Rethinking the Human–Technical Split in Cybersecurity

Jukka Vuorinen
University of Jyväskylä, Finland

jukka.a.vuorinen@jyu.fi

Abstract: This paper re-examines one of the most enduring assumptions in cybersecurity and information systems: the split between the human and the technical. For decades, research and professional practice have portrayed the human as an unpredictable source of error—"the weakest link"—in contrast to the supposedly rational and controllable domain of technology. While this separation appears practical, it stems from a deeper lineage of Western thought that positions humans and nonhumans as fundamentally separate spheres. Drawing on thinkers such as Michel Foucault and Bruno Latour, this paper traces how this conceptual division has become embedded in security discourse, from early information systems design to contemporary frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework. These standards institutionalize the split through parallel categories for "technical controls" and "human factors," shaping how security responsibilities are assigned and how failures are understood. The paper then explores what happens when this separation is challenged. Using examples such as intrusion detection systems and Trojan attacks, it shows that social and technical elements are inseparably mixed: anomalies, mimicry, and deception all rely on both code and conduct. Security decisions—from asset valuation to risk analysis—likewise emerge from socio-technical negotiations between what is desired and what is possible. To move beyond the limitations of this dichotomy, the paper introduces two frameworks that enact symmetry between human and technological agency. Conceptually, Actor–Network Theory treats both humans and artefacts as actors whose agency lies in their effects on others. Practically, Zero Trust security architectures operationalize the same symmetry by applying continuous verification equally to users and devices. Taken together, these perspectives suggest that cybersecurity should not be understood as two interacting domains but as a blended field of heterogeneous actors whose relations continually produce security. Recognizing this mixture does not dissolve the technical or the human but allows researchers and practitioners to see more clearly how each side folds into the other, reshaping what security can mean in practice.

Keywords: Cybersecurity, Human–Technical split, Sociomateriality, Actor–Network theory, Zero trust, Security frameworks

1. Introduction

Cybersecurity and Information Systems have long framed an apparent human–technical split. Typically, the story is that the human can shatter otherwise sturdy technical security (Baskerville, 1993; Loch, Carr & Warkentin, 1992). Later, the field became divided into the technical and the managerial, drawing in organizational and human aspects, with compliance emerging as a central concern (Siponen, Baskerville & Heikka, 2006; Bulgurcu, Cavusoglu & Benbasat, 2010). The division is often repeated in shorthand form: the human is the weakest link in security (Adams & Sasse, 1999; Nohlberg, 2009). This slogan performs a function: it re-establishes the split by suggesting that even if we had the strongest firewalls and most advanced technical solutions, these could be undone in an instant by a careless user.

This paper shows that the human–technical split in cybersecurity has, in fact, a strong historical context, yet the split can be counterproductive in practice, limiting and even disorienting. In terms of history, the split is not just a quirk of the field but part of a deeper lineage of Western thought. From Michel Foucault's (1970) account of the scientific order to Bruno Latour's (1993) views on modernity, there has long been a tendency in Western philosophy to separate human and nonhuman domains. The importance of paying attention to this split lies in the way it shapes our thinking, influencing what we perceive—and fail to perceive—about our environment and context. The same habit of thought informs cybersecurity: frameworks, standards, and professional practices reproduce the division, making it appear natural and necessary. Yet if we look more closely, the picture becomes more complicated in terms of how the technological and the human elements are set apart in the first place (Orlikowski, 2007). The sociomaterial turn is directly concerned with this very split (Orlikowski & Scott, 2008). If we examine the context of "the human is the weakest link," we can see that technical measures are saturated with social assumptions, while human practices are inseparable from the material infrastructures that enable them.

In this conceptual and theoretical essay, with illustrative examples, I examine three things. First, where the split comes from and how it has been inherited into the cybersecurity field, shaping how problems and responsibilities are framed in terms of technology and humans. Second, how the split is reproduced in practice—not only in popular sayings, but also in frameworks and standards that formally establish separate categories for technical and human factors (e.g. NIST, 2024; ISO/IEC 27001, 2022), even though at the level of actual practice the two are inseparably mixed. And third, how the boundaries can be approached differently.

On the operational side, Zero Trust architecture offers a case where humans and devices are treated in the same manner—each interaction checked continuously, no prior trust assumed or inherited. On the research side, Actor–Network Theory (ANT) (e.g. Latour, 2005) provides an analytic lens that refuses to recognize an ontological human–technical split, instead treating both as actors whose agency lies in their effects on others.

I do not argue that we should abolish categories like technical devices and human behavior, or deny that different types of controls (device configurations, architectures, or awareness training and compliance mechanisms) may be needed. Rather, I want to draw attention to how the split is constructed, why it has become so powerful, and how thinking differently might open new avenues for both researchers and practitioners. In other words, there is nothing inherently wrong with the split in many cases, but it can become a blinding factor if we imagine that technical solutions contain no human element or that human actors carry no technical dimensions. These are always blended. Zero Trust and ANT, taken together, provide ways to critically re-examine the division and to see cybersecurity not as two separate worlds, but as a blended field where humans and technologies constantly act on each other.

In this paper, the human–technical split refers not to any lack of integration between people and technologies in cybersecurity practice, but to an analytical distinction that treats human actors and technical artefacts as fundamentally different kinds of entities (see Orlikowski & Scott, 2008; Latour, 2005). This distinction is reproduced in cybersecurity discourse, standards, and frameworks that separate "human factors" from "technical controls" Accordingly, "social" denotes shared norms and institutionalized practices (not merely individual behavior or training), while the material/technical dimension denotes infrastructures, configurations, and algorithmic processes that enable and constrain action. Sociomateriality emphasizes that these dimensions are mutually constitutive in organizational practice.

2. Background – The Split Between Human and Technology

Saying that "the human is the weakest link" is frequently repeated in cybersecurity discourse (Adams & Sasse, 1999; Nohlberg, 2009). Whether this statement is accurate or not, it signals a widely shared view of a sharp split: on one side is the technical system while on the other is the human (user) side (e.g., Baskerville, 1993; Loch, Carr & Warkentin, 1992). These sides are seen as very different – isolated even: the former can be ruled by algorithms and is logical and predictable. Technology is programmable, but code is not impeccable. Mistakes do occur, but the code can be rewritten, corrected, and updated. Exact fixes are possible. Sometimes, however, updates in complex systems can go wrong—as in July 2024, when a CrowdStrike Falcon content update (Channel File 291) triggered a worldwide outage of Windows systems, requiring manual on-site remediation (CrowdStrike, 2024a; 2024b; CISA, 2024). Yet, systems are ultimately re-programmable and in that sense under control.

However, this split—the separation of human from others—is not unique to cybersecurity or information systems. It has a long history in how humans have understood the world and themselves, both in science and in everyday thought. Michel Foucault (1970), in The Order of Things, showed how scientific thinking developed around a special role for the human as the center of knowledge. Bruno Latour (1993), in contrast, argued that modernity itself rests on the repeated attempt to separate humans from nature, a distinction that is never fully achieved. These works reveal that separating the human from the nonhuman has been a recurring move in Western philosophy and science. Information Systems, despite often claiming to bridge the technical and the human, inherits this lineage. It connects the two, but at the same time keeps them apart. The hardware/software split is one version of the broader machine–user divide. This same manner of separation also shaped the culture of early computing (Levy, 1984; Hirschheim & Klein, 2012).

Stephen Levy's (1984) account of the hacker culture in California describes how source code was often open, free, and without passwords among enthusiastic hobbyists. There were no artificial boundaries, but in one line of thought (Stallman, 2002) everything was about developing systems together, openly, with no passwords or user accounts restricting access. While a distinction existed between developers and the system, they were nonetheless united as part of a shared collective project of development. However, boundaries existed right beside the hackers' ideology. Levy (1984) describes how large companies such as IBM or Xerox hid their code and this caused repulsive reactions among the hackers. Hidden source code created a split between computers and developers, i.e. hackers. For a long time, many wished for no user accounts at all—everything open, nothing hidden—so that users could develop the systems further (Stallman, 2002). This ethos implied no limits and no secrets, while in a related but distinct strand Raymond (1999) emphasized the open, collaborative development model as opposed to proprietary secrecy.

As computing moved into organizations and business systems, the emphasis shifted: proprietary control and secrecy became central. The shift also marked a broader historical transformation in the Information Systems field, as computing practices moved from hobbyist and technical communities into managerial and organizational domains (Hirschheim & Klein, 2012). While developers in the hacker culture were seen, and wanted to be seen, as "wizards," organizational life in business and management drew clear limits between IT systems. Models such as the Strategic Alignment Model (Henderson & Venkatraman, 1993) created separate pockets for different "actors": business goals, IT goals, organizational structures, and so on. In these framings, the user is positioned at a different level altogether, which implies the split.

The same split of social and technical is visible in cybersecurity frameworks and standards. These documents are powerful because they not only guide practice but also define what counts as security. And they repeat the division. Standards rise from best practices, and once formalized they reinforce them, producing a cycle. It is no surprise that the NIST Cybersecurity Framework (CSF) includes this split: some categories are clearly technical (system configuration, encryption, algorithmic safeguards), while others are explicitly human-focused (security awareness, training) (NIST, 2024). ISO/IEC 27001 provides a similar distinction. Access control is described in technical terms—logon procedures, password management—while separate clauses emphasize human responsibility, especially for privileged users (ISO/IEC, 2022). In both, the discourse of a technical–human divide is embedded in the very structure of the standard.

3. The mix – Illustrative Sociomaterial Practices

Intrusion detection systems (IDS) continuously monitor host or network activity to detect deviations from established patterns, using either signature-based methods or anomaly-based approaches (Satılmış, Akleylek & Tok, 2024). Here, the behavioral side becomes particularly compelling. For example, transferring an unusually large amount of data can be flagged as suspicious simply because it breaks from the established rhythm of activity. However, a sophisticated attacker can perform the same act of exfiltration gradually and imperceptibly—changing behavior—thus hiding within the flow of ordinary system operations**.** By mimicking ordinary traffic, the attacker hides exfiltration in slow, low-and-slow flows to avoid detection. As Liao et al. (2013) note, the central challenge of anomaly detection lies in modeling the "normal" so precisely that even subtle infiltration leaves detectable traces. This interplay evokes a form of mimicry, where an intrusion succeeds precisely because it appears ordinary. Today's AI technologies seek to spot anomalies through deep learning algorithms (Naseer et al., 2018).

Yet mimicry is also used in an entirely social manner in technological attacks. A Trojan attack, for instance, depends not only on code but also on trust—it enters the system disguised as something benign, something that a user desires or welcomes. As Bowles and Hernández-Castro (2015) recount in their historical overview of the "Trojan Horse" defense, malware often exploits human expectations of safety and routine to infiltrate systems unnoticed. Trojan attacks exploit trust by disguising malicious elements as benign artefacts. Such a deception took place and had consequences, as illustrated by the 2024 incident in which pagers used by Hezbollah were covertly weaponized through pre-installed explosive components—a Trojan horse, explosives hidden within an everyday communication device (BBC, 2024). The pagers, which were considered to be safer than mobile phones, were compromised. In cybersecurity, the user desires, conventions, and habits that are considered social are mixed deeply with technology (Vuorinen & Tetri, 2016). Thus, as there is desire to use something, there is also a possibility to exploit this desire by offering Trojan horses. However, the same logic extends to defense, where decoys are used to attract and misdirect attackers (e.g., Bowen et al., 2009).

An intrusion detection system defining "normal" behavior or a Trojan attack exploiting trust both show how deeply the social and technical are fused. The same applies to cybersecurity processes such as risk assessment, where protection depends on the perceived value of assets (ISO/IEC, 2022; Baskerville, 1993). Different assets receive different levels of defense, a logic that appears rational but is grounded in collective judgment: what is worth protecting and why. These values do not arise from technology itself but from socio-technical negotiation—how assets acquire meaning within business goals and how technical means enable or constrain that meaning. In this sense, value and security alike emerge from the interplay between social intention and technical possibility.

This means that security decisions are always contextual, situated within what is wanted (the social) and what can be done (the technical). The modalities of these activities—possibility, limitation, and potential—constantly mix the two. Technology is not mute here; it actively participates in shaping security decisions through its capabilities and constraints. A good example is the case of quantum technologies: they are not yet

a direct threat, but they have the potential to become one. Therefore, today's encryption must be designed with future quantum capabilities in mind. This requirement brings together multiple layers: the actual (what the situation currently is), the potential (what it might become), the technical (quantum computation), and the social (the desire to maintain confidentiality now and in the future). Recent research also highlights how advances in quantum and supercomputing are already reshaping cybersecurity strategy and preparedness (Yalcin et al., 2024).

There is no way to extract one aspect without bringing a piece of another with it. In this sense, security cannot be understood purely socially or purely technologically. I argue that this applies to every dimension of cybersecurity. The two are always mixed—each carrying traces of the other. Security itself is a social manifestation that always depends on material and technological dimensions.

4. Overcoming the Split? Implications for Research and Practice

This section outlines two paths—one in research and one in practice—for challenging the split. In research, the key question is how to treat the technical and the social symmetrically. As shown above, the field remains bifurcated: we have theories that focus on the technological side and others that focus on the human side, usually framing people either as problems to be managed or, through awareness and training, as "human sensors" who assist in security tasks (Vielberth et al., 2019). Very few approaches attempt to integrate both dimensions. The sociomaterial turn in Information Systems has been one major attempt to do so, emphasizing the mutual shaping of technology and human activity (Orlikowski, 2007; Orlikowski & Scott, 2008).

In terms of research, when it comes to overcoming the gap, sociomaterialism is certainly an option and, without doubt, provides a wide range of usable concepts that help to view technological and human agency symmetrically. However, the difficulty with this approach is that sociomaterialism does not offer a single, straightforward way to approach a subject, to inquire into knowledge, or to conduct analysis (Cecez-Kecmanovic et al., 2014), even though there are more structured methodological attempts (Gaskin et al., 2014). While it must be admitted that reality is complex and difficult to understand—and it is precisely here that the human–technology split has helped us simplify contextual complexity—it would be useful if there were a simpler approach, one that already has a strong research tradition.

Such an opportunity is provided by ANT, which was developed within science and technology studies in the late 1970s and early 1980s as a reaction to how narrowly agency had been understood—as something that belonged only to humans. Material objects were typically treated as passive tools or background props, while humans were seen as the sole decision-makers and sources of action. This is the same discussion that later emerged in the Information Systems field. Latour and Woolgar (1979) in Laboratory Life showed how scientific instruments are not neutral intermediaries but crucial participants in knowledge production. Michel Callon (1986) likewise demonstrated how technological artifacts can act, translate, and enroll others in networks of relations. This may not sound revolutionary, but it breaks a long Western philosophical lineage that placed the human at the center of agency. ANT, by contrast, treats human and material actors symmetrically. Despite its name, ANT is arguably more of a methodology than a theory, and this is precisely its strength.

The dynamic core of ANT is that actors are defined not by their intrinsic properties but by their effects on others—meaning that anything that has an effect on its surroundings is an actor (Callon & Latour, 1981). For example, a chair, which I am sitting on, enables writing; if removed, its effects become visible. The chair is not defined by its inner properties, but by the effects it produces—it makes sitting possible. Similarly, each new connection in a network changes the actor-network slightly, and thus the network evolves as relations emerge and disappear. When a new actor becomes part of a security assemblage, the configuration changes. If a new user joins a system, it may be a small adjustment overall—a mere scaling up—but still a change in the relations of trust, control, and vulnerability. Each new actor, human or nonhuman, has effects: one more potential attack vector, one more dependency, one more mediator. If the system instead connects to malicious code, the shift can be more dramatic. In either case, ANT invites us to see these changes symmetrically—as transformations in a network of relations rather than as events confined to a "human" or "technical" side. In this way, ANT provides a framework that closes, or at least narrows, the human-technology gap.

In security architectures, standards, and frameworks—as discussed above—the treatment typically follows the split. There are specialists for both sides: technology experts focusing on system configurations, and behavioral specialists focusing on human factors. However, not every development in the field adheres to this division at the level of principle. The Zero Trust security architecture, which has gained significant attention in recent years, offers a notable example. It aligns well with contemporary working models such as bring your own

device (BYOD) and the distributed nature of modern organizations. Unlike perimeter-based models, Zero Trust does not rely on a predefined boundary that separates trusted insiders from untrusted outsiders. Instead, it responds to the realities of networked, hybrid environments where such boundaries are fluid or nonexistent.

Zero Trust is distinctive because it closes the gap through its principle of continuous verification—summarized by NIST as the maxim never trust, always verify (Rose et al., 2020). In the Zero Trust framework, no entity—human or technical—is trusted by default. Every actor, whether a user, device, or service, must continually prove its legitimacy through authentication and authorization processes. If a user begins to perform actions that deviate from established patterns, the system flags this as potentially suspicious. Likewise, if a device suddenly changes its location or access behavior, it is subjected to additional checks. In Zero Trust, trust is not a permanent status but a temporary and revocable condition, granted only for as long as the verification holds.

Through this logic of continuous distrust, Zero Trust effectively treats human and technical entities in a symmetrical way. Both are considered active participants within the security assemblage, capable of legitimate or illegitimate actions. The system's role is not to judge intent but to verify behavior. By subjecting users and devices alike to the same rule of conditional trust, Zero Trust embodies a practical realization of the symmetry that ANT describes at a conceptual level. It demonstrates how, in practice, the boundary between social and technical can be narrowed through concrete design principles rather than rhetorical redefinition.

5. Discussion and Conclusions

The split between the social and the technical is an old one. It extends far beyond the fields of Information Systems and cybersecurity and is, in fact, an overarching feature of Western thought rather than a local peculiarity. Yet, although the split may feel intuitively functional—"humans are different from machines, right?"—it can also create a haze, an illusion of two distinct worlds. This illusion divides specialists into two camps: those who "know the technical side" and those who "understand human behavior." However, if we look more closely at how systems operate and how they are established, these two sides are constantly intertwined. There is no purely technological, nor purely social. What we have instead is a continuous mixture—something we can begin to approach differently through frameworks such as Zero Trust and ANT. Importantly, this argument does not deny that contemporary cybersecurity practice routinely combines technical controls with training, policies, and procedures; rather, it questions the conceptual framing that continues to treat these elements as ontologically distinct domains.

The practical takeaway of this paper could be summarized as follows: whenever a practitioner thinks that something belongs to the "human side" or the "technical side," that moment should trigger a pause. It is an opportunity to ask whether there is something social embedded within the technical—and vice versa. What social and technological ramifications arise across the entire security assemblage when one element is altered? How do people think about the devices and technologies they engage with, and how do these beliefs influence their actual behavior? The social is not confined to people, and the technical is not merely a platform on which we act; it also shapes how we think, perceive, and decide. Could a situation be framed differently? Could technologies be used in another way? What principles or values does the system ultimately serve? These are the questions that help us to move beyond the split. They are not silver bullets—nothing in this field is—but they can help practitioners to see the broader picture and to recognize how both sides continually fold into each other.

On the research side, the field does not necessarily need to be reorganized from scratch, but it should be re-imagined as operating on a single, shared level. ANT may assist in this task. It is not a magical new lens that reveals everything at once, but rather a subtle shift: a way of understanding that, in research as in practice, we might not need to analytically separate the technical and the social in organizational contexts, where they constantly co-produce one another.

While contemporary cybersecurity research and practice increasingly emphasize holistic approaches that combine technical, human, and organizational considerations, these efforts often remain framed through analytically distinct categories. Humans and technologies are coordinated, yet still treated as different kinds of entities with separate explanatory roles. This paper does not deny such integrative efforts, but questions the persistence of this underlying separation and proposes an alternative way of thinking about agency, responsibility, and trust in cybersecurity. By approaching security as a field of heterogeneous but symmetrical actors, it becomes possible to reflect differently on how controls, behaviors, and infrastructures jointly produce security outcomes. From this perspective, Zero Trust can be understood not merely as a technical

architecture, but as a practical instantiation of a broader conceptual shift with implications for both research and practice.

AI Declaration: Portions of this paper were refined with the assistance of OpenAI's ChatGPT. The tool was used to support language refinement, grammatical editing, and reference formatting. All ideas, interpretations, argumentation, and substantive content are the author's own.

Ethics declaration: No specific ethical clearance was needed for this theoretical research.

References

Adams, A. and Sasse, M.A. (1999) "Users Are Not the Enemy", *Communications of the ACM*, Vol. 42, No. 12, pp. 40–46.

Baskerville, R. (1993) "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys (CSUR)*, Vol. 25, No. 4, pp. 375–414.

BBC News (2024) *Israel Says Hezbollah Pager Blasts Were Pre-Planned Trojan Attack*, 17 September. [online] Available at: https://www.bbc.com/news/articles/cwy3l02wxqdo (Accessed: 2 October 2025).

Bowen, B.M., Hershkop, S., Keromytis, A.D. and Stolfo, S.J. (2009) "Baiting Inside Attackers Using Decoy Documents", in *International Conference on Security and Privacy in Communication Systems*, Berlin and Heidelberg, Springer, pp. 51–70.

Bowles, S. and Hernandez-Castro, J. (2015) "The First 10 Years of the Trojan Horse Defence", *Computer Fraud & Security*, Vol. 2015, No. 1, pp. 5–13.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly*, Vol. 34, No. 3, pp. 523–548.

Callon, M. (1986) "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay", in J. Law (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London, Routledge, pp. 196–233.

Callon, M. and Latour, B. (1981) "Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So", in K. Knorr-Cetina and A.V. Cicourel (eds.) *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*. Boston, MA, Routledge & Kegan Paul, pp. 277–303.

Cecez-Kecmanovic, D., Galliers, R.D., Henfridsson, O., Newell, S. and Vidgen, R. (2014) "The Sociomateriality of Information Systems", *MIS Quarterly*, Vol. 38, No. 3, pp. 809–830.

Cybersecurity and Infrastructure Security Agency (CISA) (2024) *Widespread IT Outage Due to CrowdStrike Update*. [online] Available at: https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update (Accessed: 2 October 2025).

CrowdStrike (2024a) *Falcon Sensor Update Incident — Technical Summary*, CrowdStrike Blog, 19 July. [online] Available at: https://www.crowdstrike.com/ (Accessed: 2 October 2025).

CrowdStrike (2024b) *Guidance for Customers Remediating Channel File 291*, CrowdStrike Support Advisory, 20 July. [online] Available at: https://www.crowdstrike.com/ (Accessed: 2 October 2025).

Foucault, M. (1970) *The Order of Things: An Archaeology of the Human Sciences*. London, Tavistock.

Gaskin, J., Berente, N., Lyytinen, K. and Yoo, Y. (2014) "Toward Generalizable Sociomaterial Inquiry", *MIS Quarterly*, Vol. 38, No. 3, pp. 849–872.

Henderson, J.C. and Venkatraman, N. (1993) "Strategic Alignment: Leveraging Information Technology for Transforming Organizations", *IBM Systems Journal*, Vol. 32, No. 1, pp. 4–16.

Hirschheim, R. and Klein, H.K. (2012) "A Glorious and Not-So-Short History of the Information Systems Field", *Journal of the Association for Information Systems*, Vol. 13, No. 4, pp. 188–235.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2022) *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva, ISO.

Latour, B. (1993) *We Have Never Been Modern*. Cambridge, MA, Harvard University Press.

Latour, B. (2005) *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford, Oxford University Press.

Latour, B. and Woolgar, S. (1979) *Laboratory Life: The Construction of Scientific Facts*. Beverly Hills, CA, Sage.

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. New York, Anchor.

Liao, H.-J., Lin, C.-H.R., Lin, Y.-C. and Tung, K.-Y. (2013) "Intrusion Detection System: A Comprehensive Review", *Journal of Network and Computer Applications*, Vol. 36, No. 1, pp. 16–24.

Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992) "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly*, Vol. 16, No. 2, pp. 173–186.

Naseer, S., Saleem, Y., Khalid, S., Bashir, M.K., Han, J., Iqbal, M.M. and Han, K. (2018) "Enhanced Network Anomaly Detection Based on Deep Neural Networks", *IEEE Access*, Vol. 6, pp. 48231–48246.

Nohlberg, M. (2009) "Why Humans Are the Weakest Link", in M. Gupta and R. Sharman (eds.) *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey, PA, Information Science Reference, pp. 15–26.

Orlikowski, W.J. (2007) "Sociomaterial Practices: Exploring Technology at Work", *Organization Studies*, Vol. 28, No. 9, pp. 1435–1448.

Orlikowski, W.J. and Scott, S.V. (2008) “Sociomateriality: Challenging the Separation of Technology, Work and Organization”, *Academy of Management Annals*, Vol. 2, No. 1, pp. 433–474.

Raymond, E.S. (1999) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, CA, O’Reilly.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) *Zero Trust Architecture (NIST Special Publication 800-207)*. Gaithersburg, MD, National Institute of Standards and Technology. [online] Available at: https://doi.org/10.6028/NIST.SP.800-207(Accessed: 2 October 2025).

Satılmış, H., Akleylek, S. and Tok, Z.Y. (2024) “A Systematic Literature Review on Host-Based Intrusion Detection Systems”, *IEEE Access*, Vol. 12, pp. 27237–27266.

Siponen, M., Baskerville, R. and Heikka, J. (2006) “A Design Theory for Secure Information Systems Design Methods”, *Journal of the Association for Information Systems*, Vol. 7, No. 11, pp. 725–770.

Stallman, R.M. (2002) “On Hacking”, in P. Himanen (ed.) *The Hacker Ethic and the Spirit of the Information Age*. New York, Random House, pp. 3–9.

Vielberth, M., Böhm, F., Fritsch, L. and Pernul, G. (2019) “Security Operations Center: A Systematic Study and Open Challenges”, *Computers & Security*, Vol. 87, p. 101579. https://doi.org/10.1016/j.cose.2019.101579

Vuorinen, J., & Tetri, P. (2016). “Paradoxes in information security”, *IEEE Potentials,* 35(5), 36-39.