The Easta Journal Law and Human Rights
Vol. 4, No. 03, June 2026, pp. 293 – 301
ISSN: 2985-7112, DOI: 10.58812/eslhr.v4i03

The Formulation of Cyber Responsibility Resonance Theory within the Framework of Criminal Law

Aryono[1], Yekti Mahardika[2]
[1] Universitas Duta Bangsa Surakarta, Central Java, Indonesia
[2] Pengadilan Negeri Ungaran, Semarang, Central Java, Indonesia

Article Info

Article history:
Received May, 2026
Revised May, 2026
Accepted Jun, 2026

Keywords:

Criminal Law;
Cyber Responsibility Resonance Theory (CRRT);
Digital Crime.

ABSTRACT

The rapid advancement of information technology has given rise to increasingly complex, distributed, and transnational forms of cybercrime, thereby presenting new challenges to conventional concepts of criminal responsibility. This study aims to formulate the *Cyber Responsibility Resonance Theory (CRRT)* as a novel theoretical model in cybercriminal law that provides a more comprehensive framework for understanding liability within digital ecosystems. The research adopts a normative-conceptual method with a theoretical-constructive approach, drawing upon literature review and descriptive-interpretative qualitative analysis of Causality Theory, Network Society Theory, and Actor-Network Theory. The findings indicate that criminal responsibility in cyberspace is no longer linear or strictly individual, but is instead constituted through dynamic interactions among causality, digital networks, and resonance effects involving humans, technologies, and systems simultaneously. CRRT thus reconstructs the traditional paradigm of *causal liability* toward *resonant liability*, emphasizing distributed responsibility within interconnected digital networks. Case simulations further demonstrate that the impact of cybercrime may expand systemically, implicating not only primary perpetrators but also digital platforms and other network actors. Accordingly, CRRT contributes a conceptual advancement to cybercriminal law by offering a framework that is more adaptive, responsive, and aligned with the evolving nature of contemporary digital crime.

Corresponding Author:

Name: Aryono
Institution: Universitas Duta Bangsa Surakarta, Jl. Ki Mangunsarkoro No.20, Nusukan, Kec. Banjarsari, Kota Surakarta, Jawa Tengah, Indonesia
Email: aryono@udb.ac.id

1. INTRODUCTION

The rapid development of information technology has fundamentally transformed social and legal systems, particularly within criminal law, which now faces increasingly complex and transnational forms of cybercrime [1], [2]. Cybercrime is no longer merely a conventional form of offending transferred into digital environments; rather, it has evolved into a network-based phenomenon characterized by anonymity, high velocity, and large-scale scalability [3]. From a modern criminological

perspective, cybercrime encompasses both cyber-dependent and cyber-enabled offenses, thereby requiring a more adaptive and multidimensional legal approach [2]. Consequently, the renewal of criminal responsibility concepts becomes an unavoidable necessity in responding to digital transformation [4].

Empirically, the incidence of cybercrime has increased significantly at both global and national levels [5]. Offenses such as phishing, hacking, and online fraud demonstrate a sharp upward trend in line with the digitalization of public services and economic systems [6]. Studies indicate that the impact of cybercrime extends beyond economic losses, encompassing social, psychological, and even political harm [7]. Moreover, the trans-jurisdictional nature of cybercrime creates substantial challenges for law enforcement, as national legal frameworks often struggle to reach perpetrators operating beyond territorial boundaries [1].

In practice, real-world cases of online fraud in Indonesia illustrate the complexity of cybercrime involving multiple modus operandi such as phishing, social engineering, and digital identity manipulation. According to *Kompas*, losses resulting from online fraud have reached trillions of rupiah and affected thousands of victims. Cases involving fictitious online investment schemes and fraudulent social gathering platforms demonstrate that perpetrators are not limited to individuals but often operate within organized networks. This phenomenon reflects the networked nature of cybercrime, which generates wide-ranging and cascading effects [8].

From a normative perspective, criminal law is expected to ensure legal certainty, justice, and utility in addressing cybercrime developments [9]. However, existing regulations, including the Indonesian Electronic Information and Transactions Law (ITE Law), still face limitations in addressing the complexity of cybercrime, particularly in determining criminal liability within distributed criminal structures [10]. This indicates a gap between normative legal expectations and empirical law enforcement realities, necessitating a new approach capable of integrating technological, social, and legal dimensions within a unified theoretical framework.

Previous studies have proposed various approaches to understanding cybercrime. Kigerl (2012) explains cybercrime determinants through Routine Activity Theory [1], while Djanggih and Qamar (2018) examine cybercrime from classical criminological perspectives such as strain theory and social control theory [6]. Meanwhile, Dupont and Holt (2022) emphasize the importance of an interdisciplinary approach between criminology and cybersecurity studies [8]. These studies predominantly focus on causal factors and preventive mechanisms. However, a significant research gap remains, namely the absence of a theoretical formulation that specifically explains criminal responsibility within a dynamic and networked digital system [7].

Existing literature tends to prioritize technical or criminological dimensions, without sufficiently developing a concept of criminal liability that accounts for resonance effects in cybercrime [11]. In digital reality, a single action may trigger extensive consequences involving multiple actors and interconnected systems [12]. This gap has contributed to weaknesses in criminal law constructions in addressing cybercrime. Law enforcement authorities often face difficulties in identifying principal offenders and those who bear contributory responsibility within digital criminal networks [13]. Furthermore, the multidimensional impacts of cybercrime have not been fully accommodated within existing legal frameworks [7], potentially resulting in injustice for victims and reduced effectiveness of law as an instrument of social control.

Based on these considerations, this study aims to construct a novel theoretical formulation in criminal law capable of comprehensively explaining criminal responsibility within cyberspace [12], [14], [15]. Accordingly, this research proposes the *Cyber Responsibility Resonance Theory*, which

posits that criminal responsibility in cybercrime is not solely individual in nature but also produces resonance effects within digital networks, generating broader social and systemic consequences. This theory is expected to contribute to the development of criminal law that is more adaptive, responsive, and relevant to the demands of the digital era.

2. LITERATURE REVIEW

2.1 The Causation Theory

Developed by von Kries, originates from a legal-philosophical effort to explain the rational relationship between human conduct and its consequences within the framework of criminal liability. Conceptually, this theory is supported by several key indicators, namely: (1) *factual causation* (conditio sine qua non), which examines whether the outcome would have occurred without the act; (2) *legal causation*, which filters causally relevant factors that are normatively attributable; (3) *proximate cause*, which assesses the closeness of the causal link without the intervention of intervening factors; and (4) *foreseeability*, which evaluates the offender's capacity to anticipate the consequences of their actions [16]. In cyberspace, these indicators undergo conceptual expansion, as causal relations are no longer linear but instead complex, multilayered, and distributed across digital networks, thereby opening a conceptual space for the development of "resonance-based causality" as an evolution of classical causation theory.

2.2 The Network Society Theory

Popularized by Manuel Castells, conceptualizes modern social structures as dynamic, flexible, and globally interconnected networks. Philosophically, this theory can be identified through several core indicators: (1) *nodes*, representing individuals or entities within the network; (2) *flows*, referring to streams of information, power, or capital; (3) *connectivity*, indicating the degree of interconnection among nodes; (4) *flexibility*, describing the network's adaptive capacity to change; and (5) *scalability*, which enables the network to expand beyond geographical limitations [17]. Within the context of cybercriminal law, these indicators emphasize that crime is no longer an individual act but rather the product of interactions within a digital network ecosystem. Consequently, criminal responsibility must be understood as a distributed phenomenon embedded within interconnected systems.

2.3 Actor-Network Theory (ANT)

Developed by Bruno Latour, offers an ontological approach that positions both human and non-human entities as equally significant actors in the construction of social reality. This theory is grounded in several key indicators: (1) *actors/actants*, encompassing both humans and technological entities; (2) *network relations*, which describe the interconnections among actors; (3) *translation*, referring to the negotiation and transformation of meaning between entities; (4) *generalized symmetry*, which rejects hierarchical distinctions between humans and technology; and (5) *stabilization of networks*, which reflects the formation of stable relational patterns through repeated interactions [18]. In cybercriminal law, these indicators demonstrate that technologies such as algorithms, digital platforms, and information systems are not merely passive tools but active participants in producing legal consequences. Accordingly, criminal responsibility may be understood as a relational phenomenon involving heterogeneous actors within a network that generates cascading or "resonant" effects.

3. METHODS

The research method employed in this study is normative-conceptual in nature, utilizing a theoretical-constructive approach. Rather than focusing on statutory analysis, the study emphasizes the development of

scholarly ideas through the synthesis and reconstruction of relevant theories within criminal law, criminology, and cyber studies. This research is conducted through library-based research (*library research*), involving the examination of academic literature, peer-reviewed journals, and doctrinal writings of legal scholars in order to identify key conceptual foundations related to criminal responsibility in digital environments. Furthermore, the analytical technique applied is descriptive-interpretative qualitative analysis. This involves elaborating, interpreting, and critically examining existing theoretical concepts to identify their limitations, inconsistencies, and conceptual gaps. Such a process serves as a systematic synthesis and integration aimed at constructing a new theoretical formulation, namely the Cyber Responsibility Resonance Theory. The study adopts both deductive and reflective reasoning to produce a conceptual framework that is comprehensive, logically coherent, and contextually relevant to the evolving dynamics of contemporary cybercrime.

4. RESULTS AND DISCUSSION

4.1 Conceptualization of the Cyber Responsibility Resonance Theory

Based on a synthesis of Causation Theory (von Kries), Network Society Theory (Castells), and Actor-Network Theory (Latour), it is argued that the central problem of criminal liability in cyberspace lies in the dispersion of causality, fragmentation of actors, and the non-linear interconnectivity of systemic relations. In response to this conceptual challenge, this study develops a novel theoretical model, namely the *Cyber Responsibility Resonance Theory (CRRT)*.

CRRT conceptualizes criminal responsibility as a form of *resonance* a reverberating chain of accountability that spreads within digital networks as a result of continuous interactions between humans, technologies, and systems that mutually influence one another in a non-linear manner. In this sense, responsibility is no longer static or confined to a single actor, but dynamically distributed across interconnected nodes within the digital ecosystem.

Philosophically, this theory represents a paradigmatic shift:

a. From causal liability → to resonant liability
b. From individual culpability → to distributed responsibility
c. From linear causation → to networked causation

4.2 Theoretical Formulation (Conceptual Model)

The CRRT can be simplified into the following conceptual formulation without losing its philosophical substance:

$$R_{CRRT} = (C \times NAT) \times R$$

Where:

a. C (Causality Index) represents the juridical foundation of conduct, consisting of:
   1) Factual causation
   2) Legal causation
   3) Proximate causation
   4) Foreseeability
b. NAT (Network–Actor–Technology System) represents the digital structure of diffusion, consisting of:
   1) N = network intensity
   2) A = actor multiplicity
   3) T = technological agency
c. R (Resonance Effect) represents the magnitude of impact, including viral propagation, escalation dynamics, and socio-systemic consequences.

4.3 Philosophical Interpretation

a. C (Causality) explains the legal basis of an act and its attribution.
b. NAT (Network–Actor–Technology) explains how the act is distributed and amplified within digital systems.
c. R (Resonance) explains the extent to which the consequences reverberate across the digital society.

Table 1. Indicators of Cyber Responsibility Resonance Theory (CRRT)

Dimension	Indicators	Philosophical Description	Legal Function
Causality	Factual, Legal, Proximate, Foreseeability	Establishes the basis of cause–effect attribution	Determines initial legal imputability
Network	Connectivity, Flow, Node	Structure of the digital social system	Defines distribution of roles
Actor	Human & Non-human Actants	Ontological equality of actors	Determines relational responsibility
Technology	Algorithmic Agency	Technology as an active agent	Assesses system-level contribution
Resonance	Amplification, Spread, Feedback	Chain-reaction and cascading effects	Determines escalation of harm

Source: Processed primary data (2026)

Table 2. *Conditions for CRRT Formula Validity*

Component	Minimum Requirement	Legal Implication
Complete causation	At least 3 of 4 elements met	Basis for initial legal attribution
Network involvement	≥ 2 active nodes	Excludes purely individual liability
Actor plurality	Human + technological actors	Establishes collective responsibility
Resonance effect	Evidence of dissemination	Confirms cyber offense manifestation
Predictability	Harm is reasonably foreseeable	Expands mens rea framework

Source: Processed primary data (2026)

Table 3. *Comparative Framework of Theories*

Aspect	Causation Theory (von Kries)	Network Society (Castells)	ANT (Latour)	CRRT (New Theory)
Focus	Linear causality	Network structure	Actor relations	Resonance-based responsibility
Actors	Human only	Humans in networks	Human + non-human	Human + technology + systems
Pattern	Linear	Relational	Symmetrical	Non-linear & dynamic
Responsibility	Individual	Socially distributed	Relational	Systemic resonance-based
Limitation	Not cyber-adaptive	Weak legal normativity	Not criminal-focused	Newly formulated framework

Source: Processed primary data (2026)

4.4 Case Simulation Based on CRRT

Person **A** uploads false information on social media claiming that a "bank will collapse tomorrow." The content goes viral, is amplified by platform algorithms, and spreads widely, resulting in:

a. Mass Withdrawal of Funds (Bank Run)
b. Public Panic
c. Disruption Of Local Financial Stability

4.5 CRRT Quantitative Simulation (Qualitative Scaling)

Scale:

a. Low = 1
b. Medium = 2
c. High = 3
d. Very High = 4

Table 4. *Causality Index (C)*

Component	Score	Justification
Factual causation	4	Direct trigger by A's post
Legal causation	4	Classified as harmful misinformation
Proximate cause	3	Platform acts as intermediary
Foreseeability	3	Viral risk is reasonably predictable
Σ	**C = 3,5**	

Source: Processed primary data (2026)

Table 5. *Network–Actor–Technology (NAT)*

Component	Score	Justification
Network	4	Multi-platform viral diffusion
Actor	4	A + users + bots involved
Technology	4	Algorithmic amplification
Σ	**C = 4**	

Source: Processed primary data (2026)

Table 6. *Network–Actor–Technology (NAT)*

Component	Score	Justification
Social impact	4	Mass panic
Economic impact	4	Bank run phenomenon
Chain effect	4	Systemic escalation
Σ	**C = 4**	

Source: Processed primary data (2026)

4.6 CRRT Calculation Result

$$R_{CRRT} = (3.5 \times 4) \times 4$$

Thus:

$$R_{CRRT} = 56$$

$$R_{CRRT} = 3.5 \times 4 \times 4 = 56$$

The CRRT simulation produces a score of **56**, which falls within the high or critical category. This indicates that criminal responsibility in this case cannot be attributed solely to actor A as the primary perpetrator. Instead, the digital system itself particularly the platform infrastructure and algorithmic mechanisms plays a significant role in amplifying and accelerating the harmful consequences. The case therefore reflects a form of *resonant cyber harm*, where the impact emerges through cascading interactions within a networked digital environment rather than a single linear cause.

In terms of responsibility distribution under the CRRT framework, actor A is positioned as the primary perpetrator with direct liability (*primary liability*), as the initial source of the harmful information. However, the digital platform functions as an algorithmic amplifier that contributes to systemic escalation, thereby carrying *systemic liability*. Meanwhile, other users who participate in the dissemination of the content assume a form of *secondary liability*, as their actions further extend the reach and intensity of the harm within the network.

4.7 Interpretation of Results

The simulation demonstrates that even a single act of digital misinformation can generate systemic resonance effects within a highly connected digital ecosystem. The high CRRT value (56) indicates:

a. Strong causal attribution (C)
b. Maximal network amplification (NAT)
c. Severe cascading impact (R)

Accordingly, criminal responsibility in cyberspace cannot be reduced to individual intent alone, but must be understood as a distributed and

resonant liability structure within socio-technical systems.

In conclusion, the simplified CRRT formulation demonstrates that criminal responsibility in cyberspace is no longer singular or isolated. Instead, it emerges as the result of continuous interactions among causality, digital networks, and resonance effects. This confirms that cybercrime liability must be understood as a distributed and systemically interconnected phenomenon rather than a purely individual act.

5. CONCLUSION

The findings of this study indicate that the Cyber Responsibility Resonance Theory (CRRT) successfully constructs a new paradigm in cybercriminal liability that moves beyond linear causality and individual responsibility. Instead, it emphasizes the complex interrelations among causality, digital networks, and resonance effects generated through the interaction of humans, technologies, and systems. The analysis demonstrates that in cases of viral misinformation, criminal liability cannot be attributed solely to the primary actor, but must also extend to the technological infrastructure particularly platform algorithms as well as other actors within the digital network who contribute to the amplification and escalation of harm. Accordingly, CRRT affirms that cybercriminal responsibility is inherently distributed and resonant, whereby the legal intensity of an act increases in proportion to the degree of network connectivity and the magnitude of its social impact. This model provides a novel analytical foundation in cybercriminal law for understanding digital offenses as systemic phenomena that transcend individual agency.

As a recommendation, this study suggests the need for further development of the Cyber Responsibility Resonance Theory (CRRT) to enable its operationalization within cybercrime law enforcement practice. This includes the formulation of more measurable juridical indicators to delineate the boundaries of responsibility among primary offenders, digital platforms, and other network actors. In addition, policymakers and law enforcement authorities are encouraged to adopt a distributed and impact-based liability approach in responding to the complexities of non-linear and systemic cybercrime, thereby ensuring that legal responses remain adaptive, proportionate, and aligned with the evolving dynamics of digital society.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to Universitas Duta Bangsa Surakarta, Central Java, Indonesia, for its continuous academic support and commitment in fostering a strong research culture, particularly through the implementation of the Memorandum of Understanding (MoU) in the field of collaborative research, including research funding support that has enabled the advancement of this study.

We also extend our profound appreciation to the Pengadilan Negeri Ungaran, Semarang, Central Java, Indonesia, for its valuable collaboration and institutional support in the implementation of the MoU in the field of research. This partnership, including collaborative research funding and access to practical legal insights, has significantly contributed to the enrichment and strengthening of the academic quality of this work.

Their cooperation reflects a meaningful synergy between academic institutions and the judiciary in promoting evidence-based legal research and strengthening the development of criminal law scholarship in Indonesia.

REFERENCES

[1] A. Kigerl, "Routine activity theory and the determinants of high cybercrime countries," *Soc. Sci. Comput. Rev.*, vol. 30, no. 4, pp. 470–486, 2012, doi: 10.1177/0894439311422689.

[2] B. Dupont and C. Whelan, "Enhancing relationships between criminology and cybersecurity," *Aust. N. Z. J. Criminol.*, vol. 54, no. 1, 2021, doi: 10.1177/00048658211003925.
[3] T. J. Holt, "Crime on the Internet," *Annu. Rev. Criminol.*, vol. 2, pp. 327–346, 2019, doi: 10.1146/annurev-criminol-011518-024836.
[4] M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005, doi: 10.1177/147737080556056.
[5] R. G. Smith, R. C.-C. Cheung, and L. Y.-C. Lau, Eds., *Cybercrime Risks and Responses: Eastern and Western Perspectives*. London: Palgrave Macmillan, 2015. doi: 10.1057/9781137474162.
[6] H. Djanggih and N. Qamar, "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta Res. Law J.*, vol. 13, no. 1, pp. 10–23, 2018, doi: 10.15294/pandecta.v13i1.14020.
[7] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecurity*, vol. 4, no. 1, 2018, doi: 10.1093/cybsec/tyy006.
[8] B. Dupont and T. J. Holt, "The human factor of cybercrime," *Soc. Sci. Comput. Rev.*, vol. 40, no. 4, 2022, doi: 10.1177/08944393211011584.
[9] R. Brownsword, *Law, Technology and Society: Re-imagining the Regulatory Environment*. London: Routledge, 2019. doi: 10.4324/9781351128186.
[10] A. S. Gulo, B. Nugroho, and B. Kurniawan, "Cybercrime dalam Bentuk Phishing Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *PAMPAS J. Crim. Law*, vol. 1, no. 2, 2020, doi: 10.22437/pampas.v1i2.9574.
[11] D. S. Wall, "Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime," *Information, Commun. Soc.*, vol. 11, no. 6, pp. 861–884, 2008, doi: 10.1080/13691180802007788.
[12] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007. [Online]. Available: https://books.google.com/books?id=dtN_AgAAQBAJ
[13] P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?," *Soc. Leg. Stud.*, vol. 10, no. 2, pp. 243–249, 2001, doi: 10.1177/a017405.
[14] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger/Bloomsbury Academic, 2010. [Online]. Available: https://books.google.com/books/about/Cybercrime.html?id=FRGfngEACAAJ
[15] K. Jaishankar, "Cyber Criminology: Evolving a novel discipline with a new journal," *Int. J. Cyber Criminol.*, vol. 1, no. 1, pp. 1–6, 2007, doi: 10.5281/zenodo.18276.
[16] M. S. Moore, *Causation and Responsibility: An Essay in Law, Morals, and Metaphysics*. Oxford: Oxford University Press, 2009. doi: 10.1093/acprof:oso/9780199256860.001.0001.
[17] M. Castells, *The Rise of the Network Society*. Oxford: Wiley-Blackwell, 2010. [Online]. Available: https://books.google.com/books/about/The_Rise_of_the_Network_Society.html?id=FihjywtjTdUC
[18] B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press, 2005. doi: 10.1093/oso/9780199256044.001.0001.

BIOGRAPHIES OF AUTHORS

	**Aryono** is a lecturer at Universitas Duta Bangsa Surakarta in the field of law, with academic and practical expertise in administrative and governmental law. He is actively engaged in the tri dharma of higher education through teaching, research, and community service, and has contributed to scholarly publications. In his role as an academic, Aryono plays a part in shaping students to be critical, analytical, and principled, while also supporting the development of legal education quality within the university. Can add email: Example: aryono@udb.ac.id
	**Yekti Mahardika** is a judicial officer serving as the Junior Registrar for Criminal Cases at the Ungaran District Court. In this capacity, she plays a strategic role in supporting both administrative and judicial technical aspects of criminal case management, including handling case files, scheduling hearings, and ensuring orderly court administration in accordance with applicable criminal procedural law. She is known as a meticulous, professional, and highly principled individual, committed to promoting a transparent, accountable, and just judicial system. Can add email: Example: pn.ungaran@gmail.com