Disinformation and Trust in Digital Environments: Expert Decision-making, Dismiss or Discuss?

Allison Wylde[1], Fabio James Petani[2] and Helmi Issa[3]
[1]University of Kent, School of Computing, Institute of Cyber Security for Society, Canterbury, UK
[2]Université Bourgogne Europe, Burgundy School of Business [1] Dijon, France
[3]ESSCA School of Management, Boulogne-Billancourt CEDEX, Paris, France, Casoria, Fortuna [1]
a.wylde-102@kent.ac.uk
fabio-james.petani@bsb-education.com
Helmi.ISSA@essca.fr
Fortuna.casoria@bsb-education.com

Abstract: Leveraging a management and organizations sciences perspective, this paper conceptualises AI, security and information warfare practitioner decision-making as a decision to trust or distrust, mediated by intuition. To explore how practitioners navigate trust in digital environments and benchmark to concerns a survey was conducted among 95 expert cyber security AI and information warfare practitioners. Questions explored practitioners' thoughts on sources of trusted material, intuition, and approaches to managing disinformation. Scenarios were included to explore practitioners' thoughts on unusual incidents and help elicit future threats and solutions. Findings highlight variations in decision-making approaches according to age, experience and domain. For trust in intuition, early-stage career and military/ defence individuals were found less likely to rely on intuition than public and private sector peers. When faced with out-of-the-ordinary events practitioners were spilt among four responses, re-checking data (37%), dismissing out-of-the-ordinary events (30%), pausing decision-making (19%), or seeking discussing (13%). Experience levels matter, with mid-career practitioners behaving distinctly from those at early- and late-stage careers. The contribution of this paper have direct implications for policy-makers, including recommendations for personalised stage-appropriate training in decision-making across age groups, and domains. Given the increasing velocity and uncertainty of the current and future threat landscape more precise calibration of practitioner decision-making is urgently needed.

Keywords: Disinformation, Information warfare, Trust, Intuition, Decision-making, Experts, Artificial intelligence, AI, Cyber security

1. Introduction

The 2026 World Economic Forum ranked disinformation (including AI augmented disinformation) as the second most important short-term threat, illustrating the increasing importance of decision-making by security practitioners responsible for managing this threat (WEF, 2026). Yet, although published standards and guidance provide steps in risk management and information security and zero trust architectures (Rose, 2020; NCSC, 2021), detailed knowledge on the processes and drivers for decisions taken by expert security practitioners remains under-explored. In contrast to spotting a gap in the literature, this paper leverages management and organizational studies scholarship and an interpretive approach aims to increase our depth of understanding (Alvesson & Sköldberg. 2009).

Our research questions explore topics of trust in digital environments augmented by AI to examine and benchmark concerns. The findings here concentrate on intuition and decision-making in an out-of-the-ordinary event (scenario). Further material from the larger survey on disinformation and trust has been published separately (Wylde et al., 2026) and the remaining study is in press

Given the complexity of concepts like decision-making, intuition and trust and the realities of experts, for example, fire fighters and paramedics making split-second decisions based on experience and intuition (Klein, 2017) a pragmatic approach was adopted to allow key terms such as decision-making and intuition to be simplified to issues of trust and distrust (Alvesson & Sköldberg, 2018: Weick, 1989).

This paper proceeds by reviewing key literature from management and organization sciences on trust in decision-making and intuition (self-trust). This is followed by a discussion on the methodology setting out the rationale for the selected research approach – which has to be capable of addressing the subjective contexts of trust and practitioner decision-making. To achieve this goal a scenario was included to allow practitioners to explore the current state of a system, potential future disruptions and solutions (Rasmus et al., 2025) Next,

drawing on the findings, important questions of trust are unravelled in contexts of uncertainty. The discussion and conclusion present the contribution and implications for practitioners, policy makers and academics.

1.1 Trust and Decision Making

As a research topic, interest in trust continues to grow, well-established scholarship sets out the processes for trust building (notably, Mayer et al., 1995), with trust defined as based on confident positive expectations of another's behaviour (Lewicki et al., 1998) and a willingness to be vulnerable irrespective of control or monitoring (Mayer et al., 1995). The multiple scales of trust relations have been acknowledged as ranging from inter-personal to inter-organization, institutional (Fulmer, & Gelfand 2012; Zaheer et al., 1998) and beyond, to trust in relations that are non-human (McKnight et al., 2011), and, for example, trust in AI systems.

In this paper decision-making is conceptualised a viewpoint based on whether to trust or distrust a particular individual, organization or factor. One strand of current discussions centres on the framing of the central constructs in trust and distrust with Verhoest et al. (2024) questioning whether these concepts are the opposite ends of the same continuum, arguing that they should be judged by different dimensions, ability, benevolence and integrity, compared to suspiciousness and watchfulness for negative consequences, how this ties with intuition is considered next.

1.2 Intuition and Trust

Significant evidence demonstrates that experts rely on intuition (Medvegy, 2022). In cases of crises where decisions must be made under time and risk constraints, for example, the split-second decisions by fire chiefs in a crisis were founded on intuition, drawing on past-experience and heuristics (Roghanizad et al., 2015).

In considering intuition as it intersects with trust, scholars suggest that although there are times when intuition (gut feeling) must be trusted, it is also important to consider the role of experience (Kahneman & Klein 2010: Klein, 2017). For example, as surgeons deal with some cases regularly, expert intuition is highly relevant. Yet, when unusual problems arise, there may be risks of over confidence. Indeed some experts may go along with their gut while other may draw on hindsights allowing them to trust their intuition (Kahneman & Klein 2010: Klein, 2017). At the same time, some scholars suggest that disinformation and AI augmented disinformation is successful because it contains a grain of truth, suggesting that society should reduce trust (Marco-Franco et al., 2021). Zero trust is discussed next.

1.3 Zero Trust

Zero trust emerged as a cyber security solution in response to the blurring of organizational boundaries and supply chains, and the need to evolve from simple perimeter-based security (Kindervag, 2010). In zero trust thinking, all network architectures are assumed to be breached and therefore hostile and all access requests must be verified (Rose et al., 2020; NCSC, 2021). The four main propositions of zero trust can be specified as features of: trustor disposition; the trustor-trustee relationship; the domain; and the institutional context (Wylde, 2021). In zero trust, the disposition of the trustor to a trustee is viewed as based on non-presumptive trust (zero trust), in other words, verify then trust (Lewicki et al., 1998). The nature of the trustor-trustee relationship consists of the trustor as an assessor (or controller) and a trustee as a user or subject, whether as an individual or a device, or a software application (Rose et al., 2020; NCSC, 2021). The domain-specific concerns involve the network architectures which are assumed to be breached, with the institutional context as one of mandated cybersecurity based on zero trust. On assessment, if an identity is confirmed, trust is earned (Rose et al., 2020; NCSC, 2021). Finally, continuous monitoring of the identity occurs; should any changes or indeed violations occur, trust will be withdrawn. Unlike the assessment of trust (Mayer et al., 1995), the features of zero trust operate in isolation and in parallel (Rose et al., 2020; NCSC, 2021).

1.4 Disinformation

The definition of disinformation draws from the US Cybersecurity and Infrastructure Agency (CISA, Nd) and the European Commission. (2018). Disinformation is defined by the US, CSIA as information "deliberately created to mislead, harm, or manipulate a person, social group or country" (CISA, nd.). The EU, definition considers disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or intentionally to deceive the public and may cause public harm" (European Commission, 2018). Both definitions stress disinformation creates harm through deception and manipulation. The US, scope includes people, social group and country-level (CISA, nd.) while the EU focus is on economic beneficiaries and country-level economics (European Commission, 2018). Disinformation differs from misinformation simply in terms of harm. Marco-Franco et al. (2021) recommend that to address trust in disinformation, as a society we

need to reduce our trust in the internet. Murphy (2023) sums up, arguing that disinformation involves the simultaneous presence of malign actors (with masked identities), the release intentionally harmful or destructive information, with a predetermined political, military, economic or social objective. It is with these conversations in trust, zero trust, intuition and disinformation that this paper seeks to better characterise decision-making under conditions of uncertainty and AI to generate insight and foresight (Hauptman & Steinmüller, 2019).

2. Methodology

The study was conducted among experienced cyber security practitioners focused on decision-making for cyber security and disinformation management based on questionaaries and a scenario to elicit views on current practice and future foresight (Hauptman & Steinmüller, 2019). University ethics were obtained; participants were advised the survey was anonymous, that they could with withdraw their consent at any time before the end of the survey, and, that the findings would be made available.

2.1 The Study

The survey questions were derived from published papers published on the topics of interest, trust, intuition, zero trust and disinformation (Medvegy, 2022; Kahneman, 2013; Rose, 2020; NCSC, 2021): the first questions explored the nature of decision-making.

A purposive sampling approach was used as the study required contact with appropriately experienced, domain experts (Alvesson & Sköldberg, 2018: Alvesson, 2002). The survey was web based survey hosted by Qualtrics XM, released from September 2025 to November 2025.

Participants were contacted and invited to participate directly by the authors via email and LinkedIn. Participants included recognised domain experts, personal contacts and European Conference on Cyber Warfare and Security attendees.

A total of 112 responses were collected, 4 did not consent, 1 was a test and 9 were incomplete; a final response of 95; comprising, male 67.3%, female 21.4% non-binary, prefer not to say and missing 11.3%; the age range was 18-65+; experience ranged from less that 1 year-to more than 15years.

Table 1: Survey questions, main topics

No.	Topics
1	Demographics, age, gender, self-identification, years of experience and domain expertise (sector)
2	Trust
3	Intuition
4	Scenario on an unexpected event
Note.	This paper reports on sections 3, and one scenario the remaining material will be published separately.

2.2 Research and Analysis Approach

This research focused by security practitioners as they managed complex processes of decision-making for cyber security, AI, disinformation and other aspects of digital security. Unlike lab-based experiments that can be studied using hypotheses and statistics, this study demanded a research approach capable of dealing with the messy realities of life, for example, involving people, organizations and learning (Miller& Tsang, 2011). To study the dynamics of decision-making, a simplified framework based on trust was drawn on as a lens through which to study the dynamics and factors involved (Klein, 2017, Weick, 1989). The analysis followed an interpretative approach to allow seeing beyond different levels of meaning and contrasting what the material may mean (Alvesson & Sköldberg, 2018).

An important part of the survey included scenarios. The scenario presented here explored here included an unknown out-of-the-ordinary event designed to help practitioners to explore the current state of the system, potential future disruptions and solutions (Rasmus et al., 2025), In addition the scenario helped provide respondents an opportunity to exercise their imagination and foresight (cf. Hauptman & Steinmüller, 2019: Hiltunen et al., 2025) - outside of any bias implied by zero trust architecture or systems (Rose et al., 2020; NCSC, 2021).

2.3 Findings

Results are from the study of intuition and the scenario are presented below. The analysis sought to integrate the findings through including the participant demographics (age, gender, years of experience and domain), the findings from the questions on intuition and the scenario. The findings were triangulated to increase the depth of understanding (Adams & Sasse, 1999).

2.4 Intuition

The question on intuition asked, "I rely on professional intuition when time is limited". For simplicity results from the Likert scale were aggregated: not at all and very little; slightly/ moderately; quite a bit/ very much/ a great deal.

Table 2: Relationship of relying on intuition under time pressure - to profession

	Intuition; relying on intuition under time pressure		
Profession	**Not at all/ very little**	**Slightly/ moderately**	**Quite a bit/ very much/ a great deal**
Academic/Researcher	32%	41%	27%
Cybersecurity Prof	27%	27%	46%
Military/Defense	50%	25%	25%
Private Sector	17%	33%	50%
Public Sector	0%	50%	50%

The results show that (46%-50%) of cyber security and the private sector professionals place the highest value on relying on intuition under time pressure, while 50% of the military and defense professionals said their reliance on intuition was "not at all or very little".

The reliance on intuition by experience; "very little or not at all" was found to be was the greatest in the less experienced professionals, less that 1yr (0%), 1-3yrs (50%); highly experienced (33%), compared with the mid-level practitioners, 4-7yrs and 8-15yrs who had lower levels (14%) and (26%) respectively.

However, the highest level of reliance of intuition under time pressure was (50%) for less that 1yr of experience (25%); while for 1-3yrs, mid-level practitioners, 4-7yrs and 8-15yrs (43% and 37% respectively); for the highly experienced, 8-15yrs and 15+yrs, the level was (37% and 29% respectively). The results seem to show the highest variance among the least experienced practitioners (less than 1yr, 1-3yrs), with 0% for no reliance, to 50% with a high reliance.

For "using intuition by profession", the public sector scored highest for using intuition (50% relied strongly and 50% relied moderately) along with the private sector and cyber security professionals (50% and 46% agreed strongly, respectively). The results differed for the military, 50% said they did not rely on intuition at all, compared with 25% who relied moderately and 25% relied strongly.

2.5 Scenario

Scenario 3 asked participants to imagine;

> *You have an unusual dream about a major crisis – something like a widespread power outage that disrupts communication and operational systems. The next day, the data at work seem to support what you dreamt. Surprisingly, your colleagues say they had a similar dream and agree with your risk assessment. This strange coincidence makes you question whether people around you – including yourself – are interpreting the situation clearly. You begin to wonder if your team's judgement is being influenced by something other than reliable information, and whether your usual ways of processing information, both digital and analogue, can still be trusted. What is your first reaction to this situation? Please select one of the following choices: re-check the data carefully; pause decision-making until you feel more certain; discuss the situation with someone outside the team; or, dismiss the coincidence as irrelevant.*

The findings from the scenario choices are clustered around cohorts, the largest cohort comprised those who rechecked data 37% followed by 30% who dismissed the scenario.

The next largest cohort, 19% paused further actions until they were clearer, and the final and smallest cohort were those who discussed 13%. One individual indicated they would speak with a leader. The largest % of selections were found in the recheck cohort; 1-3yrs (64%) and 15+ yrs professionals (48%) as compared the mid-career professionals (18% and 16%). The dismiss group; was highest among the mid-career group (8-15 yrs, 47% and 4-7 yrs, 36%) as compared with the lower %'s for the younger (18%) and senior (19%) groups.

A number of respondents selected more than one choice, for a first choice to recheck the data, 45% follow by discussing outside the team; notably, 41% of this cohort had no second response.

Table 3: Response to the scenario event, by years of experience

Years (yrs) of experience	Re-check the data carefully	Pause decision-making until you feel more certain	Discuss the situation with someone outside the team	Dismiss the coincidence as irrelevant
Less than 1; (1) 1-3 yrs; (10)	(7) 64%	0%	(2) 18%	(2) 18%
4-7yrs; (10#)	(2) 18%	(2) 18%	(2) 18%	(4) 36%
8-15 yrs; (19)	(3) 16%	(5) 26%	(2) 11%	(9) 47%
15+ yrs (27)	(13) 48%	(6) 22%	(3) 11%	(5) 19%
Sub-totals	(25) 48%	(13) 19%	(9) 13%	(20) 30%
#Note, 1 respondent indicated they would seek advice from a leader, not included above				

Of those who posted the second choice, to discuss, a third choice to pause further actions was selected (13%).For gender it was found that the majority of males were likely to re-check data (49%) while for females the response was to discuss (36%), only 2 responses were returned for non-binary/ prefer not to say, re-check data and dismiss.

3. Discussion

In examining the intuition findings, more junior professionals are at a learning stage, with limited self-awareness, hence more likely not to trust any intuition, rather preferring to present qualified decisions as compared with to a gut instinct. Mid-years experienced professionals are more likely to possess self trust, validated by their experience (seen it before) tied in with their domain specific knowledge and training (Medvegy, 2022). However, in highly trained personnel, for example, in the military, trusting intuition may seem like cutting corners, taking decisions that are not defensible (Medvegy, 2022), in a similar vein, senior professionals approaching retirement may take a safe bet. In addition, experienced military and security practitioners may operate under conditions of zero trust or AI driven cyber security processes, reducing intuition.

In terms of gender, the %'s presented here reflect the acknowledged over representation of males as found in the industry (ISC2, 2024). Examining differences in gender-related behaviour, an explanation could be provided by issues of socialisation, with males preferring to act alone, while females, represented by smaller numbers (ISC2, 2024), may act more collaboratively, and hence enter into discussions.

Taking a decision to dismiss an unexpected event seems to contrast with those practitioners who rechecked their data or those who discussed or paused actions. Looking at these actions in the context of trust decisions and responses by age, the highest levels of response were by juniors (64%) followed by the senior practitioners (48%), both in favouring re-checking data. As a response related to self-trust, this could indicate juniors exercising caution associated with a lack of self-trust, as compared with seniors favouring further investigation. However, in a crisis situation, both these results are could be seen as reflecting a lack of self-trust, causing a delay in response. The second highest raking response was among the mid-year experienced cohort (4-7yrs and 8-15yrs) both favour dismissing the incident (36% and 47% respectively). This result could be taken to indicate that this cohort are motivate to take decisions, but the numbers of practitioners taking this decision increased with age. This could indicate that the 8-15yrs cohort, who although they have a good deal of

experience, close to half were dismissive. This response, although quick, could indicate a bias related to training in zero trust or over confidence.

The scenario and intuition findings will be incorporated into future studies and help explore observations and responses to systems on work focused on disinformation (Wylde et al., 2026), and the assessment of current and potential future states as well as potential disruptions and solutions (Rasmus et al., 2025). As with all research, limitations are inevitable; notably issues with self-reporting, thinking about an abstract scenario, gender imbalance and the lack of statistical analysis. To overcome the problems with self-reported data, it is recommended that future studies be conducted with practitioners in the workplace during critical incident and/ or crisis management and using AI, this would allow real-time observations of behaviour and decision-making. In thinking through abstract scenarios, future work could observe practitioners during table-top simulations, AI scenarios and science fiction scenarios. For gender, future studies could seek to include more females to redress the balance.

The contribution of the study highlights different responses according to age and experience; leading to three recommendations for policy makers. Firstly, recognition that most security practitioners do not behave the same due to issues including, sector norms and prior levels of experience. Secondly, training should be directed at early stage and later stage career individuals to help build experience and overcome blind spots, respectively. Thirdly, for military and defence personnel, participation should be encouraged in joint operations with the private and public sectors, to allow experience of different aspects of decision-making under different conditions and hierarchies- including AI.

4. Conclusion

Recent fines of big Tech companies illustrate the importance that practitioners demonstrate transparent, compliant and auditable decision-making. This paper argued that although in practice, recognised standards and guidelines are implemented by security professionals, the decision-making steps involved remain under researched. The findings reported here highlight that there are distinct differences in practitioner's decision-making, related to experience and domain, highlighting key questions for future research.

The contribution raises important implications for policy makers, practitioners and scholars. To account for differences in decision-making among security practitioners, it is recommended that training be developed to addresses differing career and experience stages and domain knowledge. For example, in light of differences found across practitioners from the public and private sectors and the military, is is suggested that operations be conducted jointly among these sectors together with AI. This could allow practitioners to experience working in different contexts with different decision hierarchies and among differing levels of experience and training.

Acknowledgements

Thank you to the research participants for taking time from their busy schedules to take part in this study and for the reviewer's comments which have improved the final paper.

Ethics and AI: Ethical approval was obtained, Claude AI was used to help format the first version of the paper.

References

Adams, A. & Sasse, M. A. (1999). "Users are not the enemy." *Communications of the ACM*, 42 no.12: 40-46.

Alvesson, M. & Sköldberg. K. (2018). *Reflexive Methodology: New Vistas for Qualitative Research*. 3rd ed. London: Sage Publications.

Alvesson, M. (2002). *Understanding Organizational Culture*. London: Sage Publications.

CISA. (Nd). Foreign Influence Operations and Disinformation. *https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.*

European Commission. (2018). Action plan against Disinformation. Brussels, 5.12.2018, JOIN(2018) 36 final, https://op.europa.eu/publication-detail/-/publication/e18263d2-f962-11e8-8885-01aa75ed71a1.

Fulmer, A. C. & Gelfand. M. J. (2012). "At what level (and in whom) we trust: Trust across multiple organizational levels". *Journal of Management*, 38, no. 4: 1167-1230.

Hauptman, A., & Steinmüller, K. (2019). S*urprising scenarios. Imagination as a dimension of foresight. In Envisioning uncertain futures: Scenarios as a tool in security, privacy and mobility research,* (pp. 49-68). Wiesbaden: Springer Fachmedien Wiesbaden.

Hiltunen, E., Aalto, M., Hyytiäinen, M. & Huhtinen. A-M. (2025). *Envisioning New Ways to Use Economic Sanctions and Weaponisation in the Future*. In Proceedings of the 24th European Conference on Cyber Warfare and Security. Academic Publishing (2025).

ISC2 (2024). *Women in Cybersecurity Report Inclusion Advancement Pay Equity* https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity.

Kahneman, D., & Klein, G. (2010). "When can you trust your gut?" McKinsey Quarterly, 2, 58–67.

Kindervag, J. (2010). *No more chewy centers: Introducing the zero trust model of information security*. Forrester Research, September 14, 2010, updated September 17, 2010, https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf.

Klein, G.A. (2017). *Sources of power: How people make decisions*. MIT press.

Lewicki, R. J., Daniel J. McAllister, D. J & Bies, R. J. (1998). "Trust and distrust: New relationships and realities". *Academy of Management Review*, 23, no. 3: 438-458.

Marco-Franco, J. E., Pita-Barros, P., Vivas-Orts, D., González-de-Julián, S. & Vivas-Consuelo, D. (2021). "COVID-19, fake news, and vaccines: should regulation be implemented?". *International journal of environmental research and public health*, 18 no. 2: 744.

Mayer, R. J., Davis H & Schoorman, D. F. (1995). "An integrative model of organizational trust. *Academy of Management Review".* 20, no. 3: 709-734.

McKnight, David. Harrison, Michelle Carter, Jason Bennett Thatcher and Paul F. Clay. (2011). "Trust in a specific technology: An investigation of its components and measures". *ACM Transactions on management information systems (TMIS) 2*, no. 2: 1-25.

Medvegy, Z., Raab, M., Toth, K., Csurilla, G. and Sterbenz, T. (2022). "When do expert decision makers trust their intuition?". *Applied Cognitive Psychology*, 36(4), pp.748-757.

Miller, K.D. and Tsang, E.W. (2011). "Testing management theories: Critical realist philosophy and research methods". *Strategic Management Journal*, 32 no. 2: 139-158.

NCSC. (2021). *Zero Trust Architecture*. July 23, 2021. https://www.ncsc.gov.uk/collection/zero-trust-architecture.

Roghanizad, M.M. and Neufeld, D.J. (2015). "Intuition, risk, and the formation of online trust". Computers in Human Behavior, 50: 489-498.

Rose, S, Borchert, O. Mitchell S. & Connelly, S. (2020). *Zero trust architecture*. NIST special publication, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Verhoest, K., Latusek, D., Six, F., Maman, L., Papadopoulos, Y., Schomaker, R.M. & Trondal, J. (2024). "Trust and distrust in public governance settings: Conceptualising and testing the link in regulatory relations". *Journal of Trust Research*, 14 no. 2: 127-156.

WEF. (2026). *Global risks report 2026: Geopolitical and economic risks rise in a new age of competition*. WEF, Jan. 14, 2026 https://www.weforum.org/press/2026/01/global-risks-report-2026-geopolitical-and-economic-risks-rise-in-new-age-of-competition/

Weick, K.E. (1989). "Theory construction as disciplined imagination". *Academy of Management Review*, *14*(4), pp.516-531.

Wylde, A. (2021). *Zero trust: Never trust, always verify*. International conference on cyber situational awareness, data analytics and assessment (CYBERSA), June 14, 2021: 1-4). IEEE.

Wylde, A. Petani, F.J., Issa H. and Casoria, F. (2026). *Resilience to Disinformation Among Cyber Security and Information Warfare Professionals: Why Experts May Get it Wrong*. Presentation, AI Safety and Security (AI-SS), European Dependable Computing Conference (EDCC) IEEE 2026.

Zaheer, A., McEvily, B. and Perrone, V. (1998). "Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance". *Organization Science*, 9 no. 2: 41-159.