UNIVERSITY OF HERTFORDSHIRE (UH)

SCHOOL OF PHYSICS, ENGINEERING AND COMPUTER SCIENCE

COURSE: MSc COMPUTER SCIENCE WITH CYBER SECURITY

MODULE: CYBER OPERATION 7COM1069-0901-2023

ACADEMIC YEAR: 2023-2024

ASSIGNMENT TITLE: SUITATIONAL AWARENESS

NAME: OLUWATOBI ELIJAH AKANNI

STUDENT NUMBER: 22060310

TABLE OF CONTENTS

ABSTRACT

The Bank of America data breach in 2019 exposed the personal and financial information of approximately 100,000 customers, highlighting the importance of robust cybersecurity measures in the financial sector. This analysis examines the details of the attack, including the type of attack, targeted systems, and potential consequences, to better understand the threats faced by financial institutions and the need for effective cybersecurity strategies. The report also discusses the weaponization of information, psychological operations, and situational awareness and defense-in-depth strategies to mitigate these threats. Finally, the report outlines an incident response and recovery plan to enhance Bank of America's cybersecurity posture and protect sensitive customer information.

1.0 INTRODUCTION

Bank of America, a leading financial institution in the United States, was subjected to a significant cyberattack on 27 February 2019, resulting in the unauthorized disclosure of sensitive customer information (krebsonsecurity, 2019). This data breach, which targeted the bank's online banking system, exposed the personal and financial details of approximately 100,000 customers (Nguyen, 2019). The attackers gained access to customer names, addresses, phone numbers, and account numbers, potentially leading to identity theft and financial fraud (Choudhury, 2019). This incident highlights the importance of implementing robust cybersecurity measures in the financial sector, where sensitive customer information is a prime target for cybercriminals. This analysis will examine the details of the attack, including the type of attack, targeted systems, and potential consequences, to better understand the threats faced by financial institutions and the need for effective cybersecurity strategies.

1.1 Attack Analysis

The Bank of America data breach was a sophisticated and targeted attack, in which cybercriminals employed a phishing email campaign to deceive customers into divulging their login credentials. The attackers exploited weaknesses in passwords and outdated software to gain unauthorised access to the online banking system, resulting in the extraction of sensitive customer information, including names, addresses, phone numbers, and account numbers. This breach, which affected approximately 100,000 customers, has potentially led to identity theft, financial fraud, and reputational damage. The incident highlights the imperative need for financial institutions to implement robust security measures, including multi-factor authentication, regular security audits, and customer education programs. Moreover, the importance of incident response and disaster recovery plans cannot be overstated, as these measures enable swift and effective responses to future breaches, mitigating potential damage and protecting sensitive customer information.

1.2 Threat Model

Bank of America's online banking system is a prime target for sophisticated hacker groups seeking financial gain, identity theft, and disruption of services, who can exploit vulnerabilities such as outdated software, unsecured network protocols, insufficient access controls, inadequate employee training, and third-party access vulnerabilities to launch phishing or malware attacks, potentially leading to the exposure of sensitive customer information, including names, addresses, phone numbers, and account numbers, and resulting in identity theft, financial fraud, disruption of services, reputation damage, and legal and regulatory consequences, which can be mitigated by implementing robust access controls, regularly updating and patching software, encrypting sensitive information, providing regular employee training, implementing secure third-party access controls, and developing effective incident response planning.

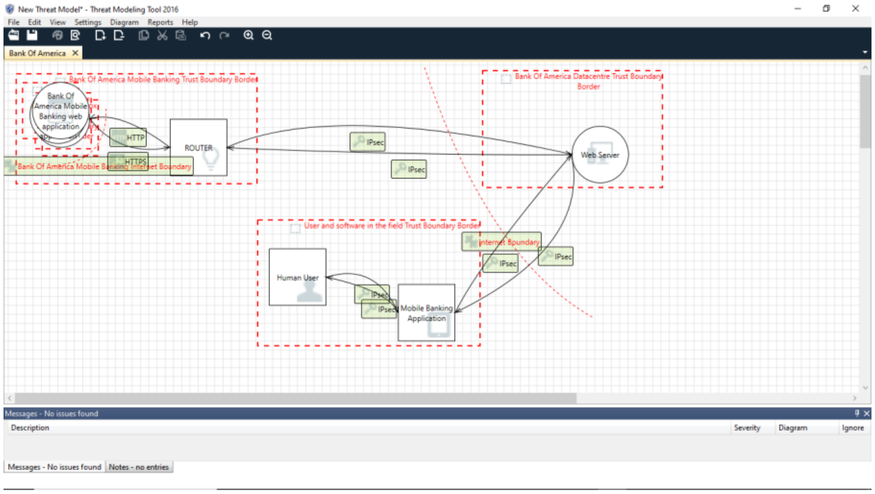
New Threat Model* - Threat Modeling Tool 2016
File
Edit
View
Settings
Diagram
Reports
Help
Bank Of America
Bank Of America Mobile Banking Trust Boundary Border
Bank Of America Mobile Banking web application
HTTP
HTTPS
ROUTER
Bank Of America Mobile Banking Internet Boundary
IPsec
IPsec
Bank Of America Datacentre Trust Boundary Border
Web Server
User and software in the field Trust Boundary Border
Internet Boundary
IPsec
IPsec
Human User
IPsec
IPsec
Mobile Banking Application
Messages - No issues found
Description
Severity
Diagram
Ignore
Messages - No issues found
Notes - no entries

Figure 1: The threat model represents the Bank of America Mobile Banking system

The Bank of America Mobile Banking threat model represents the system's components, including the human user, mobile banking application, router, HTTP, web application, web server, internet boundary, IPsec, data centre, and trust boundaries. The model illustrates data flow and interactions between components, enabling identification of potential threats and vulnerabilities. By examining trust boundaries and attack surfaces, areas requiring additional security measures can be determined, ensuring the system's safeguard. This comprehensive representation facilitates a thorough understanding of the system's security landscape, enabling proactive measures to protect against potential threats.

2.0 INDUSTRY-SPECIFIC RESEARCH

2.1 INFORMATION AS A WEAPON

In today's digital age, information has become a powerful weapon, and financial institutions are a prime target for cybercriminals and nation-state actors seeking to exploit sensitive data for financial gain or strategic advantage (Lt. Col. Jon Herrmann & Lt. Col. Brian Steed, 2018). The Bank of America data breach, which exposed the personal and financial information of approximately 100,000 customers, is a stark reminder of the devastating consequences of information warfare.

2.1.1 The Value of Sensitive Information

Financial institutions possess a vast amount of sensitive information, including customer names, addresses, phone numbers, account numbers, and financial transactions. This information is a goldmine for cybercriminals, who can use it to commit identity theft, financial fraud, and other malicious activities. Moreover, nation-state actors may seek to exploit this information to disrupt the financial system, undermine economic stability, or gain a strategic advantage over rival nations (Bowcut, 2023).

2.1.2 The Weaponization of Information

The weaponization of information has become a significant concern for financial institutions, as cyberattacks have become more sophisticated, frequent, and damaging. The Bank of America data breach is just one example of the many cyberattacks that have targeted financial institutions in recent years. Other notable examples include the Equifax data breach, which exposed the sensitive information of over 147 million people, and the JP Morgan Chase data breach, which affected over 76 million households (darktrace, 2022).

2.1.3 The Consequences of Information Warfare

The consequences of information warfare are far-reaching and devastating. Cyberattacks can result in financial losses, reputational damage, and legal and regulatory consequences. Moreover, they can undermine trust in the financial system, leading to a loss of confidence and stability. The weaponization of information has also created new challenges for financial institutions, which must now invest heavily in cybersecurity measures to protect against these threats (Natalucci, et al., 2024).

2.1.4 Mitigating the Threat of Information Warfare

To mitigate the threat of information warfare, financial institutions must adopt a robust cybersecurity strategy that includes multi-factor authentication, regular security audits, and incident response and disaster recovery plans. They must also educate customers on phishing scams and the importance of strong passwords. Furthermore, financial institutions must collaborate with government agencies and other stakeholders to share threat intelligence and best practices, and to develop a coordinated response to cyber threats (Johnson & Ariana, 2016).

In conclusion, information has become a powerful weapon in the digital age, and financial institutions are a prime target for cybercriminals and nation-state actors seeking to exploit sensitive data for financial gain or strategic advantage. The Bank of America data breach serves as a stark warning of the crippling impact of information warfare, underscoring the imperative for financial institutions to implement robust cybersecurity safeguards to mitigate these threats and protect sensitive information. By working together, we can prevent the weaponization of information and ensure the stability and security of the financial system.

2.2 PSYCHOLOGICAL OPERATIONS (PSYOPS)

In the digital age, financial institutions face a new and insidious threat: Psychological Operations (PsyOps). PsyOps is a form of psychological warfare that aims to manipulate individuals and organizations, influencing their thoughts, behaviours, and decisions. In the context of financial institutions, PsyOps can be used to compromise sensitive information, disrupt operations, and undermine trust (Sunil, 2004).

2.2.1 The Bank of America Data Breach.

The Bank of America data breach, which exposed the personal and financial information of approximately 100,000 customers, is a stark reminder of the devastating consequences of PsyOps. The breach was not just a technical failure, but also a psychological one. The attackers used social engineering tactics to trick employees into revealing sensitive information, highlighting the vulnerability of financial institutions to PsyOps.

2.2.2 Forms of PsyOps

PsyOps include phishing, pretexting, and baiting; phishing tricks individuals into revealing sensitive info through fraudulent emails, texts, or messages. Pretexting involves creating a false scenario to gain an individual's trust, while baiting involves leaving malware-infected devices or storage media in public areas. These tactics can be used to access sensitive information, disrupt operations, or even manipulate financial markets. (Sunil, 2004).

2.2.3 Consequences of PsyOps

The consequences of PsyOps are far-reaching and devastating. Financial institutions can suffer significant financial losses, reputational damage, and legal and regulatory consequences. Moreover, PsyOps can undermine trust in the financial system, leading to a loss of confidence and stability.

2.2.4 Mitigating the Threat of PsyOps

Financial institutions face a significant threat from PsyOps (psychological operations). To combat this, a comprehensive cybersecurity strategy is crucial. This includes educating employees on social engineering tactics, conducting regular security awareness training, and implementing incident response and disaster recovery plans. Collaboration with government agencies and other stakeholders is also vital for sharing threat intelligence and best practices. The Bank of America data breach highlights the devastating consequences of PsyOps. By understanding PsyOps tactics and techniques, financial institutions can develop effective defences and protect against this invisible threat. A coordinated response is essential to reduce the risk of PsyOps attacks and protect sensitive customer information (Julie & Anthony, 2019). In conclusion, a comprehensive cybersecurity strategy and collaboration with stakeholders are crucial for financial institutions to mitigate the threat of PsyOps and protect sensitive customer information.

3.0 SITUATIONAL AWARENESS AND DEFENSE-IN-DEPTH

3.1 Analyse Existing Security Posture

Bank of America, one of the largest financial institutions in the United States, suffered a significant cyberattack in 2019, resulting in the exposure of sensitive customer information. This incident highlights the importance of robust cybersecurity measures in the financial industry, where sensitive customer information is a prime target for cybercriminals. This analysis will examine the details of the attack and identify potential vulnerabilities in physical security, network security, information security, and operational security to better understand the threats faced by financial institutions and the need for effective cybersecurity strategies (Cyril, 2012).

3.1.1 Physical Security

Bank of America's physical security posture, a critical aspect of its overall security strategy, requires attention to address vulnerabilities in access control, which may be exploited through tailgating, surveillance, which may not cover all areas, and physical access to sensitive areas like data centres and server rooms containing sensitive information, which may be vulnerable to breaches (D, et al., 2016).

3.1.2 Network Security

Bank of America's network security posture, a critical aspect of its overall security strategy, requires attention to address vulnerabilities in outdated software, unsecured network protocols, and insufficient encryption, which collectively leave the online banking system and sensitive data vulnerable to exploitation and interception by cybercriminals (David & Fabro, 2006).

3.1.3 Information Security

Bank of America's information security posture, critical to protecting sensitive customer information, requires attention to address vulnerabilities in insufficient access controls, unsecured data storage practices, and insufficient data encryption, which collectively leave sensitive information vulnerable to unauthorized access, interception, and exploitation by cybercriminals (David & Fabro, 2006).

3.1.4 Operational Security

The operational security posture of Bank of America, crucial for safeguarding sensitive customer information, necessitates urgent attention to address the vulnerabilities arising from inadequate employee training in cybersecurity best practices, unsecured access to sensitive information by third-party vendors, and insufficient incident response planning. These vulnerabilities collectively render the bank susceptible to social engineering attacks, exploitation by cybercriminals, and inadequate response to cyberattacks, thereby compromising the confidentiality, integrity, and availability of sensitive customer information (David & Fabro, 2006).

3.2 Defense-in-Depth Strategy for Bank of America

To protect against the evolving threat landscape, Bank of America must implement a robust defence-in-depth strategy that addresses physical, network, information, and operational security. This multi-layered approach will provide comprehensive security and mitigate potential threats. (Jan-Erik, 2017)

3.2.1 Layer 1: Physical Security

Access Control: To ensure robust security, multi-factor authentication, biometric scanning, and smart card access should be implemented for all employees and contractors. This will provide an additional layer of security to prevent unauthorised access to the bank's facilities.

Surveillance: High-resolution cameras and motion sensors should be installed to monitor all areas of the bank's facilities. This will enable effective monitoring and detection of potential security breaches.

Physical Access to Sensitive Areas: Secure doors, locks, and access controls should be implemented for sensitive areas such as data centres, server rooms, and other areas containing sensitive information. This will prevent unauthorised physical access to these areas and protect the bank's sensitive information.

3.2.2 Layer 2: Network Security

Network security is a critical component of the bank's overall security posture. To ensure the integrity of the network, the following measures should be implemented:

Firewalls: Robust firewalls should be implemented to control incoming and outgoing network traffic. This will prevent unauthorised access to the network and protect against potential security threats.

Intrusion Detection and Prevention Systems (IDPS): IDPS should be implemented to detect and prevent unauthorised access to the network. This will enable the bank to identify and respond to potential security breaches in a timely and effective manner.

Encryption: End-to-end encryption should be implemented for all network traffic to prevent interception and exploitation by cybercriminals. This will ensure that sensitive information remains confidential and secure.

Network Segmentation: The network should be segmented into different zones, each with its own access controls and security measures. This will prevent lateral movement in the event of a breach and limit the potential damage.

3.2.3 Layer 3: Information Security

Information security is a vital component of the bank's overall security posture. To ensure the integrity, confidentiality, and availability of sensitive information, the following measures should be implemented:

Access Controls: Robust access controls, including multi-factor authentication, should be implemented to ensure that only authorised personnel possess access to confidential data. This will prevent unauthorised access and protect against potential security threats.

Data Encryption: End-to-end encryption should be implemented for all sensitive information, both in transit and at rest. This will ensure that sensitive information remains confidential and secure, even in the event of a breach.

Data Loss Prevention (DLP): DLP tools should be implemented to detect and prevent unauthorised data exfiltration. This will enable the bank to identify and respond to potential security breaches in a timely and effective manner.

Incident Response Planning: A comprehensive incident response plan should be developed and implemented to respond quickly and effectively to cyberattacks. This plan should include procedures for incident detection, reporting, containment, eradication, recovery, and post-incident activities.

3.2.4 Layer 4: Operational Security

Operational security is a crucial aspect of the bank's overall security posture. To ensure the effective management and operation of security controls, the following measures should be implemented:

Employee Training: Regular cybersecurity training should be provided for all employees to ensure they are aware of the latest threats and best practices. This will enable employees to identify and respond to potential security breaches in a timely and effective manner.

Third-Party Access: Secure third-party access controls, including multi-factor authentication and encryption, should be implemented to prevent unauthorised access to sensitive information. This will ensure that third-party vendors and contractors do not compromise the bank's security.

Incident Response Planning: A comprehensive incident response plan should be developed and implemented to respond quickly and effectively to cyberattacks. This plan should include procedures for incident detection, reporting, containment, eradication, recovery, and post-incident activities.

Continuous Monitoring: The bank's systems and networks should be continuously monitored for potential security vulnerabilities and threats. This will enable the bank to identify and respond to potential security breaches in a timely and effective manner, and to stay ahead of evolving cyber threats.

4.0 INCIDENT RESPONSE AND RECOVERY PLAN

The cyberattack on Bank of America in 2019 highlights the importance of robust cybersecurity measures in the financial sector. Intelligence gathering plays a crucial role in improving incident response capabilities. This plan outlines how Bank of America can leverage intelligence gathering to enhance its incident response and recovery strategies.

4.1 THREAT INTELLIGENCE COLLECTION

To effectively gather threat intelligence, a multi-faceted approach is necessary. This can be achieved through the following methods:

4.1.1 Open-Source Intelligence (OSINT)

OSINT involves monitoring online platforms, social media, and dark web forums to identify potential threats and indicators of compromise. This can include monitoring hacking forums, social media platforms, and other online sources for information on emerging threats.

4.1.2 Human Intelligence (HUMINT)

HUMINT involves engaging with industry partners, law enforcement agencies, and threat intelligence experts to gather information on emerging threats. This can include collaborating with other organizations, attending threat intelligence conferences, and engaging with experts in the field to gather information on potential threats.

4.1.3 Technical Intelligence (TECHINT)

TECHINT involves analyzing network traffic, system logs, and malware samples to identify potential threats and vulnerabilities. This can include analyzing network traffic patterns, system logs, and malware samples to identify potential indicators of compromise and vulnerabilities that could be exploited by attackers.

4.2 THREAT INTELLIGENCE ANALYSIS

To effectively analyse threat intelligence, a comprehensive approach is necessary. This can be achieved through the following methods:

4.2.1 Threat Modeling

Threat modeling involves identifying potential attack vectors and vulnerabilities in Bank of America's systems and applications. This includes analyzing the bank's systems and applications to identify potential weaknesses that could be exploited by attackers.

4.2.2 Pattern Analysis

Pattern analysis involves examining incident response data to identify patterns and trends in cyberattacks. This includes analyzing data from past incidents to identify common tactics, techniques, and procedures (TTPs) used by attackers.

4.2.3 Intelligence Fusion

Intelligence fusion involves combining Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), and Technical Intelligence (TECHINT) to provide a comprehensive understanding of potential threats. This includes integrating information from various sources to identify potential threats and vulnerabilities and to inform the bank's cybersecurity strategy.

4.3 INCIDENT RESPONSE AND RECOVERY STRATEGIES

To effectively respond to and recover from cybersecurity incidents, the following strategies should be employed:

4.3.1 Enhanced Authentication

Multi-factor authentication and behavioural analytics should be implemented to detect and prevent unauthorised access to systems and data. This will provide an additional layer of security to prevent attackers from gaining access to sensitive information.

4.3.2 Network Segmentation

Network segmentation should be implemented to limit lateral movement in the event of a breach. This will prevent attackers from moving freely throughout the network and reduce the potential damage of a breach.

4.3.3 Incident Response Plan

A comprehensive incident response plan should be developed and regularly exercised to ensure a swift and effective response to cyberattacks. This plan should include procedures for incident detection, reporting, containment, eradication, recovery, and post-incident activities.

4.3.4 Customer Notification

A communication plan should be established to promptly notify affected customers in the event of a breach. This will ensure that customers are informed and aware of the situation and can take necessary steps to protect themselves.

4.3.5 Continuous Monitoring

Systems and networks should be regularly monitored for potential threats and vulnerabilities. This will enable the identification and remediation of vulnerabilities before they can be exploited by attackers and ensure the continued security and integrity of systems and data.

Intelligence gathering is a critical component of incident response and recovery strategies. By leveraging OSINT, HUMINT, and TECHINT, Bank of America can enhance its incident response capabilities, improve threat detection, and reduce the risk of cyberattacks. Continuous monitoring and analysis of threat intelligence enable swift and effective response to emerging threats, protecting sensitive customer information, and maintaining the trust of customers.

4.4 INCIDENT RESPONSE PLAN

4.4.1 Detection and Identification

Systems and networks should be subject to continuous monitoring to facilitate the prompt identification of suspicious activity, and alerts should be established to notify relevant personnel of potential security incidents, enabling a swift response. Furthermore, incidents should be classified according to their severity, categorised as high, medium, or low, to inform the incident response strategy.

4.4.2 Containment and Mitigation

Affected systems and networks should be isolated promptly to prevent the spread of the incident and mitigate further damage. Affected devices and accounts should be quarantined to prevent any further exploitation or damage, and temporary fixes should be implemented to prevent further exploitation and mitigate the incident's impact, pending a more permanent solution.

4.4.3 Eradication and Recovery

Malware and other threats should be eliminated from affected systems and networks to prevent further damage and ensure a secure environment. Compromised systems and data should be restored to a known good state, ensuring the integrity and availability of critical resources, and security patches and updates should be applied to affected systems and networks to prevent future exploitation of vulnerabilities and ensure ongoing security.

4.4.4 Reporting and Communication

The incident response team and management should be promptly notified of the incident to ensure a swift and coordinated response. The incident should be reported to relevant authorities, such as the FBI or FTC, in accordance with legal and regulatory requirements. Affected customers should be informed of the incident in a timely and transparent manner, with guidance on any necessary actions to protect themselves.

Additionally, regulators, partners, and media should be communicated with in an open and transparent manner, providing necessary information and updates to manage the incident's impact.

4.4.5 Business Continuity

Backup systems should be activated to ensure the continued operation of critical business functions, minimising the impact of the incident on business continuity. Alternative processes should be implemented to maintain customer services, ensuring that customers continue to receive support and services despite the incident. Furthermore, affected customers should receive prompt support and communication, including regular updates on the incident and the actions being taken to resolve it, which will help to maintain trust and confidence in the organisation.

4.4.6 Post-Incident Activities

A comprehensive analysis of the incident should be conducted, examining the causes, consequences, and response strategies employed, to facilitate the identification of areas for improvement and inform future incident response efforts. The lessons learned and areas for improvement identified during the incident analysis should be thoroughly documented, providing a repository of knowledge to inform future incident response and planning. Furthermore, the incident response plan should be reviewed and updated accordingly, incorporating the lessons learned and areas for improvement identified during the post-incident activities, to ensure the continued effectiveness and relevance of the plan.

4.4.7 Incident Response Team

A team lead should be appointed to oversee and coordinate the incident response efforts, ensuring a unified and effective response, and the incident response team should comprise representatives from various departments, including IT, security, legal, and communications, to provide a comprehensive and multidisciplinary approach to incident management.

4.4.8 Incident Response Plan Maintenance

The incident response plan should be subject to regular review, at a minimum of once annually, to ensure its continued effectiveness and relevance, and updates should be made as necessary to reflect changes in the organisation, threats, or legal requirements. Additionally, a regular training and exercise program should be implemented to ensure that incident response team members and other relevant personnel are familiar with the plan and their roles and responsibilities within it, thereby helping to ensure the plan's effectiveness in the event of an incident.

5.0 CONCLUSION

In conclusion, the incident response plan outlined above provides a comprehensive framework for responding to security incidents in a timely and effective manner. By following the steps outlined in this plan, organizations can minimize the impact of security incidents, prevent further damage, and ensure a secure environment for their systems, networks, and data. The plan's emphasis on threat elimination, system recovery, and software patch management ensures that affected systems and networks are restored to a known good state, and that vulnerabilities are addressed to prevent future exploitation. By implementing this plan, organizations can protect their critical resources, maintain business continuity, and ensure the trust and confidence of their customers and stakeholders.

6.0. References

Bowcut, S., (2023) *cybersecurityguide.* [Online] Available at: https://cybersecurityguide.org (Accessed: 4 May 2024).

Choudhury, S. R., (2019) *cnbc.* [Online] Available at: www.cnbc.com (Accessed: 5 May 2024).

Cyril, O., (2012) *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications.* s.l.:IGI Global.

darktrace, (2022) *darktrace.* [Online] Available at: https://darktrace.com (Accessed: 5 May 2024).

David, K. & Fabro, M., (2006) *Control systems cyber security: Defense in depth strategies.* United States: Idaho National Lab.(INL), Idaho Falls, ID (United States).

D, M. E., J, A. I. H. & Hale, B. L., (2016) Cyber situational awareness. *The Cyber Defense Review,* 1(1), pp. 35--46.

Jan-Erik, H., (2017) Defense-in-Depth. *Handbook of Safety Principles,* pp. 42--62.

Johnson & Ariana, (2016) Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. *NC Banking Inst.,* Volume 20, p. 277.

Julie, M. & Anthony, K., (2019) Cyberpsychological Threat Intelligence. In: *ECCWS 2019 18th European Conference on Cyber Warfare and Security.* s.l.:Academic Conferences and publishing limited, p. 314.

krebsonsecurity, (2019) *krebsonsecurity.* [Online] Available at: krebsonsecurity.com (Accessed: 5 May 2024).

Lt. Col. Jon Herrmann, U. A. F. R. & Lt. Col. Brian Steed, U. A., (2018) Understanding Information as a Weapon. *Military review online exclusive,* Volume 1.

Natalucci, F., Qureshi, M. S. & Suntheim, F., (2024) *imf.* [Online] Available at: https://www.imf.org (Accessed: 5 May 2024).

Nguyen, J. S. a. L., (2019) *bloomberg.* [Online] Available at: www.bloomberg.com (Accessed: 5 May 2024).

Sunil, N., (2004) Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis,* 28(1), pp. 177--192.