



University of Vaasa
VAASAN YLIOPISTO

OSUVA Open
Science

This is a self-archived – parallel published version of this article in the publication archive of the University of Vaasa. It might differ from the original.

Doxxing as a Cybersecurity Threat: A Systematic Review

Author(s): Anti, Emmanuel; Dang, Duong; Vartiainen, Tero
Title: Doxxing as a Cybersecurity Threat: A Systematic Review
Year: 2026
Version: Publishers version
Copyright © Association for Information Systems 2026.

Please cite the original version:

Anti, E., Dang, D., & Vartiainen, T. (2026). Doxxing as a Cybersecurity Threat: A Systematic Review. *AMCIS 2026 Proceedings*, 32.
https://aisel.aisnet.org/amcis2026/sig_sec/sig_sec/32

Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2026 Proceedings

Americas Conference on Information Systems
(AMCIS)

August 2026

Doxxing as a Cybersecurity Threat: A Systematic Review

Emmanuel Anti

University of Vaasa, emmanuel.anti@uwasa.fi

Duong Dang

University of Vaasa, duong.dang@uwasa.fi

Tero Vartiainen

University of Vaasa, tero.vartiainen@uwasa.fi

Follow this and additional works at: <https://aisel.aisnet.org/amcis2026>

Recommended Citation

Anti, Emmanuel; Dang, Duong; and Vartiainen, Tero, "Doxxing as a Cybersecurity Threat: A Systematic Review" (2026). *AMCIS 2026 Proceedings*. 32.

https://aisel.aisnet.org/amcis2026/sig_sec/sig_sec/32

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2026 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Doxxing as a Cybersecurity Threat: A Systematic Review

Full Paper

Emmanuel Anti

University of Vaasa, Finland
emmanuel.anti@uwasa.fi

Duong Dang

University of Vaasa, Finland
duong.dang@uwasa.fi

Tero Vartiainen

University of Vaasa, Finland
tero.vartiainen@uwasa.fi

Abstract

Doxxing, the intentional public disclosure of personal information, has been widely examined as privacy violation, cyberbullying, and digital vigilantism, yet its cybersecurity implications remain underdeveloped. This study addresses that gap through a systematic review and interpretive coding of 34 peer-reviewed articles. The findings support a four-stage socio-technical escalation pathway comprising exposure, enrichment, exploitation, and systemic impact. The model explains how doxxing evolves through interactions among stakeholders, platform affordances, and governance constraints, enabling social engineering, impersonation, and broader organizational and societal harm without traditional system intrusion. The study extends cybersecurity research and highlights intervention points for threat modeling, organizational preparedness, and governance coordination.

Keywords

Doxxing, Cybersecurity, Threats, Socio-Technical Systems.

Introduction

Doxxing (or doxing), derived from “dropping documents (docs),” refers to the intentional, non-consensual collection, aggregation, and public disclosure of an individual’s personal or identifying information through digital systems (Douglas, 2016). Once associated with hacker rivalries, it has evolved into a broader digital practice. Disclosures commonly include names, email addresses, home locations, workplace details, identity documents, or family information, and are typically intended to intimidate, punish, coerce, or silence targets. Doxxing is primarily understood as personal information disclosure, with acts such as swatting or extortion considered downstream consequences. Prior work distinguishes deanonymizing, targeting, and delegitimizing forms, which differ in motivation but share reliance on exploiting personal data as a mechanism of harm (Douglas, 2016; Trottier, 2020).

Doxxing has become increasingly prevalent within contemporary digital infrastructures. Empirical studies document recurring, coordinated activity across social media platforms, forums, and paste sites (Karimi et al., 2022; Snyder et al., 2017), including GitHub Gists, JustPaste.it, X (formerly Twitter), Facebook, and TikTok. Research further shows that ordinary users—adolescents, professionals, activists, and public-facing workers—are frequently exposed to or affected by doxxing (Chen et al., 2019; Chen et al., 2018; Franz & Thatcher, 2023), with documented organizational consequences such as workplace violence, professional withdrawal, reputational damage, and long-term psychological harm (Wilson & Zwang, 2024; Zhou et al., 2024).

Research on doxxing spans multiple disciplines, most often conceptualizing it as online harassment, privacy violation, cyberbullying, or digital vigilantism (Douglas, 2016; Chen et al., 2018; Trottier, 2020). Psychological and behavioral studies emphasize motivations, moral approval, personality traits, and bystander responses (Fang, 2024; Foster & Cross, 2024; Lee, 2022), while sociopolitical and media research examines doxxing as denunciation, activism, or counter-surveillance, particularly in protest contexts (Buoziš, 2019; Lee, 2022; Li & Whitworth, 2023). Legal scholarship highlights ethical tensions and regulatory limits (MacAllister, 2016), and organizational research documents impacts on hiring, employee safety, and reputational risk (Roth et al., 2024).

Despite this breadth, doxxing is rarely examined through a cybersecurity lens, even though many studies implicitly describe core security elements such as threat actors, attack vectors, vulnerable information assets, detection mechanisms, and cascading impacts (Franz & Thatcher, 2023; Karimi et al., 2022; Snyder et al., 2017). Cybersecurity research in information systems has focused primarily on system intrusion and infrastructure protection, with doxxing treated instead as an issue of online safety, privacy, or content moderation (Chia et al., 2023). This separation obscures how doxxing exploits digital infrastructures and weaponizes personal data without requiring technical breach. As cybersecurity threats increasingly assume socio-technical forms, this gap becomes critical. Doxxing exemplifies this shift by targeting individuals, leveraging platform affordances that sustain visibility, and being reinforced by social acceptance, limited intervention, and governance weaknesses (Li et al., 2025; Trottier, 2020).

This study addresses this gap through a systematic literature review of 34 studies from information systems and related fields. The review examines how doxxing has been conceptualized and whether its security-relevant dynamics are explicitly or implicitly recognized. Guided by a socio-technical systems perspective, the analysis integrates findings across technical infrastructures, social processes, organizational practices, and governance arrangements, and develops an escalation model explaining how doxxing can evolve from personal data exposure into a broader cybersecurity threat.

The research questions guiding this study are: **RQ1:** *How is doxxing conceptualized in the IS and related literature?* **RQ2:** *To what extent is doxxing examined as a cybersecurity threat in the IS and related literature?*

Background

Research on doxxing spans multiple disciplinary traditions, reflecting its relevance to social interaction, political mobilization, organizational life, and digital governance. Existing studies examine how doxxing is enacted, justified, and experienced across social, political, and organizational contexts. Some situate doxxing within online subcultures and public shaming practices, framing it as informal social punishment rather than technical intrusion (Douglas, 2016). Others conceptualize doxxing as digital vigilantism, emphasizing denunciation and enforcement outside formal legal institutions (Trottier, 2020). Together, these perspectives depict doxxing as a communicative, data-driven practice reliant on visibility and circulation rather than system breach.

Psychological and behavioral research examines conditions under which doxxing emerges and is tolerated. Moral approval depends on perceived blameworthiness, proportionality, and social endorsement, and is associated with reduced empathy, moral disengagement, and Dark Triad traits (Foster & Cross, 2024; Li et al., 2024). Additional studies show that uncertainty about intervention, diffusion of responsibility, and weak perceptions of platform enforcement reduce reporting (Fang, 2024; Li et al., 2025), highlighting how individual behavior and social norms enable doxxing.

Beyond individual dynamics, sociopolitical and activist research frames doxxing as condemnation, counter-surveillance, and collective action. Discourse and media studies show how doxxing is justified through moral framing and narratives of accountability (Buoziš, 2019; Lee, 2022), while IS research documents coordinated disclosures and platform leverage during protests and political conflict (Cheung et al., 2024; Li & Whitworth, 2023). Organizational studies identify impacts on hiring, safety, retaliation risk, professional withdrawal, and democratic processes (Roth et al., 2024; Wilson & Zwang, 2024; Zhou et al., 2024; Hansen & Lim, 2019). Technical and regulatory work demonstrates detectability at scale and governance implications, while exposing regulatory limits (Snyder et al., 2017; Karimi et al., 2022; MacAllister, 2017; Chia et al., 2023). Despite this breadth, IS research rarely conceptualizes doxxing as a cybersecurity threat.

Socio-Technical Lens and Doxxing

Although the literature offers rich insight into the social, psychological, legal, organizational, and technical dimensions of doxxing, these perspectives remain largely disconnected. Socio-technical systems (STS) theory emphasizes that harm in digital systems arises not from isolated technical or human factors, but from interactions among technologies, social practices, organizational arrangements, and governance structures (Dang & Vartiainen, 2024; Baxter & Sommerville, 2011). Within IS research, STS has been widely applied to explain security failures stemming from misalignment among technical design, human behavior, and institutional controls (Sarker et al., 2019).

Viewed through this lens, existing doxxing research implicitly addresses socio-technical components, the mutual shaping of social practices and technical features, platform affordances enabling specific actions, and moral legitimation used to justify disclosure, yet lacks a coherent explanatory structure. Prior studies clarify what harms occur and why actors engage in doxxing but provide limited insight into how disclosure escalates across system levels into broader cybersecurity risk. This fragmentation motivates the present study. To address this gap, we develop an escalation model explaining how doxxing evolves into organizational vulnerability.

Methodology

This study employs a systematic literature review (SLR) guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework (Page et al., 2021). PRISMA is widely used in information systems research as a rigorous and transparent approach for identifying, screening, and synthesizing prior work, particularly in theory-building and integrative reviews. The objective of the review is to examine how doxxing is conceptualized and whether it is analyzed explicitly or implicitly as a cybersecurity threat in the IS and related literature. An SLR is appropriate given the fragmentation of doxxing research across disciplines and analytical lenses. PRISMA provides a structured process that enhances replicability, reduces selection bias, and enables defensible synthesis of heterogeneous studies.

Search Strategy

A keyword-based search strategy was developed to capture the breadth of doxxing-related scholarship while maintaining conceptual accuracy. The following search string was applied consistently across all databases: ("Doxxing" OR "Doxing" OR "Dox"). The inclusion of multiple spellings reflects variation in terminology across disciplines and publication venues. Searches were conducted across five major academic databases (ACM Digital Library, AIS Electronic Library, IEEE Xplore, Web of Science, and Scopus) to ensure coverage of technical, organizational, and socio-political perspectives. To reflect the period during which doxxing has become increasingly prevalent and systematically studied, the search was limited to publications from 2017 to 2025, as doxxing has evolved from a relatively fringe online practice into a persistent and scalable phenomenon with documented impacts across social, organizational, and institutional contexts.

Identification of Articles

The initial database search yielded 236 records. Table 1 summarizes the distribution of identified articles by database. All records were exported and consolidated into a single dataset for screening and duplicate removal.

Database	Articles Identified
ACM Digital Library	123
AIS Electronic Library	7
IEEE Xplore	13
Web of Science	80
Scopus	13
Total	236

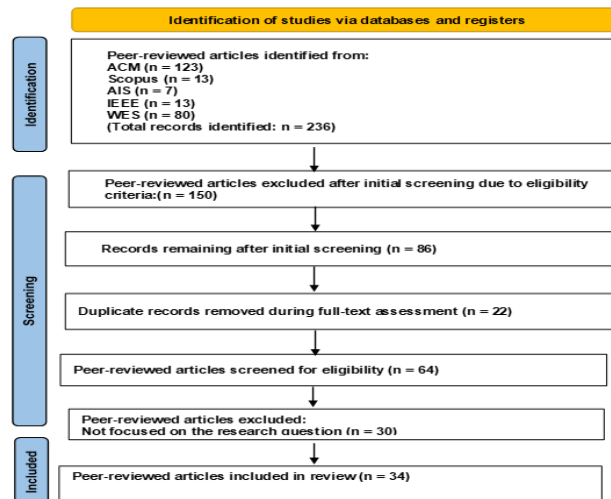
Table 1: Identified Articles

Screening and Eligibility

The screening process began with a title and abstract review to assess whether studies met the inclusion criteria, including topical relevance to doxxing, peer-reviewed status, language, and publication timeframe. At this stage, articles were evaluated for whether they substantively examined doxxing within digital or socio-technical contexts. Studies were excluded if “dox” was used in unrelated contexts, if doxxing was mentioned only in passing, or if the publication was not peer-reviewed.

Studies passing the initial screening underwent full-text review to determine eligibility for inclusion in the final synthesis. This stage involved assessing each article’s conceptual focus, methods, findings, and contribution to understanding doxxing-related mechanisms, impacts, governance, or responses. Duplicate records were removed, and additional studies were excluded if they addressed online harassment or cyberbullying broadly without isolating doxxing as a distinct phenomenon, or if they lacked relevance to digital or socio-technical systems.

Following this multi-stage screening, 34 articles were retained for final review. These studies provided empirical, conceptual, or theoretical insights into doxxing and constituted the analytical sample for examining how the phenomenon has been treated in information systems and related literature. Figure 1 illustrates the screening process.


Figure 1: Prisma Flowchart Diagram

Data Extraction and Synthesis

Data was systematically extracted from the 34 included articles using a structured, predefined coding scheme. Extracted information captured key characteristics relevant to the study’s objectives, including the research context and domain, theoretical framing, conceptualization of doxxing, research methods, and findings. In addition, particular attention was paid to identifying whether and how each study addressed cybersecurity-related elements, including threat actors, information assets, vulnerabilities, detection mechanisms, and governance structures.

The coding process followed an iterative and abductive approach. Initial open coding identified recurring concepts and themes across studies, followed by axial coding to organize these into higher-level analytical categories. Broader online harassment and cyberbullying literature was considered during screening but retained only when doxxing constituted a distinct analytical focus. Throughout the process, studies were classified according to whether cybersecurity concerns were addressed explicitly, implicitly, or not at all, and this distinction informed both coding and synthesis. To mitigate interpretive bias, coding definitions were iteratively refined through repeated comparison across studies. Consistent with the study’s integrative

aim, the synthesis was interpretive and theory driven. A socio-technical systems perspective guided the integration of findings across technical, social, organizational, and governance dimensions.

Findings

Conceptualizations of Doxxing

This systematic literature review of 34 studies shows that, while doxxing is widely recognized as harmful, it is conceptualized through fragmented lenses such as online harassment, privacy violation, cyberbullying, digital vigilantism, and political activism. Analyzed through a socio-technical systems lens, the findings reveal a consistent pattern: doxxing targets information and human assets, exploits digital infrastructures, is sustained by social norms and moral legitimization, and produces cascading harms across individual, organizational, and societal levels. Conceptualizations capture the dominant framings in the literature, while cybersecurity elements were identified through interpretive coding of security-relevant dynamics. Collectively, these findings demonstrate that doxxing constitutes a socio-technical cybersecurity threat, even when not explicitly labeled as such. Table 2 summarizes the dominant conceptualizations across the 34 studies and the extent to which cybersecurity-related elements are explicitly or implicitly addressed.

Escalation Phase	Conceptualizations	Cybersecurity Elements	Articles
Data Exposure	Privacy Violation; Cyberbullying	Confidentiality loss; personal data disclosure; psychological harm	(Chen et al., 2019, 2018; Douglas, 2016; Karimi et al., 2022; Kukul, 2023; Li et al., 2024; Logie & Maras, 2024; Schuster et al., 2024; Snyder et al., 2017)
Data Enrichment	Digital Vigilantism; Activism	Data aggregation; relational mapping; coordinated targeting; threat amplification	(Anderson, 2025; Barry, 2021; Buoziš, 2019; Cheung et al., 2024; Hansen & Lim, 2019; Jaccoud et al., 2023; Lee, 2022; Li & Whitworth, 2023; Trottier, 2020)
Exploitation	Psychological; Behavioral	Threat motivation; deterrence failure; impersonation; social engineering	(Anderson & Wood, 2022; Fang, 2024; Foster & Cross, 2024; Franz & Thatcher, 2023; Li et al., 2024, 2025)
Systemic Impact	Organizational Risk; Legal/Regulatory; Technical Detection	Governance gaps; retaliation risk; detection limitations; institutional vulnerability	(Chia et al., 2023; MacAllister, 2016; Roth et al., 2024)

Table 2 : Conceptualizations of Doxxing

A deeper analysis reveals a pattern not made explicit in much of the doxxing literature. Doxxing functions as an enabling condition for broader cybersecurity threats rather than as a discrete, isolated act. While existing studies conceptualize doxxing as a privacy violation, cyberbullying, digital vigilantism, psychological harm, organizational risk, or a technical detection issue, this review identifies an escalation pathway through which these elements combine data weaponization and amplified threat impact. Progression reflects a conditional escalation pathway in which later stages become possible when enabling conditions are present; not all incidents move through every phase, but together they illustrate how exposure can evolve into systemic harm

Data Exposure: Studies framing doxxing as a privacy violation and cyberbullying emphasize the intentional disclosure of personally identifiable information (PII) through harassment and vigilantism across social media platforms, forums, and paste sites (Douglas, 2016; Chen et al., 2018, 2019). Disclosed information, names, email addresses, physical locations, job titles, and family details represent a loss of confidentiality and control, often producing psychological distress and withdrawal from digital

participation (Logie & Maras, 2024). Once exposed, this information becomes searchable, persistent, and readily redistributable, creating a public pool of sensitive data that is vulnerable to downstream misuse (Karimi et al., 2022).

Data Enrichment: Research in activist, political, and organizational contexts shows how exposed PII is aggregated with other publicly available sources, including social media profiles, professional directories, and online databases (Li & Whitworth, 2023; Cheung et al., 2024). Through enrichment and network mapping, actors can connect individuals to broader personal and professional networks, revealing affiliations, social ties, and trust relationships (Trottier, 2020; Lee, 2022). Targeting, therefore, expands from individuals to groups and institutions. At this stage, isolated disclosures are transformed into relational datasets that enable coordinated targeting and systemic exposure (Buozis, 2019).

Exploitation: Psychological and behavioral studies explain why enriched data facilitates impersonation and social engineering once trust relationships are identifiable Foster & Cross, 2024; Fang, 2024; Li et al., 2024, 2025). Moral legitimization, reduced skepticism, and bystander inaction normalize disclosure, weaken sanctions, and lower deterrence, reducing perceived perpetrator risk..(Franz & Thatcher, 2023). Leveraging enriched datasets, attackers can craft credible phishing messages, impersonate colleagues or authorities, and manipulate routine workflows. Although rarely labeled as cyberattacks in the reviewed literature, these practices closely resemble established forms of credential abuse and social engineering.

Systemic Impact: Organizational, legal, and regulatory research documents how consequences extend beyond individual victims (MacAllister, 2016; Roth et al., 2024; Chia et al., 2023). Doxxing-related incidents disrupt operations, heighten retaliation and safety risks, damage reputations, and erode institutional trust (Wilson & Zwang, 2024; Zhou et al., 2024). In some cases, enriched data can enable unauthorized access, financial loss, or strategic disruption, particularly when governance gaps, jurisdictional limits, and weak coordination constrain responses. Emerging technologies, including AI-enabled impersonation and deep-fakes, further amplify these risks. The absence of systematic detection, monitoring, and early warning mechanisms allows incidents to escalate from personal harm to broader digital and organizational vulnerabilities.

Doxxing Threat Escalation Pathway Model

We further examine our findings through the lens of socio-technical systems to develop a socio-technical escalation pathway model for doxxing. In this model, social, technical, and environmental antecedents/enablers interact with perpetrator actions to produce escalating impacts on victims, organizations, and society. Figure 2 illustrates the socio-technical escalation pathway for doxxing as a cybersecurity threat. The model comprises four stages; details are discussed in the Discussion section.

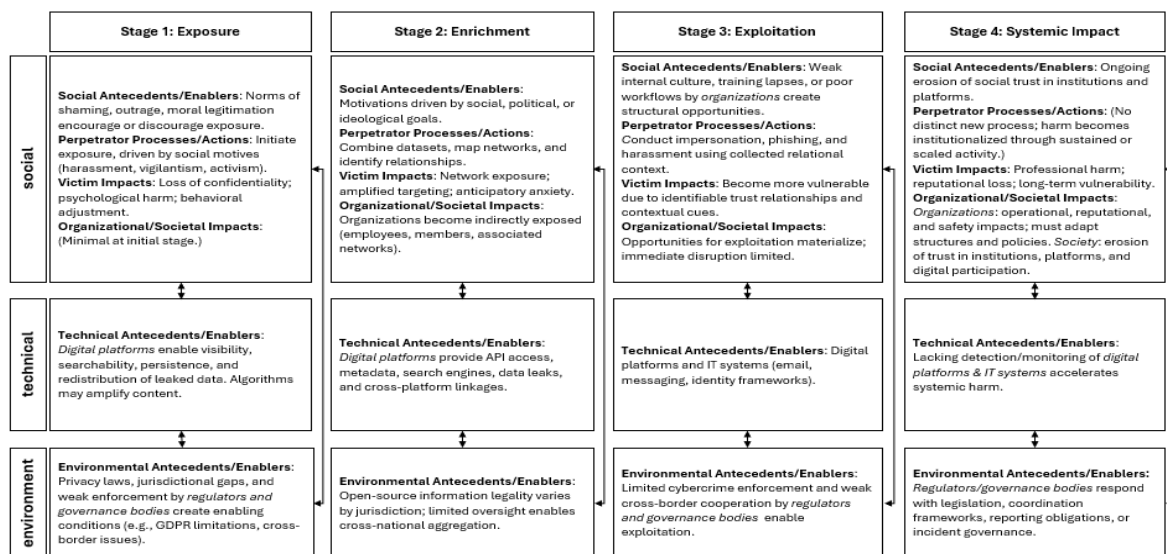


Figure 2: Doxxing Threat Escalation Pathway

Discussion and Conclusion

Reframing doxxing as a socio-technical cybersecurity threat

The socio-technical escalation pathway for doxxing as a cybersecurity threat model (Figure 2) positions doxxing as a staged socio-technical escalation process rather than an isolated incident type. Exposure, enrichment, exploitation, and systemic impact are not merely sequential steps; they are stages in which social, technical, and environmental elements co-determine escalation trajectories. At each stage, the model delineates a coherent flow from antecedents/enablers to perpetrator processes and, in turn, to impacts on victims, organizations, and society.

First, the Exposure Phase marks the onset of escalation, where social norms of outrage and moral legitimization, combined with platform affordances of visibility, searchability, persistence, and algorithmic amplification, enable initial disclosure (Anderson & Wood, 2021; Treem & Leonardi, 2013). Perpetrators, motivated by harassment, vigilantism, or activism, initiate the act. Victims immediately lose confidentiality and experience psychological harm, prompting behavioral changes. Environmental factors (e.g., jurisdictional gaps and weak enforcement) allow the information to persist and spread. At this stage, organizational and broader societal impacts remain limited. From an STS perspective, exposure emerges from the interaction of platform design and regulatory gaps, transforming individual actions into sustained structural vulnerability.

Second, the Enrichment Phase occurs as exposed data is aggregated and relationally mapped across interconnected platforms. Technical antecedents (APIs, metadata, search engines, cross-platform linkages, and data leaks) and environmental variation in open-source legality facilitate large-scale combination of datasets (Chia et al., 2023; MacAllister, 2016). Perpetrators, driven by social, political, or ideological goals, map networks and identify relationships (Li & Whitworth, 2023; Cheung et al., 2024; Lee, 2022). Victims face network exposure and anticipatory anxiety; organizations become indirectly exposed through employees and associated networks. This stage transitions isolated disclosure into coordinated targeting capability within interacting socio-technical subsystems.

Third, the Exploitation Phase operationalizes enriched intelligence within organizational and technological contexts. Social antecedents (e.g., identifiable trust relationships and weak organizational security cultures) and digital infrastructure (e.g., email, messaging, and identity frameworks) create openings for social engineering without requiring technical breaches (Workman et al., 2008). Perpetrators deploy impersonation, phishing, and harassment using relational context. Victims become markedly more vulnerable; environmental factors (e.g., limited cybercrime enforcement and cross-border cooperation) sustain the phase (Wong et al., 2021). Organizational impacts begin to materialize as internal weaknesses are exploited. Threat formation thus becomes operational without a technical breach.

Fourth, the Systemic Impact Phase reflects the institutionalization of harm. Technical shortcomings (e.g., insufficient detection, monitoring, and early warning mechanisms) accelerate propagation (Schoenebeck et al., 2023), while AI-enabled impersonation tools enhance scale, precision, and effectiveness (Singh, 2025; Anti & Dang, 2025). Victims suffer professional and reputational damage with long-term vulnerability (Douglas, 2016). Organizations face operational disruptions, reputational erosion, and safety risks that require structural adaptation. Society experiences eroded trust in institutions and digital platforms. Environmental responses—including new legislation, coordination frameworks, and reporting obligations—represent post-incident governance attempts, though jurisdictional fragmentation often limits effectiveness. Systemic impact reflects governance misalignment and failure of distributed control, completing the escalation from disclosure to institutional insecurity.

Cross-stage mechanisms and non-linearity in doxxing

The model conceptualizes doxxing as a socio-technical cyber threat through a non-linear mechanism. Drawing on socio-technical systems theory (Baxter & Sommerville, 2011; Dang & Vartiainen, 2024), doxxing is framed as a conditional escalation pathway. The pathway explains how disclosure progresses through exposure, enrichment, exploitation, and systemic impact when affordances, norms, routines, and governance gaps align. These stages are configurations in which social, technical, and environmental conditions jointly shape escalation. At each stage, it traces a flow from antecedents and enabling conditions to perpetrator processes and impacts on victims, organizations, and society. Escalation is non-deterministic, depending on relational connectivity, weak deterrence, and limited institutional

coordination. This framing distinguishes doxxing from conventional social engineering by conceptualizing it as a legitimized form of data mobilization (Buoziš, 2019; Lee, 2022; Trottier, 2020) that enables coordinated misuse of personal information across networked platforms without requiring system intrusion (Douglas, 2016; Anderson & Wood, 2021; Li & Whitworth, 2023).

Roles evolve across stages (Figure 2). Perpetrators shift from initiating exposure to curating linked data, conducting exploitation campaigns, and ultimately reorganizing, migrating, professionalizing, or exiting under pressure. Victims transition from confidentiality loss to network exposure and anticipatory anxiety, heightened susceptibility during exploitation, and longer-term professional and reputational vulnerability. Organizations move from indirect exposure to workflow compromise and broader operational, safety, and reputational impacts. Platforms and regulators jointly shape the opportunity structure through affordances, moderation practices, and cross-border governance constraints (Treem & Leonardi, 2013; Chia et al., 2023), while public legitimation influences response dynamics.

Implications

This review demonstrates that doxxing operates as a staged socio-technical risk process rather than an isolated disclosure. Prior research identifies vulnerable information assets (Douglas, 2016; Chen et al., 2018), motivated actors (Trottier, 2020; Foster & Cross, 2024), scalable harm (Cheung et al., 2024; Hansen & Lim, 2019), and partial detection mechanisms (Snyder et al., 2017; Karimi et al., 2022), but largely treats these elements in isolation. Our model integrates them into a coherent explanation of escalation from exposure to systemic impact across technical, social, organizational, and governance subsystems.

Theoretically, our model reframes doxxing as a socio-technical cybersecurity threat emerging from nonlinear interactions among social actors, platform affordances, and regulatory environments (Baxter & Sommerville, 2011; Dang & Vartiainen, 2024), rather than a linear incident sequence. Integrating doxxing and digital vigilantism research (Douglas, 2016; Trottier, 2020) with socio-technical systems theory, this research explains how visibility, searchability, and persistence enable amplification (Treem & Leonardi, 2013) and how enriched context facilitates social engineering that propagates to organizational and societal levels. The model extends prior conceptualizations (Douglas, 2016; Anderson & Wood, 2021) by foregrounding staged role dynamics among perpetrators, victims, organizations, platforms, and regulators.

In practice, framing doxxing as a socio-technical escalation pathway provides CISOs and policymakers with a basis for incorporating it into threat modeling, risk assessment, and incident response planning. Mitigation focused solely on content removal or privacy violations is insufficient; effective governance requires controls addressing amplification dynamics, organizational readiness, and coordinated responses across platforms, security teams, and regulatory authorities, including privacy-by-design settings, digital footprint management, targeted awareness training, and organizational policies protecting employees from personal data exposure.

Future Research Directions

Future IS research should empirically examine conditional transitions between exposure, enrichment, exploitation, and systemic impact to identify when escalation is interrupted or amplified. Studies should assess how platform affordances, governance fragmentation, and organizational security culture jointly shape progression across phases. Experimental and longitudinal designs could evaluate intervention points, including visibility controls, relational mapping constraints, and coordinated incident response mechanisms. Comparative research across regulatory regimes is needed to understand how institutional configurations influence escalation dynamics. Advancing such work will refine the model's boundary conditions and extend theory on human-centered, infrastructure-mediated cybersecurity risk.

REFERENCES

- Anderson, B. (2025). Doxxing to destroy: The convergence of transphobic hate speech and non-consensual disclosure on X. *Crime, Media, Culture*, 17416590251345736.
- Anderson, B., & Wood, M. A. (2021). Doxxing: A Scoping Review and Typology. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. <https://doi.org/10.1108/978-1-83982-848-520211015>

- Anderson, B., & Wood, M. A. (2022). Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing. *International Journal for Crime, Justice and Social Democracy*, 11(1), 196–209.
- Anti, E., & Dang, D. (2025). Impact of Artificial Intelligence on Employee Strain and Insider Deviance in Cybersecurity. *PACIS 2025 Proceedings*.
- Barry, P. B. (2021). Doxing racists. *The Journal of Value Inquiry*, 55(3), 457–474.
- Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1), 4–17.
- Buoziš, M. (2019). Doxing or deliberative democracy? Evidence and digital affordances in the Serial subReddit. *Convergence*, 25(3), 357–373.
- Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. *International Journal of Environmental Research and Public Health*, 16(2), 218.
- Chen, Q., Chan, K. L., & Cheung, A. S. Y. (2018). Doxing victimization and emotional problems among secondary school students in Hong Kong. *International Journal of Environmental Research and Public Health*, 15(12), 2665.
- Cheung, C. M., Risius, M., & Fang, Y. (2024). Pursuing social justice through doxing on social media: implications of the 2019 Hong Kong protests. *Mis Quarterly*, 48(4).
- Chia, S. C., Sun, Y., Lu, F., & Gudmundsdottir, A. (2023). Doxing, regulation, and privacy protection: Expanding the behavioral consequences of the third-person effect. *Asian Journal of Communication*, 33(3), 289–307.
- Dang, D., & Vartiainen, T. (2024). Exploring socio-technical gaps in the cybersecurity of energy informatics for sustainability. In *Adoption of emerging information and communication technology for sustainability* (pp. 288–304). CRC Press
- Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18(3), 199–210.
- Fang, Y. (2024). *Bystanders' Perceptions and Reporting Responses in Doxing Cases: The Influence of Online Social Dynamics*.
- Foster, S., & Cross, J. (2024). Dark doxxing: How Dark Triad traits impact support for doxxing behaviors. *Personality and Individual Differences*, 217, 112432.
- Franz, A., & Thatcher, J. B. (2023). *Doxing and doxeees: A qualitative analysis of victim experiences and responses*.
- Hansen, I., & Lim, D. J. (2019). Doxing democracy: Influencing elections via cyber voter interference. *Contemporary Politics*, 25(2), 150–171.
- Huey, L., Ferguson, L., & Towns, Z. (2025). “Cops Need Doxxed”: Releasing Personal Information of Police Officers as a Tool of Political Harassment. *Crime & Delinquency*, 71(3), 714–739.
- Jaccoud, L., Molnar, L., & Aebi, M. F. (2023). Antifa’s political violence on Twitter: A grounded theory approach. *European Journal on Criminal Policy and Research*, 29(3), 495–513.
- Karimi, Y., Squicciarini, A., & Wilson, S. (2022). Automated detection of doxing on twitter. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), 1–24.
- Kukul, B. (2023). Personal data and personal safety: Re-examining the limits of public data in the context of doxing. *International Data Privacy Law*, 13(3), 182–193.
- Lee, C. (2022). Doxxing as discursive action in a social movement. *Critical Discourse Studies*, 19(3), 326–344.
- Li, Y.-J., Cheung, C. M., Shen, X.-L., & Lee, M. K. (2024). Doxing on Social Networking Sites: An Extension of the Social Cognitive Theory of Moral Thought and Action. *Journal of the Association for Information Systems*, 25(6), 1466–1499.

- Li, Y.-J., He, Z.-Z., Cheung, C. M., Shen, X.-L., & Lee, M. K. (2025). An integrated model of ambivalence and deterrence of bystander inaction in delegitimizing doxing. *Information & Management*, 62(3), 104118.
- Li, Y.-T., & Whitworth, K. (2023). Data as a weapon: The evolution of Hong Kong protesters' doxing strategies. *Social Science Computer Review*, 41(5), 1650–1670.
- Logie, K., & Maras, M.-H. (2024). Doxing: How a darknet shop created the blackmail as a service business model. *Journal of Aggression, Conflict and Peace Research*, 16(4), 348–362.
- MacAllister, J. M. (2016). The doxing dilemma: Seeking a remedy for the malicious publication of personal information. *Fordham L. Rev.*, 85, 2451.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., & others. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery*, 88, 105906.
- Roth, P. L., Bobko, P., Shan, G., Roth, R. W., Ferrise, E., & Thatcher, J. B. (2024). Doxing, political affiliation, and type of information: Effects on suspicion, perceived similarity, and hiring-related judgments. *Journal of Applied Psychology*, 109(5), 730.
- Schoenebeck, S., Lampe, C., & Triêu, P. (2023). Online Harassment: Assessing Harms and Remedies. *Social Media + Society*, 9(1), 20563051231157297. <https://doi.org/10.1177/20563051231157297>
- Schuster, J., Franz, A., & Benlian, A. (2024). *What Makes Doxing Good or Bad? Exploring Bystanders' Appraisal and Responses to the Malicious Disclosure of Personal Information*.
- Singh, J. (2025). Navigating AI-Enhanced Social Engineering: Strategies for Countering Modern Threats. 2025 2nd International Conference on Software, Systems and Information Technology (SSITCON), 01–08.
- Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. *Proceedings of the 2017 Internet Measurement Conference*, 432–444.
- Solo, A. M. (2023). Preventing Twitter from Being Used for Defamation, Doxing, Impersonation, Threats of Violence, and Intimate Images. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, 2265–2271.
- Solo, A. M. (2024). Preventing Facebook from Being Used for Defamation, Doxing, Impersonation, Threats of Violence, and Intimate Images. *Global Congress on Emerging Technologies (GCET-2024)*, 184–190.
- Stäcker, D., Franz, A., & Hett, J. (2025). *Opening Pandora's Dox: Investigating Dynamics Among Doxing Actors Within Online Environments*.
- Treem, J. W., & Leonardi, P. M. (2013). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Annals of the International Communication Association*, 36(1), 143–189.
- Trottier, D. (2020). Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime*, 21(3–4), 196–212.
- Wilson, R. C., & Zwang, K. (2024). Call to Action: Supporting Teams when Cyberbullying and Doxing Occurs a New Form of Workplace Violence. *Nurse Leader*, 22(5), 520–525.
- Wong, R. Y. M., Cheung, C. M., Xiao, B., & Thatcher, J. B. (2021). Standing up or standing by: Understanding bystanders' proactive reporting responses to social media harassment. *Information Systems Research*, 32(2), 561–581.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816.
- Zhou, A. E., Rao, I. H., Jain, N. P., Gronbeck, C., Sloan, B., Grant-Kels, J. M., & Feng, H. (2024). Ethics of doxxing and cyberbullying in dermatology. *Clinics in Dermatology*, 42(6), 730–732.