BOOK CHAPTER | Extreme Violence Using Phones

Cyberterrorism Using Smart Phones

Tseh Richard Divine
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: richard.tseh@st.gimpa.edu.gh / tsehdivine@gmail.com
Phone: +233270322787

ABSTRACT

The explosive expansion of smart phones causes massive information security breaches. Smart phones are tempting targets and elements for attackers due to their popularity and lax security [6]. Government of Ghana should make a determined effort to promote youth awareness and foster patriotism. Multi-agency counter-cyber operations and techniques should also be included in a nation-wide strategy curtail this menace. This paper seeks to explore cyberterrorism using smart phones and counter measures in Ghana.

Keywords: Africa, Ghana, Cyberterrorism, Information Security, Multi-Agency, Terrorists

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Tseh Richard Divine (2022) Cyberterrorism Using Smart Phones
SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 41-50. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P7

1. INTRODUCTION

Cyber security is the practice of protecting computer systems, networks, and data from malicious attacks. The term applies in a variety of contexts, from business to mobile computing. Network security is the practice of securing a computer network from intruders. Information security protects the integrity and privacy of data, both in storage and in transit [5]. Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone.

This figure is more than double (112%) the number of records exposed in the same period in 2018 [4]. Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Threats from cyberspace includes: Cybercrime which refers to individuals or groups who attack systems for monetary gain or to cause disruption. Politically motivated information collection is common in cyber-attacks.

Cyberterrorism aims to induce panic or fear by undermining electronic systems. The number of new vulnerabilities in mobile operating systems increased by 42 percent between 2009 and 2010 [1]. Operating systems for mobile phones are not updated as frequently as those for PCs [28]. As a result, smart phones are being used for cyberterrorism as a result, government data has been lost, critical national infrastructure been attacked, and financial institutions have continued to lose money.

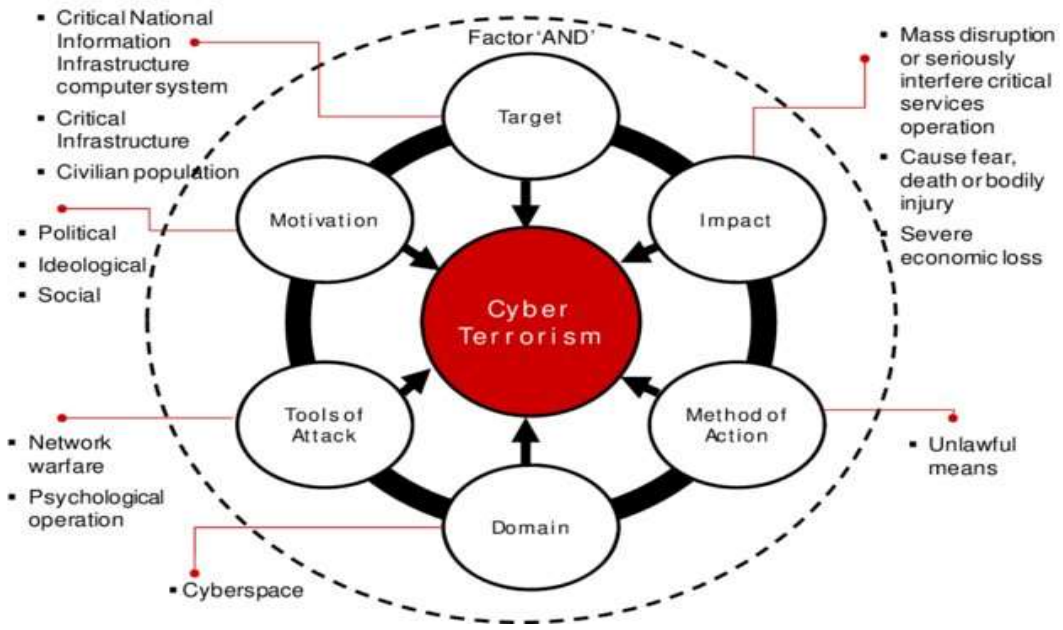

Fig 1: Perception on Cyber Terrorism: A Focus Group Discussion Approach
Source:https://www.researchgate.net/publication/267960005_Perception_on_Cyber_Terrorism_A_Focus_Group_Discussion_Approach/figures?lo=1

1.1 Background to the Study

The threat from cyberterrorism comes from a wide range of sources, including social, economic and political instability, and foreign occupation [25]. Terrorist attacks and the associated casualty rates mostly lie outside the Western sphere. A disproportionate number of terrorist incidents coincide with those regions in open conflict, or state disintegration and low development. The most recent data for 2015 is sympathetic with this long-term observation of terrorist violence [26]. Smart phones, which are mobile phones with advanced capabilities similar to those of personal computers (PCs), are becoming more common in people's pockets, handbags, and briefcases [28]. Because of their widespread use and insufficient protection, smart phones have become appealing targets for hackers. Smart phones have outsold PCs for the first time, according to a survey published earlier this year, and attackers have been taking advantage of this growing market by combining old and new approaches.

According to Symantec, one example is this year's Valentine's Day attack, in which attackers propagated a mobile picture sharing program that sent premium-rate text messages from the user's phone invisibly. According to one report, the number of new vulnerabilities in mobile operating systems increased by 42 percent between 2009 and 2010 [1].

Report on the number and sophistication of attacks on mobile phones is increasing, and countermeasures are lagging behind [27]. Smart phones and personal digital assistants (PDAs) allow users to access email, the internet, GPS navigation, and a variety of other apps from their mobile devices. Smart phones security, on the other hand, has lagged behind that of traditional computers. Mobile phones lack technical security features such as firewalls, antivirus and encryption. Operating systems are not updated as frequently as those on personal computers. Mobile social networking apps save a variety of personal information to mobile websites and mobile-based services. Users can also store sensitive data on the devices.

2. RELATED LITERATURE

Next we provide a tabulated outlook of related works and their findings

Table 1: Tabulation of Related Works

Focus	Authors	Findings
Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem.	Charlton, C.	This article provides analysis on a potential emerging trend in terrorism and cyber terrorism. It reports a brief interview with the director of the Atlantic Council's Strategic Foresight Initiative, Dr. Matthew Burrows, which highlights a potential transformation in terrorist operations with the influx of digital natives. These digital natives are likely to prefer cyber and cyber kinetic attacks over the traditional real-world attacks to meet their organisation's goals [11].
Cyber Attack Causes Second Power Grid Outage in the Ukraine in the Past Yea	Cimpanu, C.	This article describes the December 17th, 2016 cyber-attack against the Ukrainian energy company, Ukrenergo. This attack affected the area surrounding Kiev. It left the affected region without power for 45 minutes and forced operators to switch to manual mode after 75 minutes. The attack is reminiscent of the December 2015 hacks, also allegedly carried out by Russian hackers. The incident shows that extended attacks against Critical Infrastructure are possible and can be carried out remotely [12].
Securing the Skies: Cyber security in aviation.	Davis, D.	This article discusses the potential of hacking and hijacking planes. A researcher was arrested for gaining access to the planes' control system through a connection in his in-flight entertainment system. During his hack, the researcher had caused the plane to climb and perform a lateral movement. The article also reports that a number of industry and government efforts are underway to ensure the security of aircraft from cyber influences [13].

Focus	Authors	Findings
German nuclear plant infected with computer viruses, operator		This article reports that the Gundremmingen nuclear power plant in Germany has been found to be infected with computer viruses. The viruses are not able to pose a threat to the facility because it is isolated from the Internet. The malware is believed to have been spread through removable data drives such as USB sticks and mobile phones. The malware infections are not typically dangerous unless key machinery had been specifically targeted. The article also states that a 'European aircraft maker' cleans its cockpits computers of malware designed for Android phones every week. The malware had only been spread to the computer because the factory employees were charging their phones with the cockpit USB ports. The planes are not affected by the malware because they run on a different operating system [18].
Attackers Alter Water Treatment Systems in Utility Hack: Report.	Kovacs, E	This article discusses how attackers were able to gain access to the 'Kemuri Water Company' (KWC) by exploiting the outdated and poorly secured Internet-based operational technology. The attackers had gained access to the Operational Technology Programmable Logic Control systems on four separate occasions in the 60-day period leading up to the assessment by Verizon. During two of these intrusions the attackers were able to manipulate the system to impair the treatment and production capabilities of the plant [16].
New Malaysia Airlines Flight MH370 'Cyber Hijack' Theory Emerges After 'Vulnerabilities' Found in Inflight System	Ross, P.	This article entertains the possibility of Malaysia Airlines Flight MH370 being lost due to cyber hijacking. The theory is credited to British anti-terror expert, Sally Leivesley, who states that cyber terrorists could have hacked the plane through its-inflight entertainment system. She further states that the Boeing 777's speed, direction and altitude may have been changed using radio signals sent from a small device [17].

Focus	Authors	Findings
Cyber Threats to Mobile Phones	Paul Ruggiero et al	According to a report published earlier this year, smartphones recently outsold PCs for the first time, and attackers have been exploiting this expanding market by using old techniques along with new ones. One example is this year's Valentine's Day attack, in which attackers distributed a mobile picture-sharing application that secretly sent premium-rate text messages from the user's mobile phone. One study found that, from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped to 42 percent. The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up [1].
PLC-Blaster: A Worm Living Solely in the PLC	Spenneberg, R.et al	This report discusses the worm that attacks Siemens SIMATIC S7-1200 PLC controller without relying on any additional PC to proliferate. The worm operates solely on the PLC system and scans networks for new targets to infect. The worm is written in the PLC coding languages, *Structured Text*. Their worm was tested on a closed system; it was discovered that it could not be detected by any current antivirus product. A virus comparable to Stuxnet is well within the resources of private firms to create. It is therefore likely that a terrorist or criminal organisation can acquire the resources necessary to create a virus such as PLC-Blaster or Stuxnet [28].
Cyber Attacks on The Ukrainian Grid: What You Should Know	FireEye.	This document by the cyber security firm, FireEye, provides a case study for how future cyber terrorism and warfare attacks might be executed. It outlines the methods used by the Russian backed 'Sandworm team' to cause the December 2015 Ukraine power outage. The document shows that hackers gained access through a spear phishing campaign using the 'BlackEnergy3' malware, a version of the 'BlackEnergy' and 'BlackEnergy2' malware used exclusively by the Russian backed 'Sandworm team'. The attackers also used a killdisk program to wipe both control and non-control systems. The attackers also overwhelmed the Ukrainian utility call centres with automated telephone calls (a TDoS) in order to inhibit the utilities' ability to respond to the crisis. The document recommends several methods of protecting utilities including: reviewing SCADA/ICS security architecture; enhancing network security monitoring capability; searching for indicators of compromise; and reviewing incident response plans [14].

3. RESEARCH GAPS/FINDINGS

Smart phones lack effective counter measures to prevent cyberterrorist usage for their activities [7]. Training is needed to close the capacity gap that has been identified within the ranks of security agencies to counter cyberterrorism in Ghana. Such training should be conducted in a multi-agency framework, such as NIS cybersecurity framework, for maximum effectiveness [1]. It should have included elements from the judicial and security services, such as the cyber police units of Ghana police service, the Economic and Organised Crime Office staff, the Military Intelligence Units of the Ghana army, the media, and individual cybersecurity experts in Ghana. Cybersecurity awareness is the most powerful weapon when it comes to cyber defence tactics based on security issues that are vital to counter cyberterrorism in Ghana and in Africa.

It is suggested that the African Union and the Government of Ghana make a concerted effort to raise awareness and foster patriotism among the youth. This can be accomplished through e-learning programs offered by schools. The media can be utilized to raise awareness on rare occasions. Knowing their responsibilities, internet technology users will be able to take advantage of services on the internet while also helping to protect Ghana from cyberterrorists threats. This paper strongly suggests that all entities of state managing critical national infrastructure build cyber risk frameworks in order to assess their compliance with laws, regulations, and best practices relating to cyber risk, such as designing personalized cyberterrorism response plans to safeguard these critical assets [15].

4. CONCLUSION

This paper has highlighted the issues that Ghana faces on a daily basis in its digitalization agenda drive to ensure the safety of critical national infrastructure due to smart phone usage for cyberterrorism activities. It has also shown several flaws in the overall cybersecurity measures and plans; the knowledge presented can be used as a foundation for developing policies that promote safe cyberspace usage while also improving national and continental cybersecurity. It is necessary to incorporate academia in research and development (R&D), as well as innovation, in order to build acceptable computer and smart phone security that is both simple to use and inexpensive.

5. RECOMMENDATION FOR POLICY AND PRACTICES

Recommendations

This research on the impact of cyberterrorism and smart phones has revealed realities and gaps that are inherent in the overall impacts on the effectiveness of cybersecurity measures and strategies in some cases [9]. The nature of the environment in which cybersecurity agents operate is not a typical one, and accusations are sometimes directed at security agents without proper appreciation by the accusers of the background details. The only way to close this gap is to address it through policy. According to the findings, there is a need to raise awareness of cyberterrorism threats and related risks to individuals, organisations and all government agencies in Ghana. Further, counter measures for smart phones vulnerabilities should also be address through policy and technology [10].

Policy Recommendation

The necessity to safeguard nations from cyberterrorism threats in relation to the usage of smart is intended at ensuring that individuals, organizations, and governments are free to pursue their goals in a peaceful and secure environment. The point of departure is in the method and mechanisms for achieving this, despite the fact that cybersecurity is a global responsibility and that there is a need for collaboration with stakeholders from across the globe to improve capacity in dealing with cyberterrorism threats [2].

Furthermore, educating employees about cybersecurity threats and the security of their mobile devices is an important part of the policy that should be in place. The strategy should also be broadened to include multi-agency counter-cyber actions and tactics that take into account worldwide best practices from organizations and other stakeholders. Such measures should be long-term in nature and aimed at raising cybersecurity awareness. The use of intelligence to drive actions should be mainstreamed in the international approach to cybersecurity. To assess the relationship between the use of smart phones for cyberterrorist activities and the adoption of strategies, a comprehensive policy with an effective monitoring and evaluation mechanism should be put in place. The policy is to have activities and programs that bring the two parts together in order to reduce the level of mistrust and suspicion [3].

6. DIRECTION FOR FUTURE WORKS

The focus of the research was on threat of cyberterrorism in Ghana employing smart phones. The findings are given in the context of asymmetric cyberterrorism threats to national security, which is a prevalent cliché. The threat appears to defy all available techniques and countermeasures. There is a widespread lack of empirical studies on cyberterrorism and its security ramifications. This has resulted in the loss of government data, while financial entities continue to record money losses [4]. In situations where it is necessary to conduct research on homegrown solutions based on the local context. These are topics that have been overlooked and may require additional research to determine how they play out in the context of cyberterrorism and the use of social media [8].

7. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Cyber-threats are becoming more prevalent among African businesses and consumers. This pattern emphasizes the significance of bolstering cybersecurity defences. This means that businesses must raise their investment in cybersecurity technologies, offer personnel with cybersecurity training, and hire specialists such as CISOs. It's also critical to raise customer awareness about cybersecurity. Policymakers on the continent should concentrate on raising public knowledge of cybersecurity practices and improving regulatory and enforcement capacities. Regulations mandating firms to take effective cybersecurity precautions should be introduced and amended. Initiatives should also focus on improving law enforcement capabilities to increase the certainty of punishment for cybercriminals in Africa [24].

Before I wrap up, I would like to recommend a few potential study directions. According to previous studies, cybercrime targeting developing economies, such as those in Africa, is concentrated in specialized industries. China's online gaming and e-commerce industry, Brazil's banking and financial sector, and India's offshore outsourcing sector are all examples [22,23].

Scholars should analyse and contrast economic sectors experiencing high-profile cyberattacks in major African economies with those in non-African developing economies in future conceptual and empirical studies [24].

Some supranational bodies, such as the African Union Commission (AUC), have expressed an interest in combating cybercrime. African economies, on the other hand, differ greatly in their efforts. Examining the causes of cybercrime-related legal and regulatory frameworks in African economies could be a second focus of future research. Various actors are active in the fight against this crime, including supranational and private sector entities. Businesses and individuals are upgrading their technological and behavioural security measures to protect themselves [24].

REFERENCES

1. Cyber Threats to Mobile Phones - CISA
   https://www.cisa.gov/uscert/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf
2. Cybercrime and Cyber Terrorism | Disasters - ReadyNH.gov
   https://www.readynh.gov/disasters/cyber.htm
3. Legal Digest Searches Incident to Arrest in the Smartphone Age
   https://leb.fbi.gov/articles/legal-digest/legal-digest-searches-incident-to-arrest-in-the-smartphone-age
4. The use of the Internet for terrorist purposes
   https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
5. Defining cyberterrorism
   https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005
6. Mobile-Devices--The-Case-for-Cyber-Security-Hardened-Systems
   https://www.researchgate.net/publication/282121258_Mobile_Devices_The_Case_for_Cyber_Security_Hardened_Systems
7. Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smart Phones
   https://www.researchgate.net/publication/255965434_Cyber_Security_and_Mobile_Threats_The_Need_For_Antivirus_Applications_For_Smart_Phones
8. Cybercrime is moving towards smartphones – this is what you could do to protect your company
   https://www.cyberdb.co/cybercrime-is-moving-towards-smartphones-this-is-what-you-could-do-to-protect-your-company/
9. Cyber terrorism handling in Indonesia
   https://cberuk.com/cdn/conference_proceedings/conference_30092.pdf
10. Cyber Terrorism
    https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2984101
11. Charlton, C. (2017, January 28). Armchair Warriors: Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem. *The Sun.* Retrieved from https://www.thesun.co.uk/news/2643688/cyber-terrorism-attacks-threatlevel-isis-facebook-energy/

12. Cimpanu, C. (2016, December 20). Cyber Attack Causes Second Power Grid Outage in the Ukraine in the Past Year. *Bleeping Computer.* Retrieved from https://www.bleepingcomputer.com/news/government/cyber-attack-causes-second-power-gridoutage-in-the-ukraine-in-the-past-year/
13. Davis, D. (2016, August 23). Securing the Skies: Cyber security in aviation. *CSO*. Retrieved from http://www.csoonline.com/article/3111448/internet-of-things/securing-the-skies-cybersecurity-inaviation.html
14. FireEye. (2016). *Cyber Attacks on The Ukrainian Grid: What You Should Know*. Milpitas, CA, United States of America. Retrieved from https://www.fireeye.com/content/dam/fireeyewww/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf
15. Konstantas, J. (2016, April 19). Dam Hackers! The Rising Risks to ICS and SCADA Environments. *Security Week*. Retrieved from http://www.securityweek.com/dam-hackers-rising-risks-ics-andscada-environments
16. Kovacs, E., (2016, March 22). Attackers Alter Water Treatment Systems in Utility Hack: Report. *Security Week*. Retrieved from http://www.securityweek.com/attackers-alter-water-treatmentsystems-utility-hack-report
17. Ross, P. (2014, March 16). New Malaysia Airlines Flight MH370 'Cyber Hijack' Theory Emerges After 'Vulnerabilities' Found in Inflight System. *International Business Times.* Retrieved from http://www.ibtimes.com/new-malaysia-airlines-flight-mh370-cyber-hijack-theory-emerges-aftervulnerabilities-1561723
18. Steitz, C. & Auchard, E. (2016, April 27). German nuclear plant infected with computer viruses, operator says. *Reuters*. Retrieved from http://www.reuters.com/article/us-nuclearpower-cybergermany-idUSKCN0XN2OS
19. What is Cyber Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
20. Souppaya, M. and Scarfone, K. (2013), Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-83r1 (Accessed May 15, 2022)
21. Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology https://www.researchgate.net/publication/324662275_Cyber_Terrorism_Research_Review_Research_Report_of_the_Australian_National_University_Cybercrime_Observatory_for_the_Korean_Institute_of_Criminology/figures?lo=1
22. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global South*. Basingstoke, U.K: Palgrave Macmillan: Houndmills. [Crossref], [Google Scholar]
23. Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, 18(4), 1–5. doi:10.1080/1097198X.2015.1108093 [Taylor & Francis Online], [Web of Science ®], [Google Scholar]
24. Cybercrime and Cybersecurity in Africa https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527

25. *Akhmat*, *Zaman*, *Shukui*, & *Sajjad*, *2014*;*Pilat*, *2013*;*Hussain*, *Hussain*, *Asad* & *Khan*, *2014*;*Pape* & *Feldman*, *2010*). https://www.researchgate.net/figure/Spectrum-of-Cyber-Enabled-Terrorist-Operations-Adapted-from-Yannakogeorgos-2014-p_fig1_32466227
26. *LaFree et al*., *2015* https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12532
27. Guide to Malware Incident Prevention and Handling for ... - NIST https://www.nist.gov/publications/guide-malware-incident-prevention-and-handling-desktops-and-laptops
28. PLC-Blaster: A Worm Living Solely in the PLC https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf