A Guide to Stakeholder Analysis for Cybersecurity Researchers

James C. Davis
Purdue University
davisjam@purdue.edu

Sophie Chen
Carnegie Mellon University
scchen@andrew.cmu.edu

Huiyun Peng
Purdue University
peng397@purdue.edu

Paschal C. Amusuo
Purdue University
pamusuo@purdue.edu

Kelechi G. Kalu
Purdue University
kalu@purdue.edu

Abstract

Stakeholder-based ethics analysis is now a formal requirement for submissions to top cybersecurity research venues. This requirement reflects a growing consensus that cybersecurity researchers must go beyond providing capabilities to anticipating and mitigating the potential harms thereof. However, many cybersecurity researchers may be uncertain about how to proceed in an ethics analysis. In this guide, we provide practical support for that requirement by enumerating stakeholder types and mapping them to common empirical research methods. We also offer worked examples to demonstrate how researchers can identify likely stakeholder exposures in real-world projects. Our goal is to help research teams meet new ethics mandates with confidence and clarity, not confusion.

1 Introduction

Cybersecurity research is motivated by the goal of improving the safety, privacy, and integrity of computing systems. However, the process of conducting and publishing cybersecurity research may itself cause harm. Research may expose sensitive information, disrupt services, violate legal or ethical norms, or enable malicious actors by disclosing tools, methods, or vulnerabilities. Individual researchers [1] and academic venues alike have pointed out that ethical considerations in security research are frequently insufficient [2], perhaps because the authors lack awareness of their work's potential ethical implications.

To mitigate these risks, academic venues increasingly require researchers to engage in ethical analysis. For example, the USENIX Security 2026 Call for Papers requires that all submissions include a stakeholder-based ethics analysis on a dedicated supplemental page [3]. This requirement reflects a broader expectation that cybersecurity research must account for its potential harms—not just in methodology, but also in publication. A core component of this process is identifying who may be affected by the research. Before we can reason about effects, we must understand what stakeholders exist, and how they may be impacted.

We recognize that stakeholder-based ethics analysis is a new requirement for the cybersecurity research community, and that not all research teams may be prepared for it. We prepared this guide to improve our own research process, and are sharing it to help other research teams get started. We specifically focus on the first task: *identifying stakeholders*. In §2 we define stakeholder-based ethics analysis and specialize it to cybersecurity. §3 discusses the interaction between research methods and the resultant stakeholders. In §4, we provide worked examples of stakeholder identification connected to several papers from our lab. Finally, §5 offers guidance on using this paper during research planning or ethics documentation, and discusses topics such as the role of ethical frameworks and the boundaries of responsible research.

This paper is intended as a practical resource for researchers preparing submissions to USENIX Security and other cybersecurity venues with ethics requirements. Researchers may use this work to identify relevant stakeholders in their own studies, understand the kinds of impacts those stakeholders may experience, and articulate their ethical reasoning in a principled and reproducible manner. By grounding ethics analysis in examples drawn from typical research practice, we aim to reduce the burden of compliance while increasing the rigor and utility of ethics statements.

2 Background

We begin by establishing the conceptual foundations of stakeholder-based ethics analysis, situating it within established ethical frameworks and principles that guide computing research. Building on this foundation, we define the notion of a stakeholder in this context and present a structured process for identifying both direct and indirect stakeholders who may be affected by the research process or its outcomes.

2.1 Ethics Analysis

Ethics in security research requires researchers to systematically consider who may be affected by their work and how.

This approach builds on efforts to bring principled ethical reasoning to computing research. The Menlo Report [4] articulates four core principles for computing research that were adapted from biomedical ethics: respect for persons, beneficence, justice, and respect for law and public interest [5]. These principles serve as a baseline for evaluating both research procedures and research outputs. Although originally written for information and communication technology (ICT) research, the Menlo principles have since been applied and extended to domains such as adversarial machine learning, vulnerability research, and platform security [6, 7]. In these settings, researchers must often weigh tradeoffs between the public good and individual risk, and stakeholder identification becomes a necessary foundation for any such analysis.

Recent work by Segal *et al.* [6] revisits these principles through the lens of contemporary security research. They argue that researchers often face ethical tradeoffs with no clear resolution, such as disclosing a vulnerability versus preventing immediate harm. In these cases, considering multiple ethical frameworks—consequentialist [8], deontological [9], or virtue ethics [10]—can yield a more nuanced analysis. *Across all frameworks, however, a common starting point is the identification of stakeholders: those who are potentially harmed or benefited by the research.*

USENIX Security 2026 adopts this principle explicitly. Its Call for Papers requires that all submissions include a stakeholder-based ethics analysis or justify an alternative. The analysis must describe which stakeholders may be affected by the research process and by the publication of results [3]. The assumption is that ethical research begins with the recognition of who bears the consequences of our work.

Figure 1 illustrates how ethics analysis proceeds in parallel with the research process. Stakeholder identification begins as soon as research goals are articulated. Ethical analysis may influence the proposed methodology, trigger oversight mechanisms, or lead to changes in design, execution, or dissemination. When considered early and iteratively, stakeholder analysis can prevent avoidable harms and support more responsible research.

Beyond serving as a compliance requirement, ethics analysis can also strengthen the quality of security research by clarifying the project's implicit or under-specified requirements. Stakeholder analysis, in particular, forces researchers to consider the expectations, constraints, and vulnerabilities of those affected by the work. This analysis may reveal new goals, assumptions, or failure modes that an attacker might exploit or a defender might seek to protect. This process naturally complements threat modeling by helping researchers define the system boundaries, trust assumptions, and attacker profiles that structure the work [11]. By surfacing these factors early, ethics analysis may prompt adjustments to data collection, modeling choices, evaluation metrics, or publication plans that make the research both more responsible and more robust. In this way, ethics reflection can function not as an external constraint, but as a source of epistemic rigor and design clarity.

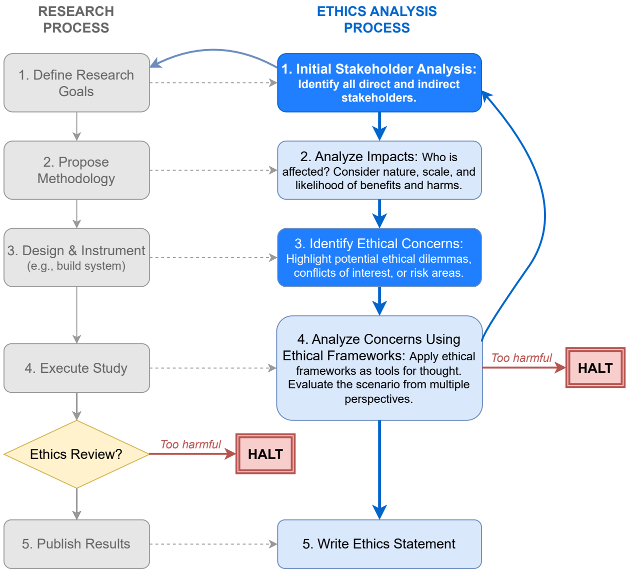
RESEARCH PROCESS
ETHICS ANALYSIS PROCESS
1. Define Research Goals
2. Propose Methodology
3. Design & Instrument (e.g., build system)
4. Execute Study
Ethics Review?
Too harmful
HALT
5. Publish Results
1. Initial Stakeholder Analysis: Identify all direct and indirect stakeholders.
2. Analyze Impacts: Who is affected? Consider nature, scale, and likelihood of benefits and harms.
3. Identify Ethical Concerns: Highlight potential ethical dilemmas, conflicts of interest, or risk areas.
4. Analyze Concerns Using Ethical Frameworks: Apply ethical frameworks as tools for thought. Evaluate the scenario from multiple perspectives.
Too harmful
HALT
5. Write Ethics Statement

Figure 1: Parallel processes of research planning and ethics analysis. Arrows represent information flow, with feedback between study execution and mitigation planning. Dark blue boxes indicate that stakeholder analysis occurs in (at least) two stages, both during the initial project design (ethics box 1) and during the more detailed design (ethics box 3).

2.2 Stakeholder Identification

Definition: Stakeholder

A stakeholder is any person, group, or institution that can affect, or be affected by, a system or its development, operation, or analysis [12]. *Direct* stakeholders interact with, or are explicitly involved in, the research process (*e.g.*, as participants or collaborators). *Indirect* stakeholders may be affected by the consequences of the research, even without direct interaction (*e.g.*, through exposure to harms or the use of resulting technologies) [13].

General concepts and process. Stakeholder identification is the process of enumerating individuals, groups, and institutions who may be impacted by a research project. This includes both "direct stakeholders"—such as study participants or software maintainers—and "indirect stakeholders", such as users of affected systems, vulnerable populations, or the broader public. The distinction reflects the length and complexity of the cause/effect pathway between research and its stakeholders [14]: direct stakeholders are typically affected through short, observable links to the research process or artifacts, while indirect stakeholders may be impacted through

Table 1: Representative stakeholders in cybersecurity research. Following the definition in §2.2, this table distinguishes typical *direct* stakeholders from plausible *indirect* stakeholders. This particular example distinguishes between direct and indirect stakeholders by supposing a "systems" project that is improving backend systems and incorporating human factors data from the systems' engineering staff.

	Stakeholder	**Description**
Direct	Study participants	Individuals who actively provide data or behavior during user studies, interviews, surveys, etc.
	System operators	People or teams responsible for the systems or services being analyzed or measured (*e.g.*, admins of crawled web services).
	Software maintainers	Developers of the software or platforms studied for vulnerabilities, bugs, or compliance.
	Data subjects	Individuals whose personal data appears in datasets, logs, or telemetry used in the study.
	The research team	The investigators themselves, who may be exposed to legal, professional, or reputational risk.
Indirect	End users	Users of affected systems who may be harmed by exposure, insecurity, or disruptions.
	Vulnerable populations	Groups disproportionately affected by exploitation or disclosure (*e.g.*, activists, minors, marginalized communities).
	Adversaries	Actors who might misuse published results to carry out attacks or bypass controls.
	Broader public	Society at large, particularly if trust in infrastructure, institutions, or norms may be impacted.
	Research community	Other researchers who may reuse, replicate, or extend the work and inherit any embedded harms.
	Technology community	Groups interested in security and technology who may implement or adopt the work and inherit any embedded harms.
	Private Institutions	Private organizations, companies, or sponsors whose systems, data, or reputations may be implicated.
	Public Institutions	Public organizations and governments whose systems, data, or reputations may be implicated.

more diffuse or downstream effects, including the adoption, misuse, or unintended consequences of research outputs.

In requirements engineering, stakeholder identification is a foundational step for eliciting system goals, constraints, and assumptions [12, 15]. Stakeholders are often grouped into classes such as *users*, *developers*, *regulators*, and *operators*, with attention to their influence, interests, and modes of interaction [16]. This framing usefully extends to research ethics: a stakeholder is not merely a data point or source of input, but an actor with values, expectations, and potential to be harmed or helped by the research process or its outcomes.

Specialization to Security Research. Security research is broadly concerned with understanding, analyzing, and improving the trustworthiness of systems, infrastructure, and users. The U.S. National Institute of Standards and Technology (NIST) defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks" [17]. The 2025 Calls for Papers for IEEE Symposium on Security and Privacy [18], USENIX Security [19], NDSS [20], and ACM CCS [21] all emphasize novelty, rigor, and impact across a diverse set of technical and human-centered topics.

The global reach and leverage of computing systems mean that advances can affect people, organizations, and environments far beyond the original research context. Security and IT research often must account for adversarial stakeholders—attackers, competitors, deceivers—who may misuse research outputs or be targeted by defensive tools. These properties blur the boundary between direct and indirect stakeholders, creating distinctive challenges in security research to map activities to affected parties:

- *Scale and indirectness:* Security research can produce effects far beyond its original scope, as impacts propagate globally through interconnected systems—often with delayed, indirect, or hard-to-trace consequences. For example, a dataset study may not involve users directly, but could still expose them to privacy harms via re-identification [22]. These indirect effects challenge traditional notions of informed consent and risk assessment [23].
- *Dual-use potential:* Research outputs, such as tools, datasets, and attack techniques, can be used both to defend and to harm. A novel exploit, even if disclosed responsibly, may inspire malicious actors before defenses are deployed [24]. The longstanding tension between openness and control in dual-use publication is a central concern in cybersecurity [25].
- *Adversarial response:* Unlike many domains, security research exists in an adversarial context, where attackers may adapt strategically to research disclosures. Published defenses may provoke bypass techniques or trigger new attack variants [26]. Security researchers must therefore anticipate not only technical outcomes, but also adversary reactions — an expectation uncommon in other scientific disciplines.
- *Ambiguity in ethical responsibility:* The indirect and adversarial nature of security research can obscure who might be

harmed, and who bears responsibility for preventing or mitigating that harm. Attribution is especially difficult: harms may result from chains of actions involving researchers, developers, deployers, and adversaries, with no clear line of causality or control. For example, an insecure design pattern documented for defensive awareness might later be incorporated into offensive malware by an unrelated actor. These ambiguities complicate the mapping from research decisions to ethical duties [7].

Table 1 presents a canonical set of stakeholder categories relevant to common types of cybersecurity research. We distinguish between direct and indirect stakeholders, and include brief descriptions of each. This list may be extended or refined depending on the project context, but it provides a baseline for constructing the ethics section required by the USENIX Security 2026 CFP. In §4, we will specialize these categories for example research scenarios.

3 Research Methods & Stakeholder Exposure

To interpret the stakeholder categories in Table 1, we consider how *problem domains* and *research methods* each shape ethical risk in security studies. Both dimensions influence stakeholder exposure, but in different ways. For example, studies on password reuse directly implicate end-users and service providers, whereas protocol-level vulnerability research more directly affects software maintainers and operators. Research methods, in turn, introduce distinct forms of exposure, especially for direct stakeholders. A quantitative analysis of software packages and a qualitative interview study may both examine supply chain security, but in different ways. The former may reveal vulnerabilities in widely used packages, increasing opportunities for exploitation, while the latter risks compromising participants' privacy or reputation if insider knowledge about development practices is disclosed. Thus, problem domains determine *who* is exposed, whereas research methods determine *how* those risks materialize.

To support consistent stakeholder identification across these various types of research, we organize common security research methods into a set of clusters derived from the SIGSOFT Empirical Standards [27]. Table 2 presents representative groupings of methods that interact with similar kinds of stakeholders. We also provide example security papers from each group, although note that a single work may fall into multiple groups.

4 Example Studies and Stakeholder Analysis

To illustrate how the method–stakeholder framework in §3 can be applied in practice, this section presents worked examples of stakeholder identification for representative security research studies. Table 3 gives a summary. Each example includes a concise project description, identifies the research method(s) and problem domain, and lists the plausible direct and indirect stakeholders. Where appropriate, we also include commentary on unusual exposures or particularly salient ethical concerns. To mitigate concerns about bias or blame, we only discuss papers whose authors are represented on the author list of the present guide. We selected papers from a range of research methods.

These examples are intended to help research teams anticipate the kinds of stakeholder relationships they may encounter in their own work. As described in §2, stakeholder identification is a precursor to further ethical analysis using frameworks such as deontological, consequentialist, or virtue-based reasoning (cf. §5.1). We do not aim to perform full ethics reviews here, but instead to concretely demonstrate the process of naming and describing stakeholder groups.

4.1 Example A: Software Validation Project

This example represents papers concerned with validating the security of software. The following analysis is on the paper "*Systematically Detecting Packet Validation Vulnerabilities in Embedded Network Stacks*", which appeared at ASE 2023 [32]. Papers with similar analyses may include [44] and [45].

4.1.1 Study Overview

Embedded Network Stacks connect critical embedded systems to external networks. As a result, vulnerabilities in ENS can be remotely exploited to cause denial of service, arbitrary code execution, or physical-world harm. Prior dynamic analysis based approaches relied on non-deterministic mutations and provided no security guarantees. This work aims to provide a more systematic dynamic analysis framework to uncover security vulnerabilities in these critical components.

Problem Domain Detection of security vulnerabilities in embedded network stacks.

Methods Two methods were applied:

- *Corpus Analysis*: Analyzed 61 reported vulnerabilities (CVEs) across six embedded network stacks.
- *Tool Design and Evaluation*: Designed and evaluated the effectiveness and performance of EmNetTest, a novel systematic testing framework, on real embedded network stacks.

4.1.2 Stakeholder Identification

Direct Stakeholders

- *Software maintainers*: Developers and maintainers of ENS studied in the paper (*e.g.*, FreeRTOS, Contiki-ng, lwIP, PicoTCP).

Table 2: Cybersecurity research methods grouped by examples of direct stakeholders. Method categories are derived from the SIGSOFT Empirical Standards [27]. Citations in **bold** are included in the analysis in §4.

Method(s)	Description	Typical Direct Stakeholders	Example Papers
Controlled Experiments, Surveys, Interviews	Designed interaction with human participants to study behavior, decision-making, or perception.	Study participants	**[28]**, [29]
Case Study, Action Research	In-depth investigation or intervention in a real-world system or organization.	Internal developers, administrators, system maintainers.	[30], [31]
Repository Mining, Corpus Analysis	Analysis of public artifacts such as source code, commits, vulnerability disclosures, or usage telemetry.	OSS maintainers, contributors, downstream users.	**[32]**, [33]
Tool Evaluation, Benchmarking	Evaluation of tools or techniques against benchmarks to assess effectiveness, efficiency, or coverage.	Tool developers, analysts, affected system operators.	**[34]**, [35], [36]
Simulation, Optimization	Modeling or optimization of system behavior under constraints or attack scenarios.	Simulated users, designers of real-world systems, policymakers.	**[37]**, [38]
Longitudinal Studies, Meta-Science	Empirical analyses of trends over time or research practices across populations of studies.	Research community, prior authors, funding agencies.	[39], [40], [41]
Systematic Review, Replication	Reproduction or synthesis of published results to assess validity, generalizability, or evidence strength.	Original study authors, readers of syntheses, methodology developers.	[42], [43]

- *The research team*: Authors of the work, who may face legal, professional, or reputational risks associated with vulnerability discovery and disclosure.
- *Adversaries*: Malicious actors who could either exploit disclosed vulnerabilities before they are patched, or use the provided security tool to discover new vulnerabilities in other software products.

Indirect Stakeholders

- *System operators*: Organizations or engineers integrating ENSs into their products (*e.g.*,, IoT device vendors, integrators).
- *End users*: Individuals using products containing vulnerable ENSs, who could be affected by service disruption or compromise.
- *Broader public*: Society at large, where IoT failures may erode trust in connected technologies or disrupt essential services.

4.1.3 Ethical Considerations

- *Risk of exploiting new vulnerabilities*: Publicly providing descriptions of new vulnerabilities could facilitate exploitation if accessed before affected systems are patched.
- *Risk of exploiting other software of similar characteristics*: Adversaries could use the tool designed in this paper to discover and exploit zero-day vulnerabilities in other network stacks or embedded software.

4.2 Example B: Empirical Software Security Study

This example represents papers concerned with empirically measuring the security of software and the effectiveness of security tools and techniques. The following analysis is on the paper "*Do Unit Proofs Work? An Empirical Study of Compositional Bounded Model Checking for Memory Safety Verification*", which will appear at ICSE 2026 [34]. Papers with similar analyses may include [46] and [47].

4.2.1 Study Overview

Organizations are increasingly adopting bounded model checking to verify the memory safety of real software. However, their methods for creating these "unit proofs" vary and are prone to errors. This increases the cost of the process and lead to missed security vulnerabilities. The goal of this work is to provide an empirical basis for the process to inform other organizations of the costs and benefits.

Problem Domain Practical compositional bounded model checking of real software.

Methods This study employed two methods:

- *Tool/Technique Evaluation*: Evaluated the effectiveness and the cost of systematic unit proofing for memory safety verification.
- *Corpus Analysis*: Analyzed the characteristics of the unit proofs used to verify real embedded operating systems.

Table 3: A summary of the stakeholder analysis examples, including example background and resulting stakeholders

Example	Context	Method	Stakeholders	
			Direct	*Indirect*
A (§4.1)	Vulnerability detection in embedded network stacks (ENS), whose flaws enable remote exploitation.	Corpus analysis of CVEs; tool design/evaluation on real ENSs	Software maintainers; research team	System operators; adversaries; end users; broader public
B (§4.2)	Organizations adopt bounded model checking but their methods vary and are error-prone, missing vulnerabilities	Process evaluation; corpus analysis of unit proofs for embedded OSs	Software maintainers; research team	System operators; adversaries; end users; broader public
C (§4.3)	Software signing adoption is uneven despite mandates, with a gap in understanding organizational challenges	Semi-structured interviews with 18 practitioners from 13 organizations	Interview participants; their organizations; research team; adversaries	Other software producers; standards bodies; software consumers; broader public
D (§4.4)	Modern apps rely on dependencies with reachable vulnerabilities, which can be mitigated with runtime defenses	Corpus analysis of library vulnerabilities; Zero-Trust Dependencies tool evaluation	System operators; software maintainers; research team; adversaries	Java maintainers; end users; broader public

4.2.2 Stakeholder Identification

Direct Stakeholders

- *Software maintainers* — Maintainers of the studied embedded software (Zephyr, Contiki-ng, RIOT-OS, FreeRTOS) and bounded model checking tools (CBMC).
- *The research team* — Authors conducting the study.

Indirect Stakeholders

- *System operators*: Organizations or engineers integrating ENSs into their products (*e.g.*,, IoT device vendors, integrators).
- *Adversaries*: Malicious actors who could exploit disclosed vulnerabilities, or be hindered if mitigations are widely deployed.
- *End users*: Individuals using products containing vulnerable ENSs, who could be affected by service disruption or compromise.
- *Broader public*: Society at large, where IoT failures may erode trust in connected technologies or disrupt essential services.

4.2.3 Ethical Considerations

- *Risk of exploiting new vulnerabilities*: Publicly providing descriptions of new vulnerabilities could facilitate exploitation if accessed before affected systems are patched.
- *Risk of exploiting other software of similar characteristics*: Adversaries could use the tool designed in this paper to discover and exploit zero-day vulnerabilities in other network stacks or embedded software.
- *Risk of downtime during patching:* Recreated defects and unit-proof results signal patching and deployment risk. Operators may face downtime risks and must plan for timely updates, regression testing, and staged rollouts to avoid service disruption while addressing memory-safety issues.

4.3 Example C: Qualitative Study of Organizational Security Practices

This example encompasses studies that investigate and measure security practices and adoption by organizations. The following analysis is on the paper "*An Industry Interview Study of Software Signing for Supply Chain Security*", which was published in USENIX 2025 [28]. Papers with similar analyses may include [48] and [49].

4.3.1 Study Overview

Industry and regulatory bodies increasingly mandate practices like software signing, yet adoption in practice remains uneven and unclear. Existing research has largely focused on technical measurements of signing prevalence, leaving a limited understanding of organizational challenges and practitioner perspectives. This paper addresses that gap by situating signing within broader industry trends, regulatory pressures, and real-world production workflows.

Problem Domain This work examines the industrial adoption of Security practices, specifically software supply chain security practices, focusing on the role and challenges of software signing in ensuring provenance and integrity of artifacts.

Methods *Interviews*: The study employed a semi-structured qualitative interview instrument with 18 senior security practitioners from 13 organizations. Responses were analyzed using thematic and framework analysis (with the Software Supply Chain Factory Model as a reference) to examine four concerns in software signing adoption — real-world practices, implementation challenges, perceived importance, and the influence of standards, regulations, and security incidents.

4.3.2 Stakeholder Identification

Direct Stakeholders

- *Interview Participants*: Practitioners who take part in the study may be at risk if their identities are not properly anonymized, as their participation could unintentionally reveal organizational practices. This exposure may lead to reputational or professional risks if flaws or poor practices are highlighted in the research.
- *Organizations of participating practitioners*: Organizations whose employees participated in this study may face reputational or regulatory scrutiny, or even security risks to their signing infrastructure, if weaknesses in their policies or practices are revealed. These risks are heightened if the identities of participating organizations are not properly anonymized.
- *The research team*: Responsible for accurate representation and avoiding overgeneralization. They must balance transparency with the risk that exposing gaps could inadvertently harm the organizations studied or aid adversaries. In addition, they face potential legal implications if participant identities or organizational details are inadvertently disclosed, violating confidentiality agreements or data protection regulations.
- *Adversaries*: Could exploit weak or absent signing, and may benefit from publicized research findings if disclosures are not carefully managed. Risks increase if the identities of participating organizations or practitioners are revealed, providing attackers with more direct targets.

Indirect Stakeholders

- *Other software producing-organizations adopting signing*: Beyond the companies directly participating in this study, other organizations that rely on software signing may also face indirect concerns if the research highlights weaknesses in current implementations. Such findings could expose gaps in industry practices, leading to reputational harm, regulatory pressure, or increased scrutiny of their signing infrastructures.
- *Standards organizations*: Bodies that produce guidelines for software signing may be indirectly affected if the research exposes gaps or ambiguities in existing standards. Such findings could challenge their credibility, but also create pressure to revise or strengthen their recommendations.
- *Software consumers*: Individuals and organizations relying on signed software products may lose confidence in the trustworthiness of signing mechanisms if research findings highlight serious flaws. While such disclosures could ultimately improve long-term security, they also risk short-term confusion or distrust among users.
- *Broader public*: Broader society may be affected if research reveals systemic weaknesses in software signing that undermine trust in critical digital infrastructure. Public confidence in software supply chain security could be eroded, potentially discouraging the adoption of secure technologies or fueling fear around the safety of connected products.

4.3.3 Ethical Considerations

- *Risk of reputational harm*: Publicly highlighting organizational shortcomings in signing practices could damage trust in individual companies or entire sectors if anonymity is not carefully maintained.
- *Risk of aiding adversaries*: Detailed descriptions of weak or absent signing may be misused by attackers to identify and exploit unprotected software supply chains.
- *Risk to participants*: Interviewees may face professional or organizational consequences if their responses are linked back to them, raising concerns about privacy and proper anonymization.
- *Regulatory and compliance exposure*: Findings could increase external scrutiny on organizations, potentially triggering audits, penalties, or stricter mandates if deficiencies are publicized.
- *Power dynamics*: Practitioners who participated in interviews may not have decision-making power over signing adoption, yet their responses could still expose organizational vulnerabilities or poor practices outside their control.
- *Societal trust*: Revealing widespread issues in signing implementations could reduce public confidence in software ecosystems and critical infrastructure that rely on them, even as the research aims to improve overall security.

4.4 Example D: Design for Security Defense

This example represents papers that introduce new architectures and designs for preventing vulnerability exploitation. The following analysis is on the paper "*ZTD-Java: Mitigating Software Supply Chain Vulnerabilities via Zero-Trust Dependencies*", which appeared at ICSE 2025 [37]. Papers with similar analyses may include [50], [51], and [52].

4.4.1 Study Overview

Modern applications rely heavily on third-party dependencies. As a result, they are susceptible to any reachable vulnerabilities within these libraries. Prior defenses were insufficient as they did not enforce zero-trust principles on the dependencies. This paper defines and measures the effect of a Zero-Trust Architecture approach as applied to runtime dependencies.

Problem Domain Preventing exploitation of vulnerabilities in third-party dependencies.

Methods We applied two distinct methods in this study:

- *Corpus Analysis:* This paper analyzed vulnerabilities in third-party libraries, popular third-party libraries, and a benchmark of real applications that use third-party libraries.

- *Tool Evaluation*: This paper presented a system design and prototype for preventing vulnerability exploitation and evaluated its effectiveness, performance overhead, and the configuration effort it requires.

4.4.2 Stakeholder Identification

Direct Stakeholders

- *System operators*: Organizations deploying software that incorporates third-party dependencies. ZTD-Java provides them with the tool to protect their application from vulnerable dependencies.
- *Software maintainers* - Maintainers of the vulnerable third-party libraries studied in the paper.
- *The research team*: Authors of the work, who may face technical, professional, or reputational risks associated with proposing security defenses.
- *Adversaries*: Malicious actors who attempt to exploit software applications through vulnerable dependencies.

Indirect Stakeholders

- *Java maintainers*: Maintainers of the Java language and the Java Development Kit.
- *End users*: Individuals and enterprises relying on software that uses third-party dependencies, whose security and privacy could be compromised by supply chain attacks.
- *Broader public*: Society at large, whose services, security, and privacy can be impacted by large-scale software supply chain compromises.

4.4.3 Ethical Considerations

- *For maintainers of studied vulnerable libraries:* By studying vulnerabilities in third-party libraries, maintainers of these libraries may face additional reputational and legal risks.
- *For adversaries:* Malicious actors can get motivation and insight from this paper to attack applications using vulnerable third-party libraries.
- *For the research team:* The research team can face legal and reputational risks if the proposed security defenses are misconfigured or cause functional errors when deployed in applications.

5 Discussion

Many papers and treatises have been written on the topic of ethics analysis in the context of cybersecurity. We contribute some of our own thoughts here: next steps for research teams after stakeholder analysis (§5.1); whether "doing no harm" might lead to a chilling effect (§5.2); and the relation between ethics analysis and the standard sections on limitations and threats to validity (§5.3).

5.1 From Stakeholder Identification to Ethics Analysis

This paper is intended to help research teams respond to the ethics requirements described in the USENIX Security 2026 Call for Papers [19], which mandates a stakeholder-based ethics analysis. By identifying stakeholder categories and providing method-informed guidance, we aim to support researchers in preparing a rigorous and transparent ethics section. Although our examples focus on stakeholder identification, we recognize that a complete ethics analysis will also involve reasoning about benefits, harms, and justifications for study design and publication. To that end, we encourage researchers to engage with relevant ethical frameworks.

Several traditions in moral philosophy can help guide reasoning about research ethics. A consequentialist approach evaluates actions based on outcomes, aiming to maximize benefit and minimize harm. A deontological approach emphasizes duties and rights, such as respecting consent and autonomy, even when outcomes are favorable. Virtue ethics focuses on the character and intentions of the researcher. These perspectives can reinforce each other or reveal tensions, especially when stakeholder interests conflict. We refer the reader to The Menlo Report and to recent work articulating how these frameworks apply in cybersecurity research [4, 6].

We further acknowledge that stakeholder identification is not a one-time process. Stakeholders are embedded within broader sociotechnical and institutional contexts, and their roles and relevance often emerge through their interactions with others. Analyzing these interactions through the ethical analysis process can reveal additional stakeholders who may not be apparent when stakeholders are considered in isolation. Thus, a comprehensive stakeholder identification process must occur iteratively with ethical analysis in order to accurately account for the stakeholder relationships.

We also note that ethical expectations may vary across institutional, national, and cultural contexts. Security researchers often work in multinational teams or study systems deployed globally. Therefore, it may be appropriate to frame stakeholder analysis within broader cultural values or legal systems. Prior work in engineering ethics and intercultural competence, including frameworks by Hofstede *et al.* [53] and analyses by Zhu *et al.* [54, 55], argues that ethical decision-making is shaped by societal norms about authority, risk, and responsibility.

5.2 Should Cybersecurity Researchers Do No Harm?

We reflect briefly on the assertion, implicit in the USENIX ethics policy, that cybersecurity research should not cause harm. This aligns with ethical norms in human subjects research and the broader computing community. Yet security research often involves adversarial contexts in which some stakeholder (*e.g.*, malicious actors) may be harmed by design. Moreover, some research may produce tools or knowledge that are dual-use. In such cases, the justification to proceed must be made cautiously and transparently, weighing harm to some against protection for others. The researcher's role is not to avoid discomfort altogether, but to act with deliberation and integrity in anticipating and mitigating harms.

Why has this shift toward formalized ethics analysis occurred now? The recent USENIX Security policy likely responds, at least in part, to high-profile controversies in the field. One notable example is the retraction of the paper "On the Nature of Hypocritical Commits" [56] from IEEE S&P, which sparked sustained debate about consent, deception, and the ethical treatment of software developers. Such cases make clear that security research can cause real harm—and that ethical oversight is necessary to maintain trust within the community and with the public.

While we do not oppose ethics standards, we also caution the research community against too abruptly shifting away from adversarial research. Adversaries are at the heart of the discipline of cybersecurity. Their capabilities are rapidly evolving, and there are active threats from both state-sponsored actors (*e.g.*, APT29 "Cozy Bear" [57], China's PLA Unit 61398 [58], the US NSA [59], and Israel's Unit 8200 [60], to name but a few) and criminal syndicates operating via the dark web [61]. These actors are not constrained by ethical review boards nor principles of research beneficence. If ethical mandates prevent researchers from exploring or disclosing certain risks, there is a real danger that defenders will be (further) outpaced by attackers. Ethical caution must be balanced with the imperative to understand, anticipate, and mitigate emerging threats.

In short: ***These ethics mandates must not create a chilling effect on cybersecurity research***. Rather, it should enable researchers to proceed conscientiously, with awareness of the possible harms and a commitment to act with integrity. We hope our guide supports that confidence, both by helping researchers think carefully about whom their work may affect, and how; and by helping peer reviewers perform pragmatic assessments of harms to real stakeholders rather than overblown hypothetical ones.

5.3 Ethics Analysis vs. Limitations and Threats to Validity

Stakeholder ethics analysis is distinct from, but complementary to, the "Limitations" and "Threats to Validity" sections found in many computing research papers. Those sections typically address the extent to which the research findings are generalizable, robust, or methodologically sound. They are primarily epistemological in focus: concerned with what we can know from the results and how confidently we can make claims. In contrast, ethics analysis is *normative*: it addresses what the researchers ought to do, what harms may arise, and what responsibilities they bear to others. Whereas a limitations section might admit that a study lacks ecological validity or statistical power, an ethics section should explain whether stakeholder interests were acknowledged and protected. Ethics analysis is structured not by research method alone but by the broader impact context of the work, and it is likely to include reflection on value-laden choices, such as whether to proceed with a study, disclose results, or disseminate findings responsibly.

6 Conclusion

Security research is conducted in a high-stakes, adversarial environment where ethical missteps can cause real harm—or prevent meaningful progress. In response to evolving expectations from the research community, we have presented a practical guide to stakeholder identification, grounded in empirical methods and accompanied by illustrative examples. Our goal is to help researchers anticipate who might be affected by their work and understand how methodological choices influence ethical exposure.

This guide may be used during project ideation, IRB preparation, or ethics section drafting. It may also assist reviewers and institutional reviewers in evaluating the completeness and clarity of submitted ethics analyses. Ultimately, we hope it enables thoughtful engagement with ethics without drifting into an overly restrictive "do no harm" mindset—one that might hinder critical inquiry rather than improving it.

Acknowledgment of Assistance

This manuscript was developed with the assistance of various iterations of ChatGPT. The human authors defined the structure and key ideas of the work. ChatGPT was used to compose much of the initial draft, subject to human supervision and revision.

References

[1] P. Rogaway, “The moral character of cryptographic work,” *Cryptology ePrint Archive*, 2015.

[2] USENIX Security Symposium 2025 Program Co-Chairs, “Message from the usenix security ’25 program co-chairs,” 2025, accessed: 2025-08-14. [Online]. Available: https://www.usenix.org/sites/default/files/sec25_message.pdf

[3] USENIX Security Symposium 2026 Program Committee, “USENIX Security ’26 Call for Papers,” 2025, accessed: 2025-07-31. [Online]. Available: https://www.usenix.org/conference/usenixsecurity26/call-for-papers

[4] D. Dittrich and E. Kenneally, “The menlo report: Ethical principles guiding information and communication technology research,” U.S. Department of Homeland Security, Tech. Rep., 2012. [Online]. Available: https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/

[5] T. L. Beauchamp and J. F. Childress, *Principles of Biomedical Ethics*, 8th ed. Oxford University Press, 2019.

[6] T. Kohno, Y. Acar, and W. Loh, “Ethical frameworks and computer security trolley problems: foundations for conversations,” in *2023 Proceedings of the 32th USENIX Security Symposium*, 2023, pp. 5145–5162.

[7] B. Friedman, P. H. Kahn Jr., and A. Borning, *Value Sensitive Design and Information Systems*. John Wiley & Sons, Ltd, 2008, ch. 4, pp. 69–101. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470281819.ch4

[8] J. S. Mill, *Utilitarianism*. Parker, Son, and Bourn, 1863.

[9] I. Kant, *Groundwork of the Metaphysics of Morals*, 1785, translated by Mary Gregor (Cambridge Unviersity Press, 2nd ed., 2012).

[10] G. Anscombe, “Modern moral philosophy,” *Philosophy*, vol. 33, no. 124, pp. 1–19, 1958.

[11] A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014.

[12] H. Sharp, A. Finkelstein, and G. Galal, “Stakeholder identification in the requirements engineering process,” in *Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99*, 1999, pp. 387–391.

[13] R. E. Freeman, *Strategic Management: A Stakeholder Approach*. Pitman Publishing, 1984.

[14] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, 2012.

[15] I. Sommerville and P. Sawyer, *Requirements Engineering: A Good Practice Guide*, 1st ed. USA: John Wiley & Sons, Inc., 1997.

[16] ——, “Viewpoints: principles, problems and a practical approach to requirements engineering,” *Annals of software engineering*, vol. 3, no. 1, pp. 101–130, 1997.

[17] National Institute of Standards and Technology, “Computer security resource center glossary: Cybersecurity,” 2024, accessed: 2025-07-31. [Online]. Available: https://csrc.nist.gov/glossary/term/cybersecurity

[18] IEEE S&P 2025 Program Committee, “Call for Papers,” 2024, accessed: 2025-07-31. [Online]. Available: https://sp2025.ieee-security.org/cfpapers.html

[19] USENIX Security Symposium 2025 Program Committee, “USENIX Security ’25 Call for Papers,” 2024, accessed: 2025-07-31. [Online]. Available: https://www.usenix.org/conference/usenixsecurity25/call-for-papers

[20] NDSS Symposium 2025 Program Committee, “NDSS Symposium 2025 Call for Papers,” 2024, accessed: 2025-07-31. [Online]. Available: https://www.ndss-symposium.org/ndss2025/submissions/call-for-papers/

[21] ACM CCS 2025 Program Committee, “Call for Papers,” 2024, accessed: 2025-07-31. [Online]. Available: https://www.sigsac.org/ccs/CCS2025/call-for-papers/

[22] A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets,” in *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 2008, pp. 111–125.

[23] J. Metcalf, E. Keller, and d. boyd, “Ethics in emerging technology: A particular focus on data and privacy,” *Journal of Information, Communication and Ethics in Society*, vol. 14, no. 2, pp. 77–92, 2016.

[24] D. Brumley, P. Poosankam, D. Song, and J. Zheng, “Automatic patch-based exploit generation is possible: Techniques and implications,” in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 143–157.

[25] T. Riebe and C. Reuter, “Dual-use and dilemmas for cybersecurity, peace and technology assessment,” in *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Springer, 2019, pp. 165–183.

[26] O. Mutlu and J. S. Kim, “Rowhammer: A retrospective,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 8, pp. 1555–1571, 2019.

[27] P. Ralph et al., “Empirical Standards for Software Engineering Research,” *arXiv:2010.03525 [cs.SE]*, 2021.

[28] K. G. Kalu, T. Singla, C. Okafor, S. Torres-Arias, and J. C. Davis, “An industry interview study of software signing for supply chain security,” in *2025 Proceedings of the 34th USENIX Security Symposium*, 2025, pp. 81–100.

[29] R. Ramesh, A. Vyas, and R. Ensafi, “"all of them claim to be the best": Multi-perspective study of VPN users and VPN providers,” in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 5773–5789. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-vpn

[30] J. Chen, X. Ma, L. Luo, and Q. Zeng, “Tracking you from a thousand miles away! turning a bluetooth device into an apple airtag without root privileges,” in *2025 Proceedings of the 34th USENIX Security Symposium*, 2025, pp. 4345–4362.

[31] C. Villa, S. Mirza, and C. Pöpper, “Exposing the guardrails: Reverse-engineering and jailbreaking safety filters in dall·e text-to-image pipelines,” in *2025 Proceedings of the 34th USENIX Security Symposium*, 2025, pp. 897–916.

[32] P. C. Amusuo, R. A. C. Méndez, Z. Xu, A. Machiry, and J. C. Davis, “Systematically detecting packet validation vulnerabilities in embedded network stacks,” in *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2023, pp. 926–938.

[33] C. Munteanu, G. Smaragdakis, A. Feldmann, and T. Fiebig, “Catch-22: Uncovering compromised hosts using ssh public keys,” in *2025 Proceedings of the 34th USENIX Security Symposium*, 2025, pp. 861–878.

[34] P. C. Amusuo, O. Cochell, T. L. Lievre, P. V. Patil, A. Machiry, and J. C. Davis, “Do unit proofs work? an empirical study of compositional bounded model checking for memory safety verification,” *arXiv preprint arXiv:2503.13762*, 2025.

[35] B. Kondracki and N. Nikiforakis, “Smudged fingerprints: Characterizing and improving the performance of web application fingerprinting,” in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4625–4640. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/kondracki

[36] S. Ullah, M. Han, S. Pujar, H. Pearce, A. Coskun, and G. Stringhini, “Llms cannot reliably identify and reason about security vulnerabilities (yet?): A comprehensive evaluation, framework, and benchmarks,” in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 862–880.

[37] P. C. Amusuo, K. A. Robinson, T. Singla, H. Peng, A. Machiry, S. Torres-Arias, L. Simon, and J. C. Davis, “ZTD$_{\text{java}}$: Mitigating software supply chain vulnerabilities via zero-trust dependencies,” in *2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE)*, 2025, pp. 1294–1306.

[38] J. Zhang, J. Huang, L. Zhao, D. Chen, and Ç. K. Koç, “ENG25519: Faster TLS 1.3 handshake using optimized x25519 and ed25519,” in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 6381–6398. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/zhang-jipeng

[39] A. Hilton, C. Deccio, and J. Davis, “Fourteen years in the life: A root Server’s perspective on DNS resolver security,” in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 3171–3186. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/hilton

[40] T. Marjanov and A. Hutchings, “Sok: Digging into the digital underworld of stolen data markets,” in *2025 IEEE Symposium on Security and Privacy (SP)*, 2025, pp. 1–18.

[41] K. Beadle, K. I. Turk, A. Eusebi, M. Tran, M. Ordekian, E. Mariconti, Y. Zou, and M. Vasek, “Sok: A privacy framework for security research using social media data,” in *2025 IEEE Symposium on Security and Privacy (SP)*, 2025, pp. 1178–1196.

[42] A. Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang, and T. Hardjono, “Sok: Security and privacy of blockchain interoperability,” in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 3840–3865.

[43] J. Liang, D. Hu, P. Wu, Y. Yang, Q. Shen, and Z. Wu, “Sok: Understanding zk-snarks: The gap between research and practice,” in *2025 Proceedings of the 34th USENIX Security Symposium*, 2025, pp. 2085–2104.

[44] S. Hebrok, S. Nachtigall, M. Maehren, N. Erinola, R. Merget, J. Somorovsky, and J. Schwenk, “We really need to talk about session tickets: A Large-Scale analysis of cryptographic dangers with TLS session tickets,” in *32nd USENIX Security Symposium (USENIX Security*

23). Anaheim, CA: USENIX Association, Aug. 2023, pp. 4877–4894. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/hebrok

[45] E. Wang, J. Chen, W. Xie, C. Wang, Y. Gao, Z. Wang, H. Duan, Y. Liu, and B. Wang, "Where urls become weapons: Automated discovery of ssrf vulnerabilities in web applications," in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 239–257.

[46] M. Busch, P. Mao, and M. Payer, "Spill the TeA: An empirical study of trusted application rollback prevention on android smartphones," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 5071–5088. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/busch-tea

[47] G. Calderonio, M. M. Ali, and J. Polakis, "Fledging will continue until privacy improves: Empirical analysis of google's Privacy-Preserving targeted advertising," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4121–4138. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/calderonio

[48] K. L. Wu, M. H. Hue, N. M. Poon, K. M. Leung, W. Y. Po, K. T. Wong, S. H. Hui, and S. Y. Chau, "Back to school: On the (In)Security of academic VPNs," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 5737–5754. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/wu-ka-lok

[49] G. t. Napel, M. van Eeten, and S. Parkin, "Speedrunning the maze: Meeting regulatory patching deadlines in a large enterprise environment," in *2025 IEEE Symposium on Security and Privacy (SP)*, 2025, pp. 504–521.

[50] Y. Chen, Q. Yin, Q. Li, Z. Liu, K. Xu, Y. Xu, M. Xu, Z. Liu, and J. Wu, "Learning with semantics: Towards a Semantics-Aware routing anomaly detection system," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 5143–5160. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/chen-yihao

[51] T. Wallez, J. Protzenko, B. Beurdouche, and K. Bhargavan, "TreeSync: Authenticated group management for messaging layer security," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 1217–1233. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/wallez

[52] Z. Cheng, Q. Lv, J. Liang, Y. Wang, D. Sun, T. Pasquier, and X. Han, "Kairos: Practical intrusion detection and investigation using whole-system provenance," in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 3533–3551.

[53] G. Hofstede, G. J. Hofstede, and M. Minkov, *Cultures and Organizations: Software of the Mind*, 3rd ed. McGraw-Hill, 2010.

[54] Q. Zhu and B. K. Jesiek, "Engineering ethics in global context: Four fundamental approaches," in *2017 ASEE Annual Conference & Exposition*, 2017.

[55] ——, "Practicing engineering ethics in global context: A comparative study of expert and novice approaches to cross-cultural ethical situations," *Science and Engineering Ethics*, vol. 26, no. 4, pp. 2097–2120, 2020.

[56] Y. Wu and K. Lu, "On the feasibility of stealthily introducing vulnerabilities in open-source software via hypocrite commit," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, retracted.

[57] Cybersecurity and Infrastructure Security Agency, "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally," 2023, accessed: 2025-07-31. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

[58] D. Mcwhorter, "Mandiant Exposes APT1 – One of China's Cyber Espionage Units – and Releases 3,000 Indicators," 2013, accessed: 2025-07-31. [Online]. Available: https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

[59] Von SPIEGEL Staff, "Documents Reveal Top NSA Hacking Unit," 2013, accessed: 2025-07-31. [Online]. Available: https://www.spiegel.de/international/world/a-940969.html

[60] "Unit 8200," accessed: 2025-08-19. [Online]. Available: https://en.wikipedia.org/wiki/Unit_8200

[61] "Internet organised crime threat assessment (iocta)," Europol, Tech. Rep., 2023. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf