Advanced Research on Information Systems Security

ARIS²
an
international journal

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Social Engineering as a Tool for Warfare: A Look at the 2022 Dollar Bill Rejection Hoax in Nigeria

Dauda Sule[a]*, Fredrick Ifeanyi Okonkwo[b], Kamaludeen Bature Shehu[a] Tajuddeen Muhammad Mashkur[a]

[a]Cyber Security Department, Air Force Institute of Technology, NAF Base, Kaduna, Nigeria
[b]Information and Communication Technology Dpt., Air Force Institute of Technology, NAF Base, Kaduna, Nigeria
[a]Email: daudas@gmail.com
[b]Email: ifeanyifredrick@afit.edu.ng
[c]Email: kamalbatureshehu@gmail.com
[d]Email: muhdtaju@gmail.com

Abstract

In November 2022, a blog went viral in Nigeria which claimed the United States of America was going to reject Dollar bills printed before the year 2021 as a means of curbing corruption in African countries where criminals and corrupt politician hoard the currency. It turned out to be a false tale but had resulted in a brief reduction in the exchange rate of the United States Dollar to the Nigerian Naira. This illustrated how fake news could influence events and attitudes in a country, in this case, there was an economic impact (positive for the country); however, other social engineering techniques have been used to manipulate citizenry of countries in recent times, like suspected Russian interference in the United States Presidential elections in 2016 which swayed public opinion in favor Donald Trump and his emergence as president. Social engineering can be managed and controlled by way of awareness training and programs.

Keywords: cognitive manipulation; fake news; hybrid warfare; propaganda dissemination; cyber security awareness

Citation: D. Sule, "Social Engineering as a Tool for Warfare: A Look at the 2022 Dollar Bill Rejection Hoax in Nigeria", ARIS2-Journal, vol. 3, no. 2, pp. 3–10, Dec. 2023.

DOI: https://doi.org/10.56394/aris2.v3i2.29

----

* Corresponding author. Email address: daudas@gmail.com

1. Introduction

Social engineering has come to become widely deployed by criminals and adversarial forces as a Launchpad for other cyber-attacks or even kinetic attacks; the reason for this being that it is easier and more cost effective to compromise (hack) a human than a secured (even if minimally) information system. The human element is the weakest link in an information system due to its inherent weaknesses. Social engineering involves the cognitive manipulation of the human element to make it do something it would ordinarily would not have done. Malicious actors have come to realize that social engineering makes it much easier for them to successfully carry out attacks against targets. Non-contact forms of warfare have become more common place; even kinetic attacks could be initiated or aided with social engineering (which is a non-contact technique for attacks). The combination of different attack types of modules known as hybrid warfare.

1.1. Social Engineering

Social engineering is the cognitive manipulation of targeted victims to manipulate them into doing something they would not normally do, in order to compromise the victim or victim's organization. The victim is manipulated to release confidential data, grant unauthorized physical access, removing security protocols and so on. The European Union Agency for Cybersecurity (ENISA) [1] defined social engineering as simply all the techniques used illegitimate intent to convince a target to reveal certain information or perform a specific action. There are different techniques that can be used to manipulate victims like phishing, bating, pretexting, shoulder surfing, tailgating, dumpster diving and so on. Phishing is the most commonly deployed form of social engineering [2].

Malicious actors are increasingly adopting social engineering to initiate their attacks as it is much cheaper and easier to deploy without the need for advanced hardware, software, or advanced technical know-how [3]. In physical conflict, like kinetic warfare, social engineering can be used by an adversary destabilize and demoralize troops on ground; a recent example was the deepfake video of the President of Ukraine asking his troops to surrender to the Russians [4]. A milestone in the use of social engineering in conflicts was Stuxnet; this was the first recorded case of a cyber-attack against physical infrastructure. Stuxnet destroyed centrifuges in the Iranian uranium enrichment plant in Natanz, which was an air-gapped facility (not connected to the Internet to avoid cyber-attacks), the worm infected the facility by way of external contractors who had their computers infected most likely by phishing, they became unwitting couriers of the worm [5]. Virtually all major cyber-attacks in recent times have been initiated and deployed by way of a social engineering method or the other.

1.2. Hybrid Warfare

Adaptive Mobile Security described hybrid warfare as a combination of overt military force with other means like diplomatic, economic, and technological to fight adversaries; that is a combination of both military and non-military means [6]. For example, the United States has economic sanctions against Iran, and used technology in the form of Stuxnet against them as well, a combination of different methods. Warfare in modern times is moving more and more into the hybrid sphere, not that it is new – propaganda dissemination and demoralization techniques have been deployed in the past. In the article, "The Word and the Sword" [7], the authors highlighted how a combination of civilian bombings and propaganda helped the allies defeat the Nazis in World War II by emphasizing the destruction and loss of the life inflicted by the allies on the Germans; including the BBC even reporting Nazi successes against the allies before the Nazis did, making the German public more inclined to listening to the BBC for "honest reporting". The result was that the German public were mores exposed to demoralizing news regarding their situation, resulting in increased opposition to the Nazis. This is an illustration of how a combination of physical attacks and reporting on the situation can result in swing the tide of events in a certain direction, the allies were initially targeting German military infrastructure unsuccessfully, but their change in tactics to demoralize the German populace was believed to have catalyzed their defeat of the Nazis [7]. Of course, the information or propaganda dissemination was a form of social engineering, applied to shift the perspective of the German public.

In recent times there have been social engineering techniques deployed to sway elections, like suspected Russian meddling the United States Presidential elections in 2016 by leaking data that painted the Democratic Presidential candidate in a bad light, resulting in the emergence of Donald Trump as President, data leaks unfavorable to French President Macron in 2021 [8]. These kinds of attacks involve fake news or information manipulation (a situation where actual real events are presented in a way to exert certain reactions) and can have far reaching national security consequences. WhatsApp restricted the number of recipients that could be forwarded a message to five due to lynchings in India based on false allegations of child abduction against certain individuals whose images were spread with the allegations which went viral [9].

1.3. The Nigerian 2022 United States Dollar Rejection Hoax

In the last quarter of 2022, there was a blog post in Nigeria that the United States would no longer accept Dollar bills printed prior to 2021 by the year 2023, the reason being that the move would checkmate billions of illegal dollars stashed in African countries by terrorists, drug dealers and other criminals, and especially corrupt politicians [10]. The news went viral on social media, and even some alternative news sites reported it, some claiming Reuters as the source, and even adding that the United States President had advised his counterparts in the United Kingdom and the European Union to take similar steps [11]. The blog also claimed that the decision was reached in November, 2022 at a meeting with the World Bank, International Monetary Fund and Governors of African Central Banks [12], which further helped it sound more believable as the Central Bank of Nigeria had announced a redesign of some denominations of the Nigerian currency to control currency in circulation, manage influence and counter counterfeiting, as well as similar motives to the alleged United States stance [11], also having a 2023 deadline for old notes. The news was later debunked as false, with the United States Treasury stating it was baseless [13]. The source and motive of the fake news is unknown, but its effect was felt, albeit temporarily.

The Naira (Nigeria's currency) gained strength against the United States Dollar as a result of the hoax. Apparently, those who were hoarding the Dollars heard the fake news and started bringing them out of hiding so as to avoid them becoming obsolete, incurring them huge losses; this resulted in decrease in the scarcity of the Dollar in the Nigerian economy and caused the exchange rate to drop against the Naira. The status quo on the exchange rate was restored shortly, probably as a result of it becoming widely known that it was a hoax.

1.4. Outlook

This article seeks to show how social engineering techniques that appear to be low level can have adverse effects on a nation in terms of security and warfare. The focus is on the 2022 Dollar rejection hoax that occurred in Nigeria and how it affected the country to buttress how such, and similar techniques can be used to bring a country to its knees.

2. Research Method

The work involves an overview and interpretation of the case study (the Dollar rejection hoax) to buttress the potential divesting effects of social engineering, especially fake news, in warfare based on observations. The work does not seek to discover the motive or source of the hoax, but rather focuses on the type of effect it had and how similar techniques can impact a country's security and stability. The work is quite limited by scanty data available on the case study and it effects, and it is also heavily based on assumptions.

3. Effect of the Dollar Rejection Hoax on Nigeria

The hoax had a short-lived positive impact on the Nigerian economy, however, there are somethings that should be taken into note:

- It was timed to correspond with the Naira re-design project of the Central Bank of Nigeria, which made it seem more realistic.
- It resonated among the elite as can be seen by the panic disposal of stockpiled Dollars.
- It spread wide within a relative short period of time, like wildfire.

The fake news claimed that the United States had sat with the Governors of African Central Banks, among others, at a time when the Central Bank of Nigeria was planning to withdraw some denominations of the Naira and replace them with new ones in a bid to improve the economy and counter criminal activity, as well as corrupt politicians and public servants. This made it appear as though the Central Bank of Nigeria was acting in line with the discussion supposed meeting with the United States, making the news more believable. The believability of the fake news increases its potential of spreading and being successful.

The elite and especially those believed to being hoarding United States Dollars started disposing the currency in their possession by exchanging the Dollar for Naira or depositing in commercial banks so as not to lose value. The elite are composed of the most educated members of the society and policy makers, who should have known better about such an issue. The news could have been something less easy to confirm its validity, in which case the response could have taken a longer time and probably have a more lasting effect.

The power of social media was well demonstrated in this case and the message continued to grow exponentially. The ability to spread like wildfire increases the possibility of the fake news being effective. The content can easily influence people on a large scale; hence can sway public opinion and actions.

It can be observed from the above that the hoax had some far-reaching effects on Nigerians, so one can imagine if it had been something more sinister – it could have had a more devastating effect. It can be assumed that the hoax was not carried out by an adversary of Nigeria, that the initiator did not have any serious malicious intent and there probably was not strategic planning involved. Notwithstanding the absence of a serious source and planning, it affected the economy of the country, albeit short-lived.

4. Weaponization of Fake News

Fake news can be used to cause damage to a nation, especially by exploiting social media, as could be seen in the case of the lynching's in India that led to WhatsApp limiting the number of recipients a message could be forwarded to [9], and also Russian meddling in other countries elections [8]. Fake news ca be used to sway public opinion in a way that adversely affects a country. It can come in the form of having more direct and obvious motives like exposing secrets of politicians towards elections, setting a demographic against another, and so on. It can also come in forms that the motive might not be directly obvious, like the Dollar rejection hoax, which if well planned strategically can have effects that might not be realized in the short run. The latter form of fake news can be more devastating.

An adversarial nation or organization can take advantage of existing issues and inequities within a country to strategically create a situation that would favor the adversary. In the United States of America, there had been the issue of police brutality and racial profiling leading to demands and protests to “defund the police”, in Nigeria there was also a similar situation of police brutality causing the “End SARS” protests. The United States had some states responding to the defund the police demands by reducing funding to the police, not surprisingly crime rates increased, and then the defunding's started getting reversed about a year later [14]. An adversary could simply take advantage of something like police brutality to justify withdrawal of police from strategic areas or defunding them to cause a spike in crime rate in a country, which can render the country greatly unstable and can affect the economy, and even stir the populace against the leadership. The adversary can diminish military capability of a country by spreading news emphasizing the defense budget, showing it is excessive while other sectors are suffering; suggesting that there are no real threats to the country and imply the budget is meant to line the pockets of corrupt politicians, defense manufacturers and contractors. This can lead to public outcry against defense spending resulting in major cuts, possibly reducing the size of the armed forces and their weaponry, in the long run the country's defense capabilities could greatly diminish giving the adversary an upper hand to successfully carry out direct physical attacks against the country.

Among the reasons for imposing economic sanctions against countries is to cause economic hardship on the citizenry which would motivate them to embark on regime change, believing the leadership is responsible for their woes – either at the ballot or by revolting. Economic sanctions can be viewed as a form of economic warfare. An adversary can adapt this goal of economic sanctions to social engineering, by damaging a country's economy causing economic hardship that can lead to demands for regime change or cause civil unrest. The adversary can spread fake news that promotes investments that in reality are not profitable, create elaborate scams like Ponzi schemes that will eventually render participants broke; if the adversary is very meticulous the country's treasury could even be successfully targeted with such phony investments and scams. Once economic hardships set in, the adversary again uses fake news to steer the citizenry into believing their leadership are solely to blame for the economic woes, inciting them to revolt. The political instability can cause division and weakening of the country targeted, that might be the end goal of the adversary, or they might carry out kinetic attacks knowing the country's defenses have been weakened.

It has been reported that the Iranian increased in using cyber-enabled influence operations as a result of their shortcomings in more technical cyber-attack capabilities [15]. These operations involve social engineering techniques aimed at boosting morale of their supporters and creating fear, loss of morale, instability, and tension among their adversaries; this being achieved by way of simple message spreading with minimal sophistication and cost.

4.1. Countering the Effects of Fake News and Social Engineering Attacks

The best defense against social engineering attacks is awareness. Training and enlightenment and the ingredients that can ensure effective awareness, which is still not foolproof. Training and awareness programs can be in the form of lectures, seminars, conferences and so on, but those have limited effect. It is better to inculcate practical training like gamification and simulation that demonstrate how social engineering attacks like fake news can be deployed and what they take advantage of, to help better understand what was taught theoretically by having a practical feel of it. Social engineering penetration tests, like phishing tests, can be organized. The shortfall of these awareness and training programs is that they are easy to deploy in an organization, but for the citizenry of a country it can be difficult to reach everybody. An approach is to use various communication media can be used to present how social engineering is carried out and its effects, for example TV and radio programs, edutainment, inculcation into the education curriculum at all levels from elementary to tertiary. This can be included in a national strategic policy as part of ensuring security in a nation.

5. Conclusion

Social engineering, and especially fake news, is a very potent weapon for warfare, as could be seen from the Dollar rejection hoax of 2022. The effect of this hoax was just the tip of the iceberg as far as such manipulative cognitive attacks go, but it had a significant impact, although short-lived. Cognitive attacks have been adopted as part of hybrid warfare to adversely affect adversaries, whether for kinetic attacks, economic sabotage, creating unrest or shifting public opinion.

Curbing the effects of social engineering attacks is easier done at organizational level with training and awareness programs, but at the national level it becomes more difficult. It can, however, be implemented be means of wide-ranging national policies to include it into communication media and the education curriculum; this would go a long way in minimizing the effects.

References

[1] European Union Agency for Cybersecurity, "What is Social Engineering?," ENISA, n.d.. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering. [Accessed 13 May 2023].

[2] Team Copado, "12 Types of Social Engineering Attacks to Look Out For," Copado, 2022. [Online]. Available: https://www.copado.com/devops-hub/blog/12-types-of-social-engineering-attacks-to-look-out-for. [Accessed 13 May 2023].

[3] A. Rudra, "Why Do Cyber Attackers Commonly Use Social Engineering Attacks?," DMARC, 2022. [Online]. Available: https://powerdmarc.com/cyber-attackers-use-social-engineering-attacks/. [Accessed 13 May 2023].

[4] J. Wakefield, "Deepfake presidents used in Russia-Ukraine war," BBC, 2022. [Online]. Available: https://www.bbc.com/news/technology-60780142. [Accessed 14 May 2023].

[5] S. Winer, "'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad," Times of Israel, 2019. [Online]. Available: https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/#:~:text=At%20the%20request%20of%20the,details%20told%20the%20news%20site.. [Accessed 14 May 2023].

[6] Adaptive Mobile Secuirty, Spectrum of Violence: Mobile Network Enabled Attacks in Hybrid Warfare, Adaptive Mobile Secuirty Ltd, 2022.

[7] H.-J. Voth, R. Enikolopov, M. Petrova and M. Adena, "The sword and the word: How Allied bombing and propaganda undermined German morale during WWII," CEPR, 2020. [Online]. Available: https://cepr.org/voxeu/columns/sword-and-word-how-allied-bombing-and-propaganda-undermined-german-morale-during-wwii. [Accessed 14 May 2023].

[8] J. Hakala and J. Melnychuk, Russia's Strategy in Cyberspace, Latvia: NATO Strategic Communications Centre of Excellence, 2021.

[9] A. Hern, "WhatsApp to restrict message forwarding after India mob lynchings," The Guardian, 2018. [Online]. Available: https://www.theguardian.com/technology/2018/jul/20/whatsapp-to-limit-message-forwarding-after-india-mob-lynchings. [Accessed 14 May 2023].

[10] I. Onuba, "FACT CHECK: Reports Of US Plan To Reject Dollars Printed Before 2021 FALSE," The Whistler, 2022. [Online]. Available: https://thewhistler.ng/fact-check-reports-of-us-plan-to-reject-dollars-printed-before-2021-false/. [Accessed 14 May 2023].

[11] E. Ogunbamowo, "False! US not planning to reject dollar notes printed before 2021," Dubawa, 2022. [Online]. Available: https://dubawa.org/false-us-not-planning-to-reject-dollar-notes-printed-before-2021/. [Accessed 14 May 2023].

[12] H. Hussaini, "Is The US Planning To Reject Bills Printed Before January 2021?," Daily Trust, 2022. [Online]. Available: https://dailytrust.com/is-the-us-planning-to-reject-bills-printed-before-january-2021/. [Accessed 14 May 2023].

[13] B. J. Frank, "Fact check: Billions of pre-2021 US dollars will remain valid currency after January 2023," USA Today, 2022. [Online]. Available: https://www.usatoday.com/story/news/factcheck/2022/11/24/fact-check-false-claim-pre-2021-us-dollars-invalid-2023/10740604002/. [Accessed 14 May 2023].

[14] Z. Elinson, D. Frosch and J. Jameson, "Cities Reverse Defunding the Police Amid Rising Crime," The Wall Street Journal, 2021. [Online]. Available: https://www.wsj.com/articles/cities-reverse-defunding-the-police-amid-rising-crime-11622066307. [Accessed 14 May 2023].

[15] Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect, "Microsoft, 2023.