsApp only: Divine S.K Agbeti: +447852588270| Evelyn Kwarteng: +233554327286| Simeon Mede: +233261829993.

End of Statement