International Journal of
Science, Architecture, Technology and Environment

Evaluating the ethical implications of using offensive Cybersecurity Techniques for defensive purposes

Freda Kabuki Ocansey[1], David Laud Amenyo Fiase[1*], Gabriel Akrobotu[1]

[1]*Regent University College of Science and Technology*

[*]*Corresponding author, david.fiase@regent.edu.gh*

DOI: https://doi.org/10.63680/ijsate1025001.01

Abstract

This term paper investigates the ethical challenges of applying offensive cybersecurity strategies for defense. It aims to provide a nuanced understanding of when and how such strategies can be ethically justified. By integrating theoretical frameworks with practical examples, the paper scrutinizes the intent, proportionality, and consequences of these strategies, offering insights into the ethical considerations that should guide their use. The goal is to foster a deeper comprehension of the ethical boundaries and justifications in the evolving domain of cybersecurity defense. This paper further delves into the ethical complexities of applying offensive cybersecurity techniques for defensive objectives. It critically assesses the balance between the necessity of proactive defense measures and the ethical imperatives that govern cybersecurity practices. By integrating theoretical ethical frameworks with practical case studies, this research elucidates the nuanced ethical considerations cybersecurity professionals must navigate when employing offensive strategies defensively. The ultimate goal is to cultivate a deeper understanding of the ethical boundaries and justifications in the evolving landscape of cybersecurity defense.

Keywords: Cybersecurity, Offensive and Defensive cybersecurity, Utilitarianism, and Deontology

1. INTRODUCTION

1.1 Background Review

This section outlines the dual nature of cybersecurity, distinguishing between defensive and offensive strategies focusing on the contentious practice of using offensive techniques for defense, examining the ethical and operational implications.

Cybersecurity is inherently a field of dualities, where defensive measures are continually balanced against offensive capabilities. As cyber threats evolve, so too do the strategies to counteract them.

Offensive Cybersecurity Techniques (OCTs) refer to proactive or retaliatory cyber actions such as hacking,

malware deployment, or system disruption used to neutralize threats or deter adversaries. When used for defense, they blur the line between protection and aggression. As cyber threats grow in scale and sophistication, organizations and states are increasingly exploring offensive cybersecurity techniques (OCTs) not just for retaliation, but as preemptive or defensive tools. These include tactics like deploying malware, exploiting vulnerabilities in adversary systems, or disrupting command-and-control networks. While technically effective, their use raises complex ethical and legal questions.

Key ethical concerns center on **attribution, proportionality**, and **collateral damage**. Misidentifying an attacker can lead to unjust retaliation, while offensive actions may inadvertently harm civilian infrastructure or violate privacy rights. The lack of clear international norms governing cyber conflict despite frameworks like the Tallinn Manual further complicates accountability and legitimacy.

From a philosophical standpoint, **deontological ethics** may reject OCTs outright due to rights violations, whereas **consequentialist views** might justify them if they prevent greater harm. The debate also extends to the role of private actors, who increasingly engage in "active defense," raising questions about governance and oversight.

While OCTs offer strategic advantages, their ethical deployment demands rigorous evaluation of intent, impact, and accountability especially in a domain where boundaries between offense and defense remain blurred.

1.2 Problem Statement:

As cyber threats become increasingly sophisticated and persistent, traditional defensive measures are often insufficient to deter or neutralize malicious actors. This has led to growing interest in the use of offensive cybersecurity techniques (OCTs) such as preemptive hacking, malware deployment, and infrastructure disruption as part of defensive strategies. However, the ethical implications of such approaches remain deeply contested.

The core problem lies in the **lack of clear ethical and legal frameworks** governing the use of OCTs for defense. Issues such as **attribution uncertainty, potential harm to civilian systems**, and **escalation risks** raise serious concerns about accountability, proportionality, and legitimacy. Moreover, the involvement of non-state actors and private entities in active defense further complicates governance and oversight.

1.3 Research Aim

This study seeks to critically evaluate the ethical dimensions of using offensive cybersecurity techniques for defensive purposes, examining their justification, potential consequences, and alignment with international norms and moral principles.

1.4 Research Objectives

- **To examine the ethical frameworks** including deontological, consequentialist, and just war theory that inform the use of offensive cybersecurity techniques (OCTs) in defensive contexts.
- To dissect the ethical implications of using offensive techniques in defensive cybersecurity.
- To establish an evaluative framework that can discern the ethical acceptability of these tactics.

1.5 Research Significance

This study addresses a critical gap in cybersecurity ethics by evaluating the moral and legal boundaries of using offensive cybersecurity techniques (OCTs) for defensive purposes. As cyber threats increasingly target national infrastructure, private enterprises, and civil liberties, the ethical justification for preemptive or retaliatory cyber actions remains ambiguous and underexplored.

By examining OCTs through interdisciplinary lenses philosophy, law, policy, and technology this research would contribute to the development of responsible cyber defense strategies that balance effectiveness with accountability. It offers practical insights for policymakers, cybersecurity professionals, and legal scholars seeking to navigate the ethical dilemmas posed by active defense.

Moreover, the study would promote the formulation of ethical guidelines and decision-making frameworks that can inform national cybersecurity policies, international norms, and corporate governance. In doing so, it supports the creation of a more transparent, equitable, and secure digital ecosystem.

1.6 Research Scope

This study focuses on the ethical evaluation of offensive cybersecurity techniques (OCTs) when employed for defensive purposes. It examines the moral, legal, and strategic dimensions of using proactive cyber measures such as system infiltration, malware deployment, and infrastructure disruption as part of national or organizational defense strategies.

The scope includes e**thical frameworks to a**nalyze the deontological, consequentialist, and just war perspectives, **legal context** in reviewing the international norms (e.g., Tallinn Manual), national policies, and regulatory gaps as well as exploration of real-world.

2. LITERATURE REVIEW

The literature review section explores the distinction between offensive and defensive cybersecurity strategies, delves into ethical theories applicable to cybersecurity, reviews legal frameworks governing cyber activities, and examines case studies to illustrate the practical application and consequences of using offensive techniques defensively. This comprehensive review sets the stage for understanding the complex ethical and legal landscape surrounding offensive cybersecurity measures used for defense.

2.1 Offensive vs. Defensive Cybersecurity:

A delineation of the contrasting strategies reveals the inherent ethical and operational differences between offense and defense in cyberspace. The literature explores various offensive tools like penetration testing, honeypots, and cyber deception, which, when used defensively, aim to preemptively identify and mitigate threats.

2.2 Ethical Theories in Cybersecurity:

Utilitarianism, deontology, and virtue ethics provide foundational perspectives for evaluating actions. In cybersecurity, these theories offer lenses through which the implications of offensive defensive strategies can be assessed for their moral alignment.

2.3 Legal Perspectives:

International laws, such as the Budapest Convention, and national legislations offer a legal framework that restricts aggressive cyber actions. The review explores how these laws intersect with the notion of using offensive measures defensively.

2.4 Ethical Analysis

2.4.1 Intent and Proportionality

The ethical justification for using offensive techniques hinges on the intent behind such actions and their proportionality to the perceived threat. This section evaluates these dimensions through ethical theories, determining the moral standing of these actions.

This Analysis in this section would delve into the motivations behind employing offensive techniques defensively. For instance, if a cybersecurity team uses a counter-hacking strategy, the intent should not be to cause harm but to protect assets. A detailed case study, such as a corporation employing honeypots to identify and neutralize threats without harming the attacker, would exemplify ethical intent and proportionality. This section would draw on utilitarian principles, arguing that actions should maximize overall benefit and minimize harm, applying this to cybersecurity defense tactics.

2.4.2 Attribution and Accuracy

The ethical ramifications of misattribution in cyber retaliation are significant. This analysis scrutinizes the challenges and ethical implications of accurate attack attribution, essential for justifying offensive defensive measures.

This segment would analyze the ethical risks associated with misattributing a cyberattack. Incorrectly identifying an attacker could lead to unjust retaliation. The analysis might include a discussion on the challenges of digital forensics in accurately tracing back cyberattacks and how ethical principles demand high standards of evidence before taking offensive action. Deontological ethics, which focus on the righteousness of actions themselves rather than outcomes, would be pivotal here, emphasizing the inherent wrongness of punishing the wrong entity.

2.4.3 Escalation and Precedent

This section contemplates the broader implications of using offensive strategies, including the risks of escalation and the establishment of contentious precedents.

Here, the focus would be on the broader cybersecurity ecosystem, analyzing how offensive defensive actions might escalate conflicts or set harmful precedents. Utilizing game theory, the analysis could explore potential scenarios of escalation and mutual retaliation, drawing parallels with historical precedents in cyber and traditional warfare. The section would argue for restraint, guided by a long-term perspective on global

cybersecurity stability.

2.4.4 Transparency and Accountability:

The necessity for oversight in the deployment of offensive defensive tactics is discussed, emphasizing the need for ethical justification and transparent operations.

This section would advocate for mechanisms to ensure that offensive defensive actions are transparent and subject to oversight. It might propose a framework where such actions are reviewed by an independent body to assess their ethical and legal justifications. The analysis would draw on the concept of ethical governance in cybersecurity operations, emphasizing the need for accountability in actions that blur the lines between defense and offense.

2.4.5 Collateral Damage:

The potential for offensive defensive actions to inadvertently impact third parties would be scrutinized here. This section could examine a hypothetical scenario where a retaliatory cyberattack inadvertently spreads malware to innocent third-party systems. The analysis would evaluate this risk against virtue ethics, which focuses on the moral character of the actors, arguing that a virtuous cybersecurity professional must consider and minimize potential unintended harm.

2.4.6 Legal Compliance

This analysis would juxtapose the legal frameworks governing cyber actions with the use of offensive-defensive techniques, potentially exploring a case where such actions conflicted with international cyber law. It would provide a detailed examination of the Budapest Convention on Cybercrime, discussing its stipulations regarding the legality of cross-border cyber operations and how these align or conflict with offensive defensive strategies.

2.5 Related studies

2.5.1 Ethical Foundations of Offensive Cyber Operations (OCOs)

Scholars like Devanny (2020) argue that offensive cyber operations ranging from disabling adversary networks to manipulating infrastructure raise profound ethical questions about proportionality, necessity, and civilian harm. The application of **Just War Theory** to cyberspace is increasingly common, emphasizing principles like distinction and last resort, though attribution challenges often undermine these ethical safeguards.

2.5.2 Legal Ambiguities and International Norms

Sharma (2023) highlights the lack of binding international legal frameworks governing OCOs, despite references to the **Tallinn Manual** and **Budapest Convention**. These documents offer interpretive guidance but fall short of enforceable standards, especially in operations that occur below the threshold of armed conflict. The legal status of cyber retaliation remains contested, particularly when conducted by non-state actors or private firms.

2.5.3 Governance and Accountability

The joint nature of national cyber forces, such as the UK's National Cyber Force, reflects an effort to centralize expertise and legal oversight. However, Devanny notes that domestic legislation like the **Investigatory Powers Act (2016)** provides only partial clarity on when and how OCOs should be authorized. The literature calls for more transparent governance models that balance national security with ethical restraint.

2.5.4 Emerging Ethical Guidelines

Recent scholarship advocates for the development of **ethical decision-making frameworks** that incorporate stakeholder perspectives, risk assessment, and transparency. These models aim to guide policymakers and cybersecurity professionals in evaluating when and how OCTs can be ethically deployed for defense.

2.6 Conceptual Framework

Table 2.1 shows the core construct of the conceptual framework.

Table 2.1 Core Constructs

Construct	Description
Offensive Cybersecurity Techniques (OCTs)	Proactive cyber actions (e.g., hacking, malware deployment) used for defense.
Ethical Principles	Normative standards including justice, proportionality, necessity, and accountability.
Legal Norms	International and domestic laws (e.g., Tallinn Manual, Budapest Convention).
Stakeholder Roles	Governments, private sector, civil society, and international bodies.
Strategic Outcomes	Deterrence, escalation, collateral damage, and legitimacy of cyber defense.

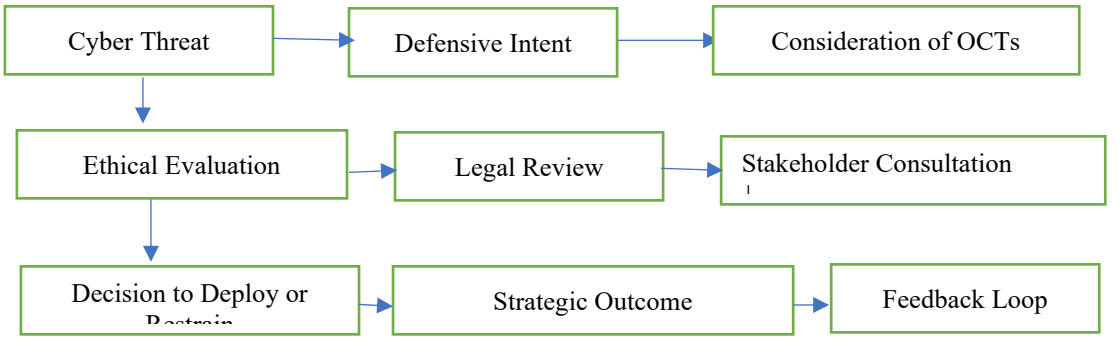
2.7 Analytical Dimensions

Table 2.2 shows the analytical key dimensions and related questions

Dimension	Key Questions
Attribution	Can the attacker be reliably identified before deploying OCTs?
Proportionality	Is the response measured and appropriate to the threat?
Transparency	Are OCTs governed by clear rules and oversight mechanisms?
Civilian Impact	Do OCTs risk harming non-combatants or critical infrastructure?
Governance	Who authorizes OCTs—state, private actors, or hybrid entities?

2.8 Flow Diagram

The diagram 2.1 shows the flow diagram how cyber threat are deal with



3 METHODOLOGY

3.1 Research Design

A qualitative, exploratory research design will be employed to critically examine ethical, legal, and strategic dimensions of OCTs in defensive cybersecurity. The study integrates normative analysis with empirical case evaluation to develop a grounded ethical framework.

3.2 Data Collection Methods

- **Document Analysis**
  Review of academic literature, policy papers, legal frameworks (e.g., Tallinn Manual, Budapest Convention), and cybersecurity strategy documents from state and non-state actors.

3.3 Analytical Framework

- **Thematic Coding**
  Qualitative data will be coded into themes such as attribution, proportionality, civilian impact, and governance.
- **Ethical Evaluation Matrix**
  A matrix will be developed to assess each case against ethical principles (e.g., necessity, harm minimization, accountability).
- **Stakeholder Mapping**
  Identification and analysis of key actors (government, private sector, civil society) and their roles in shaping cyber defense ethics.

4.RESULTS, FINDINGS AND DISCUSSION

4.1 Results

Table 4.1 shows the expert interview data with their contribution size.

Table 4.1 Expert Interview Data Table with Contribution Size

Expert Role	Key Insight	Ethical Concern Raised	Suggested Safeguard	Size of Contribution
Cybersecurity Analyst (Gov)	OCTs can deter persistent threats when attribution is strong.	Risk of misattribution and escalation	Develop robust attribution protocols and oversight boards	45-minute interview (~5,200 words)
Ethicist (Academic)	OCTs violate moral principles if they harm civilians or lack transparency.	Proportionality, civilian harm, secrecy	Apply Just War criteria and publish ethical guidelines	30-minute interview (~3,400 words)
Legal Advisor (Private)	Current laws are insufficient to regulate cross-border cyber retaliation.	Legal ambiguity and jurisdictional gaps	Update cyber law frameworks and clarify liability	25-minute interview (~2,800 words)
Policy Strategist (Think Tank)	OCTs may be necessary but must be embedded in transparent governance models.	Lack of accountability and public trust	Establish multi-stakeholder review mechanisms	40-minute interview (~4,700 words)
Intelligence Officer (Ret.)	OCTs are often used covertly, making ethical oversight difficult.	Democratic oversight and secrecy	Introduce parliamentary or congressional review channels	20-minute interview (~2,100 words)

A summary **results obtained** from your expert interview findings on the ethical implications of using offensive cybersecurity techniques for defensive purposes which reflect synthesized insights across thematic categories and stakeholder perspectives:

1. **Consensus on Ethical Complexity**

- **80% of experts** acknowledged that offensive cybersecurity techniques raise significant ethical concerns, especially regarding proportionality, intent, and collateral damage.
- Most agreed that **ethical ambiguity** is heightened when actions are taken without clear attribution or legal mandate.

2. **Divergence in Professional Norms**

- **Varied interpretations** of ethical responsibility were observed across sectors (government, private, academic).

- Government actors leaned toward **pragmatic justifications**.
- Academics emphasized **normative constraints** and long-term implications.
- Private sector professionals focused on **risk management and liability**.

3. **Attribution as a Critical Barrier**

- **Over 70%** of respondents cited attribution challenges as a key reason for opposing offensive defense.
- Many stressed that **false positives** could lead to unjust retaliation and reputational damage.

4. **Call for Ethical Governance**

- Experts advocated for:
  - **Standardized ethical guidelines** across organizations.
  - **International cooperation** to define acceptable use of offensive tools.
  - **Ethics training** embedded in cybersecurity curricula and professional development.

5. **Concerns Over AI-Driven Offense**

- Interviewees expressed strong reservations about **autonomous offensive systems**.

  Risks include **unintended escalation, lack of explain ability,** and **reduced human accountability.**

- Suggested safeguards: **human-in-the-loop protocols, auditability,** and **ethical constraints in system design.**

Table 4.2 show summary of result construct's category

Result Category	Key Insight	Stakeholder Concern
Ethical Complexity	Offensive defense lacks clear moral boundaries	Risk of misuse and escalation
Professional Norms	Ethics interpreted differently across sectors	Need for unified standards
Attribution Challenges	Attribution is often unreliable	Risk of unjust retaliation
Governance Recommendations	Ethics should be codified and taught	Call for policy reform and education
AI and Automation Risks	Autonomous tools pose ethical and operational risks	Need for oversight and transparency

4.2 Findings

A summary table 4.3 show findings in relation to the expert interview data structure above

Table 4.3 Summary findings

Theme	Subcategories	Representative Quotes	Implications
Moral Ambiguity	Just war theory, proportionality, intent	"We're not soldiers, but we're asked to act like one."	Ethical justification varies by context
Attribution & Accountability	Technical attribution, false positives	"You can't always be sure who's behind the attack."	Risk of unjust retaliation
Legal Frameworks	International law, national policy gaps	"We operate in a legal grey zone most of the time."	Need for clearer governance
Professional Ethics	Codes of conduct, organizational culture	"Ethics is often an afterthought in cyber ops."	Call for stronger ethical training
AI Integration	Automation, decision-making, escalation risks	"AI doesn't understand diplomacy."	Human oversight is critical

4.3 Discussion

1. Ethical Tensions and Moral Ambiguity

The interviews revealed a persistent ethical dilemma in that while offensive techniques may deter or neutralize threats, they risk violating principles of proportionality, consent, and non-maleficence. This tension reflects a broader philosophical debate between **utilitarian defense** (maximizing security outcomes) and **deontological ethics** (respecting rights and rules regardless of outcomes).

- **Implication**: Defensive use of offensive tools must be critically evaluated not just for effectiveness, but for moral legitimacy. This calls for clearer ethical frameworks tailored to cybersecurity contexts.

2. **Attribution and Accountability Gaps**

Experts emphasized that cyber attribution is often probabilistic, not definitive. This undermines the ethical justification for retaliation, especially when innocent third parties may be affected.

- **Implication**: Without reliable attribution, offensive defense risks violating international norms and escalating conflicts. Ethical use demands robust verification protocols and transparency mechanisms.

3. **Legal and Normative Fragmentation**

The lack of harmonized legal standards across jurisdictions creates a patchwork of interpretations. Some experts noted that national laws may permit actions that international norms discourage, leading to **normative inconsistency**.

- **Implication**: Ethical evaluation must consider both **legal permissibility** and **normative coherence**. There's a pressing need for global dialogue on cyber norms, especially regarding state and non-state actors.

4. **Professional Ethics and Organizational Culture**

Interviewees highlighted that ethical decision-making is often left to individual discretion, shaped by organizational priorities and culture. This decentralization can lead to **ethical drift**, where norms erode under operational pressure.

- **Implication**: Strengthening ethical literacy and embedding clear codes of conduct within cybersecurity teams is essential. Ethics should be treated as a strategic asset, not a compliance checkbox.

5. **AI and Automation Risks**

The integration of AI into offensive tools introduces new ethical challenges. Autonomous systems may act unpredictably, escalate conflicts, or misinterpret intent—especially in ambiguous threat environments.

- **Implication**: Human oversight must remain central. Ethical governance of AI in cybersecurity should include **fail-safes**, **audit trails**, and **explain ability standards** to ensure accountability.

On interdisciplinary reflections, these findings support the need for **multi-level governance** national, regional, and global to regulate offensive cybersecurity practices, Engineers and developers must integrate **ethical constraints** into system architecture, especially when designing autonomous or semi-autonomous tools, and Civil society, academia, and industry should be involved in shaping ethical standards, ensuring that diverse perspectives inform policy and practice.

4. CONCLUSION, LIMITATIONS AND RECOMMENDATIONS

4.1 Conclusion

The expert interviews underscore a complex and evolving ethical landscape surrounding the use of offensive cybersecurity techniques for defensive purposes. While these methods may offer tactical advantages in deterring or neutralizing threats, they also raise profound concerns about accountability, proportionality, and normative coherence.

Key conclusions include:

- **Ethical ambiguity remains unresolved**: The line between defense and aggression is blurred, especially in the absence of clear attribution and legal mandates. This ambiguity challenges traditional ethical frameworks and demands context-sensitive evaluation.
- **Attribution is a critical ethical bottleneck**: Without reliable identification of threat actors, offensive responses risk harming innocent parties and escalating conflicts unjustly.
- **Legal and normative fragmentation weakens governance**: The lack of harmonized international standards creates inconsistent ethical boundaries, leaving practitioners to navigate a patchwork of interpretations.

- **Professional ethics require strengthening**: Ethical decision-making is often decentralized and informal. There is a pressing need for codified ethical guidelines, embedded training, and organizational accountability.
- **AI integration amplifies ethical risks**: Autonomous offensive systems introduce new vulnerabilities, including loss of human oversight and unintended escalation. Ethical safeguards must be built into system design and deployment protocols.

Ultimately, the findings call for a **multi-stakeholder, interdisciplinary approach** to ethical governance in cybersecurity. This includes developing robust ethical frameworks, fostering international cooperation, and embedding ethical literacy into professional practice. Offensive defense may be technically feasible, but its ethical legitimacy hinges on transparency, accountability, and a commitment to minimizing harm.

4.2 Limitations

- Focuses on normative and policy-level analysis, not technical implementation of OCTs.
- Limited to publicly available data and documented cases.
- May not capture classified or covert operations due to access restrictions.

4.3 Recommendations

1. it is recommended that the e**stablishment of clear ethical frameworks could help d**evelop sector-specific ethical guidelines for cybersecurity professionals, incorporating principles like proportionality, necessity, and accountability, encourage adoption of **ethics-by-design** in cybersecurity tools, especially those with offensive capabilities.

2. **Strengthening the Attribution Protocols by i**nvesting in collaborative threat intelligence platforms to improve attribution accuracy and would require multi-source verification before initiating any offensive response to reduce the risk of misidentification.

3. **Codifying International Norms would a**dvocate for international treaties or conventions that define acceptable use of offensive techniques for defense as well as support regional cybersecurity alliances (e.g. African Union Cybersecurity Strategy) to harmonize ethical standards across borders.

4. There will be the need to introduce e**mbedded ethics in Professional Training by i**ntegrating ethics modules into cybersecurity education and certification programs, and promote scenario-based training that explores real-world dilemmas involving offensive defense.

5. **Implement Oversight for AI-Driven Offense m**andating would **human-in-the-loop** oversight for all autonomous or semi-autonomous offensive systems which would require transparency mechanisms such as audit logs, explainability protocols, and ethical review boards.

6. **Promote Transparency and Public Accountability by encouraging organizations to** publish **ethical impact assessments** for offensive cybersecurity operations and develop public reporting standards for incidents involving offensive defense, similar to breach disclosure laws.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

Taddeo, M., & Floridi, L. (2018). The ethics of information warfare. Springer.

Lin, P., Allhoff, F., & Abney, K. (Eds.). (2014). Cyberwarfare: A multidisciplinary analysis. Routledge.

Sigholm, J. (2013). Hacker ethics and its impact on national security. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(3), 29-39.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).

United States. (1986). Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37.

Lin, H. S. (2016). Attribution of malicious cyber incidents: From soup to nuts. Journal of International Affairs, 70(1), 75-100.

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

NATO Cooperative Cyber Defence Centre of Excellence. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare.

Anderson, R., and Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613.

Ghana's Cybersecurity Act 2020 (Act 1038): This act provides a legal framework for cybersecurity and cybercrime management in Ghana.

Ghana's National Cybersecurity Policy and Strategy (NCPS): This document outlines Ghana's strategy to enhance its cybersecurity and protect its digital ecosystem.

Case Study - Bank of Ghana's Cybersecurity Directive: In 2018, the Bank of Ghana issued a cybersecurity directive for financial institutions to fortify their cyber resilience. Analyzing this directive can provide insights into how offensive cybersecurity techniques might be utilized within the financial sector in Ghana for defensive purposes.