frontiers in Physics

TYPE Review
PUBLISHED 26 October 2026
DOI 10.3389/fphy.2026.1984375

Check for updates

OPEN ACCESS

EDITED BY
Feng Fu,
Dartmouth College, United States

REVIEWED BY
Lucas Skoufa,
Griffith University, Australia
Aming Li,
Peking University, China

*CORRESPONDENCE
The Anh Han,
t.han@tees.ac.uk
Matjaz Perc,
matjaz.perc@gmail.com

RECEIVED 31 August 2026
REVISED 23 September 2026
ACCEPTED 02 October 2026
PUBLISHED 26 October 2026

CITATION
Bashir A, Shamszaman ZU, Perc M and Han TA (2026) Social physics of cybersecurity.
Front. Phys. 14:1984375.
doi: 10.3389/fphy.2026.1984375

COPYRIGHT
© 2026 Bashir, Shamszaman, Perc and Han. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Social physics of cybersecurity

Adeela Bashir[1], Zia Ush Shamszaman[2], Matjaz Perc[3,4,5,6]* and The Anh Han[1,7]*

[1]School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough, United Kingdom, [2]Department of Informatics, Faculty of Natural, Mathematical and Engineering Sciences, King's College London, London, United Kingdom, [3]Faculty of Natural Sciences and Mathematics, University of Maribor, Maribor, Slovenia, [4]Community Healthcare Center Dr. Adolf Drolc Maribor, Maribor, Slovenia, [5]University College, Korea University, Seoul, Republic of Korea, [6]Department of Physics, Kyung Hee University, Seoul, Republic of Korea, [7]Centre for Digital Innovation, Teesside University, Middlesbrough, United Kingdom

Cybersecurity is increasingly recognised as a complex adaptive socio-technical system in which security outcomes emerge from the interactions of attackers, defenders, users, organisations, regulators, and autonomous artificial intelligence (AI) agents. These interactions generate adaptive feedback loops, strategic behaviour, information diffusion, and network effects that drive the evolution of cyber threats and defences. Consequently, phenomena such as attack propagation, cyber-risk contagion, cascading failures, and systemic resilience cannot be fully understood through static or purely technical perspectives. Although evolutionary game theory (EGT), complex systems science, network science, behavioural research, and cyber economics have each provided valuable insights, the literature remains fragmented, with no unified perspective for explaining cybersecurity as an evolving socio-technical ecosystem. This review develops the concept of Social Physics of Cybersecurity as an interdisciplinary perspective that brings these approaches together with human-AI interaction to explain how collective security outcomes emerge from adaptive interactions within interconnected cyber ecosystems. We synthesise research on attacker-defender co-evolution, finite and structured population dynamics, cyber contagion, critical transitions, systemic cyber risk, and the growing role of AI-enabled multi-agent systems. Building on these perspectives, we propose a unified multilevel view of cybersecurity that links individual strategic behaviour, network-level interactions, and system-wide resilience. We argue that cybersecurity should be understood as a social-physical phenomenon in which resilience and vulnerability emerge from the collective dynamics of interacting human and artificial agents. Finally, we identify key research opportunities for developing empirically grounded, data-driven, and AI-enabled models capable of predicting, analysing, and governing increasingly interconnected and autonomous cyber ecosystems.

KEYWORDS
Complex Adaptive Systems (CAS), cyber governance, cyber resilience, cybersecurity, evolutionary game theory (EGT), human-AI systems, network science, social physics

1 Introduction

Cybersecurity has traditionally been studied as a technical problem centred on software vulnerabilities, cryptographic protocols, and defensive mechanisms. While these technical foundations remain essential, contemporary cyber ecosystems increasingly exhibit behaviours that cannot be understood solely through engineering perspectives [1]. Cybersecurity emerges from the interactions of heterogeneous actors, including attackers,

defenders, users, organisations, artificial intelligence (AI) systems, and regulators, whose behaviours continuously adapt in response to one another [2]. As a result, cybersecurity is fundamentally a complex adaptive socio-technical system [3, 4].

The increasing interconnectedness of digital infrastructures has amplified this complexity. Cyber attacks rarely occur in isolation; rather, they unfold within dynamic environments where defensive measures trigger attacker adaptation, user behaviour shapes organisational risk [5, 6], and regulatory interventions alter incentives for both attackers and defenders [7]. These interactions generate feedback loops that operate across multiple temporal and organisational scales. Consequently, vulnerabilities, attacks, and defensive strategies evolve together, often producing emergent outcomes that are difficult to anticipate using traditional static models [8].

This perspective aligns naturally with the broader research agenda of social physics [9], which seeks to understand how collective phenomena emerge from interactions among many adaptive agents [10]. Over the last 2 decades, social physics and complex systems science have provided powerful tools for analysing cooperation, coordination, contagion, and collective decision-making in social systems [11–13]. Evolutionary game theory (EGT), network science, statistical physics, and agent-based modelling have revealed how simple local interactions can produce large-scale patterns of social organisation, resilience, and collapse [9, 12–15]. Similar mechanisms are increasingly visible in cybersecurity, where collective behaviours determine the spread of attacks, the adoption of defensive technologies, and the resilience of interconnected infrastructures [16, 17]. Recent advances in generative AI, autonomous cyber agents, and increasingly interconnected cyber-physical infrastructures further reinforce the need for a social-physics perspective. AI systems are becoming active participants in cyber defence while simultaneously enabling increasingly sophisticated attacks [13, 18, 19]. Consequently, cybersecurity is transitioning towards hybrid human-AI ecosystems in which autonomous agents continuously interact, adapt, and influence cyber risk [20, 21].

In this review, we define *Social Physics of Cybersecurity* as the study of how collective cybersecurity outcomes emerge from interactions among adaptive human and artificial agents embedded within interconnected socio-technical networks. Drawing upon EGT, complex systems science, network science, behavioural science, cyber economics, and AI-enabled multi-agent systems, this perspective seeks to explain cyber resilience, vulnerability, and systemic risk through the principles of emergence, self-organization, evolutionary dynamics, and feedback-driven adaptation. Evolutionary approaches are particularly relevant because cyber actors rarely possess perfect information or unlimited computational capabilities. Instead, attackers and defenders operate under uncertainty, learn from experience, imitate successful strategies, and adapt to changing environments [22, 23]. Rather than assuming fully rational actors who instantaneously optimise their decisions, evolutionary models explain how strategies spread, persist, or disappear over time through adaptation and selection [24]. These approaches have successfully explained the emergence of cooperation in social systems and provide a promising framework for understanding cyber conflict and cyber resilience [25, 26].

In contrast to this background, this review argues that social physics provides a unifying framework for understanding cybersecurity as a complex adaptive system. We first examine the foundations of social physics in cybersecurity and discuss how concepts from complex systems science, network science, and statistical physics explain collective cyber behaviour. We then review evolutionary approaches to attacker–defender interactions, highlighting how EGT, finite-population models, and structured population dynamics capture adaptive cyber conflict. Next, we examine behavioural cybersecurity and emerging human-AI cyber ecosystems, where trust, delegation, and collective adaptation increasingly shape security outcomes. Finally, we synthesise these research directions into a unified social-physics framework and identify key challenges and future opportunities for understanding and governing cybersecurity in increasingly interconnected and autonomous digital societies. The contribution is therefore not a new cybersecurity model but a multilevel synthesis that connects established theories of adaptation, interaction, and collective behaviour into a common framework for analysing cyber ecosystems.

2 Cybersecurity as a complex adaptive system

Cybersecurity is increasingly recognised as a complex adaptive socio-technical system in which security emerges from the interactions of interconnected human, technological, and institutional components. Rather than being determined solely by technical vulnerabilities or defensive mechanisms, cyber ecosystems evolve through continuous adaptation, feedback, and collective interactions among diverse actors. This systems perspective provides the foundation for understanding cybersecurity through the principles of social physics.

2.1 Interconnected cyber ecosystems

Cybersecurity should be viewed not simply as a technical challenge but as a complex adaptive system. In such systems, security outcomes emerge from interactions among many interconnected actors, technologies, and institutions rather than from the behaviour of any single component. Attackers, defenders, users, organisations, and increasingly AI agents continuously adapt to changing conditions, creating a dynamic environment in which risks and defensive strategies co-evolve [27]. A defining characteristic of cyber ecosystems is their strong dependence on network structure [28]. Modern digital infrastructures are highly interconnected through communication networks, cloud services, software dependencies, and supply chains. This interconnectedness enables attacks, vulnerabilities, and information to spread rapidly across systems [29–31]. Consequently, local incidents can generate wider system-level effects, as illustrated by large-scale supply-chain compromises and vulnerabilities in widely deployed software components [32, 33].

2.2 Emergence and self-organization

The interconnected nature of cyber ecosystems gives rise to emergent behaviours that cannot be explained by analysing

individual components in isolation. Security is therefore an emergent property of collective interactions rather than a fixed characteristic of isolated systems [8]. As attackers and defenders continuously adapt to one another, feedback loops shape the evolution of both offensive and defensive strategies, allowing cyber ecosystems to self-organise in response to changing threats. These adaptive processes shift cybersecurity beyond a vulnerability-centric perspective towards a systems-level understanding of resilience. Rather than focusing solely on preventing individual attacks, a complex systems perspective emphasises the collective dynamics that determine whether cyber ecosystems absorb, amplify, or recover from disturbances. This shift is particularly important in an era characterised by increasing interdependence, automation, and AI-driven adaptation.

2.3 Network effects and systemic risk

Viewing cybersecurity through the lens of social physics provides a natural bridge between technical security research and broader theories of collective behaviour. As illustrated in Figure 1, interactions among cyber actors generate evolutionary and social dynamics that produce system-level phenomena, including attack propagation, security adoption, cyber-risk contagion, cascading failures, and critical transitions. These emergent processes ultimately determine whether cyber ecosystems evolve towards resilience or systemic collapse.

Cyber resilience should therefore be understood not merely as a property of technologies but as an emergent property of interactions among individuals, organisations, infrastructures, and institutions operating within a continuously evolving environment. This perspective motivates the analytical foundations discussed next, focusing on emergence, adaptation, feedback, network dynamics, and critical transitions.

Figure 1 presents the conceptual framework that guides this review. It illustrates how the principles of social physics provide a common lens for connecting evolutionary dynamics, network interactions, behavioural processes, and AI-enabled cyber ecosystems. In addition, Figure 1 shows representative feedback pathways rather than every possible interaction. Feedback can occur both within and across the micro, meso, and macro levels. Macro-level outcomes can feed back into incentives, regulations, threat perceptions, and defensive behaviour, further shaping subsequent adaptation. These interactions are further examined in the following sections.

3 Foundations of social physics in cybersecurity

Social physics seeks to explain how large-scale collective behaviours emerge from the interactions of many adaptive agents. Rather than analysing individuals in isolation, it focuses on how local interactions, network structure, and feedback mechanisms generate system-level phenomena. These principles have been successfully applied to biological, social, and economic systems and are increasingly relevant to cybersecurity, where security outcomes arise from the continuous interactions of attackers, defenders, users, organisations, and AI agents embedded within interconnected digital environments.

3.1 Collective behaviour emergence and self-organization

A defining characteristic of complex systems is emergence, whereby global system behaviour cannot be inferred solely from the properties of individual components. In cybersecurity, large-scale phenomena such as cyber-risk propagation, coordinated attacks, security adoption, and organisational resilience emerge from numerous local interactions among heterogeneous actors. Consequently, cybersecurity should be viewed as a collective behavioural process rather than a collection of isolated technical events.

Self-organization further distinguishes cyber ecosystems from traditional engineered systems. Without central coordination, attackers, defenders, users, and organisations adapt to changing conditions, collectively shaping the long-term evolution of cyber ecosystems.

3.2 Adaptation, feedback, and network dynamics

Cyber ecosystems continuously evolve through feedback between offensive and defensive behaviours. Successful attacks stimulate stronger defensive mechanisms, while improved defences encourage attackers to develop increasingly sophisticated techniques. This reciprocal adaptation creates co-evolutionary dynamics that drive the long-term evolution of cybersecurity [8]. Amplifying feedback can increase cyber risk through rapid attack diffusion and behavioural contagion, whereas stabilising feedback can support learning, cooperation, and adaptive defence. Understanding these feedback mechanisms is essential for explaining why some cyber systems become increasingly resilient while others remain persistently vulnerable.

Cyber ecosystems also contain actors that adapt on substantially different timescales. Automated AI systems may update decisions or responses within seconds or minutes, whereas human users, organisational processes, and regulatory institutions may adapt over hours, months, or years. This creates a timescale mismatch in which rapidly adapting artificial or adversarial agents can operate within environments constrained by slower organisational and institutional responses. From a social-physics perspective, adaptation speed therefore becomes an important system-level variable: resilience depends not only on the quality of a defensive strategy, but also on whether organisational and institutional feedback can respond sufficiently quickly to changes in the threat environment. Such timescale mismatches may create transient vulnerabilities even when appropriate defensive capabilities exist, whereas shorter organisational feedback cycles may improve adaptation to rapidly changing threats. Future social-physics models should therefore consider heterogeneous adaptation rates across interacting populations and examine how differences in response times influence stability, escalation, and critical transitions.

These adaptive processes occur within complex communication, organisational, and technological networks rather than within isolated systems. Consequently, network topology strongly

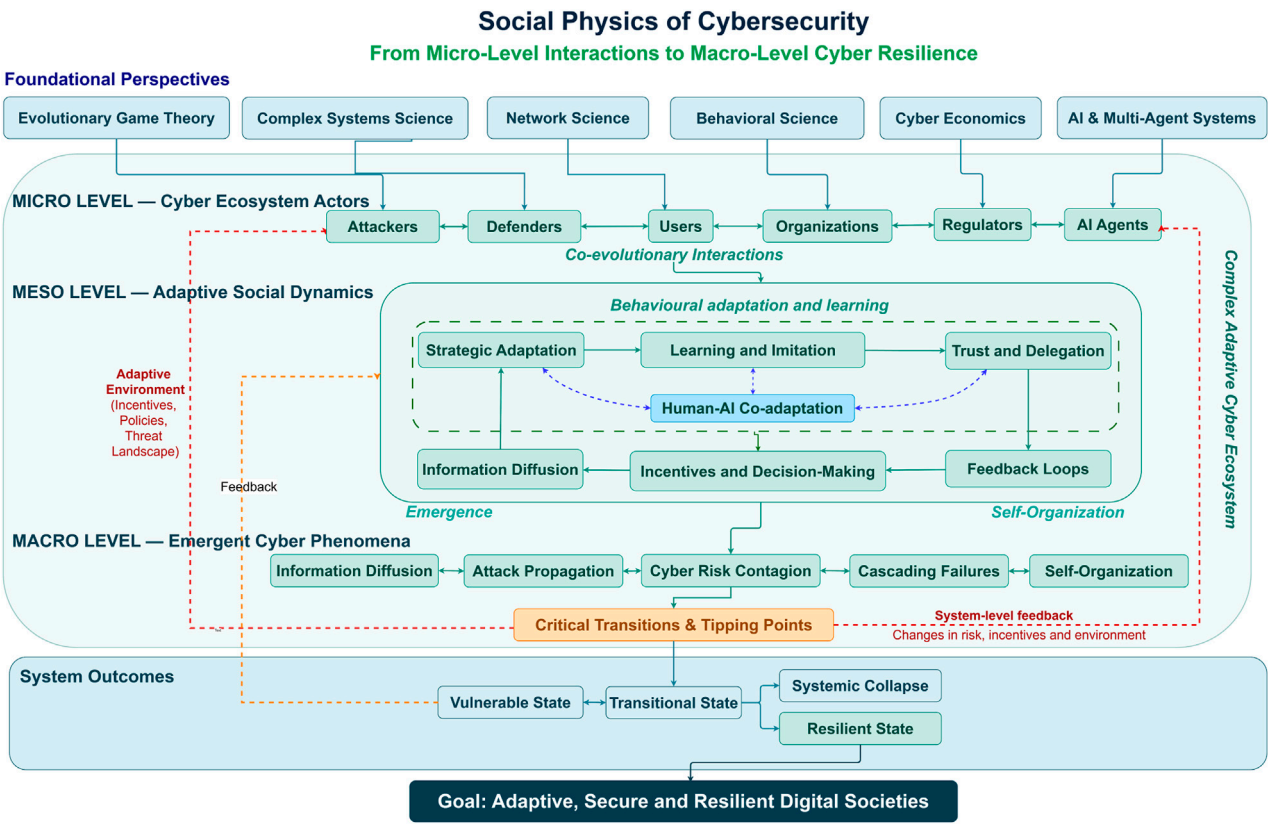


FIGURE 1
Social Physics of Cybersecurity as a complex adaptive socio-technical ecosystem. Cybersecurity emerges from the co-evolutionary interactions of attackers, defenders, users, organisations, regulators, and AI agents. Guided by insights from EGT, complex systems science, network science, behavioural science, cyber economics, and multi-agent systems, these interactions generate adaptive social dynamics that give rise to emergent cyber phenomena, including attack propagation, security adoption, cyber-risk contagion, cascading failures, and self-organization. Through feedback, critical transitions, and tipping points, cyber ecosystems evolve toward either resilience or systemic collapse, highlighting cybersecurity as an emergent property of complex adaptive systems rather than a purely technical problem.

influences how attacks, defensive information, trust, and security practices spread across cyber ecosystems [34, 35]. Concepts such as information diffusion, contagion, percolation, and cascading processes therefore provide powerful tools for understanding system-level cyber behaviour. The resilience of a cyber ecosystem depends not only on the security of individual components but also on the structure and connectivity of the underlying networks through which information and attacks propagate [36].

3.3 Critical transitions, resilience, and statistical physics

Complex adaptive systems often exhibit nonlinear behaviour in which gradual changes accumulate until critical thresholds are reached, triggering abrupt system-wide transitions. Similar phenomena are increasingly observed in cybersecurity. Small changes in attacker capability, defensive adoption, or network connectivity may lead to disproportionate changes in cyber risk, resilience, or system stability [27]. From a social-physics perspective, cyber resilience is therefore an emergent property of the entire ecosystem. Identifying critical thresholds before cascading failures occur represents an important challenge for future cybersecurity research.

Many of the concepts used to study physical systems have direct analogues in cybersecurity. Statistical physics provides mathematical tools for analysing collective behaviour, non-equilibrium dynamics, phase transitions, and large-scale interactions among many adaptive entities. When combined with EGT, network science, and behavioural modelling, these approaches provide a unified framework for understanding how cyber ecosystems evolve over time.

4 Evolutionary dynamics of attacker-defender systems

Among the various analytical frameworks used within social physics, EGT provides a useful approach for modelling adaptive cyber conflict. By explicitly capturing how attacker and defender strategies evolve through repeated interactions, evolutionary models explain how collective security outcomes emerge from strategic adaptation rather than isolated decision-making. Attackers seek to exploit vulnerabilities and maximise gains, while defenders attempt

to minimise risks and protect valuable assets. Classical game theory has long been used to model these interactions under assumptions of rational decision-making and well-defined incentives [2, 37]. Such models have generated valuable insights into cyber conflict, but they often struggle to capture the uncertainty, bounded rationality, and adaptive behaviour that characterise real-world cyber environments.

4.1 Evolutionary game theory in cybersecurity

EGT addresses these limitations by focusing on how strategies evolve through adaptation, learning, imitation, and selection rather than assuming fully rational optimisation. Strategies that perform well tend to spread within a population, while less successful strategies gradually disappear. As a result, EGT is particularly well suited to cybersecurity, where attackers and defenders continuously adjust their behaviours in response to changing threats and defensive measures [38, 39]. The application of EGT to cybersecurity has produced a diverse set of modelling approaches, including static and dynamic games [40], stochastic games [41], differential games [42], Stackelberg games [43], and evolutionary models based on replicator dynamics [8, 44]. While each framework offers unique insights, EGT is particularly useful for capturing long-term adaptation and population-level behavioural change.

A central contribution of EGT is its emphasis on evolutionary dynamics rather than equilibrium outcomes alone. Security outcomes emerge from the interaction of populations whose strategies continuously evolve in response to observed successes and failures. Attackers experiment with new attack vectors, defenders deploy countermeasures, and both sides adapt over time. Evolutionary mechanisms provide a mathematical framework for analysing how these strategic behaviours spread, persist, or decline within a population. This evolutionary view can be expressed through replicator dynamics (Equation 1), where the frequency of a strategy changes according to its relative payoff. For a strategy i with frequency x_i, payoff f_i, and average population payoff $\bar{f}$, the dynamics are given by

$$\frac{dx_i}{dt} = x_i\left(f_i - \bar{f}\right). \tag{1}$$

In an attacker-defender system, this equation links individual performance to population-level change. Strategies with higher payoffs increase in frequency, while less successful strategies decline. Thus, security states emerge from repeated adaptation rather than from a single optimal decision [8].

Beyond its relevance to cyber conflict, EGT establishes a direct link between cybersecurity and social physics. The same theoretical frameworks used to study cooperation, competition, and collective behaviour in biological and social systems can be applied to cyber ecosystems [12, 45–47]. This connection enables cybersecurity research to draw upon broader advances in evolutionary dynamics, network science, and statistical physics, providing a foundation for understanding cyber resilience as an emergent property of complex adaptive systems.

4.2 Attacker-defender co-evolution

A central theme in evolutionary cybersecurity is the co-evolution of attacker and defender strategies. Early game-theoretic studies established the importance of strategic interaction in cybersecurity, demonstrating how attackers and defenders adjust their behaviours in response to changing incentives and information. Subsequent work extended these ideas to dynamic settings in which both sides learn and adapt over time. Such models show that security outcomes depend not only on the strategies available to individual actors but also on how these strategies evolve within interacting populations [8].

Such co-evolutionary dynamics are visible across several cybersecurity domains. Intrusion detection systems encourage attackers to develop evasion techniques, which in turn stimulate improvements in detection algorithms [48, 49]. Adaptive malware modifies its behaviour to avoid identification, forcing defenders to adopt increasingly sophisticated analytical methods [50, 51]. Similarly, moving target defence strategies continuously alter system configurations to increase uncertainty for attackers, thereby changing the evolutionary landscape of cyber conflict [52, 53].

This population-level perspective is illustrated by the attacker-defender evolutionary model developed in [8]. The model represents attackers and defenders as two interacting populations whose strategy frequencies change according to their relative payoffs. As given in Equation 2, replicator dynamics capture how successful strategies spread or decline over time, allowing the system to move between qualitatively different equilibrium states.

$$\begin{aligned}\dot{\beta} &= \beta(1-\beta)\left(b_d - c_d - b_d\alpha + \nu b_d\alpha + \nu w\alpha\right),\\ \dot{\alpha} &= \alpha(1-\alpha)\left(-c_a + b_a - mp - b_a\nu\beta - \nu ns\beta + \nu mp\beta\right).\end{aligned} \tag{2}$$

Here, β and α denote the frequencies of defence and attack, respectively. The equations capture how changes in relative fitness drive the evolution of attack and defence strategies within the two interacting populations [8]. The analysis identifies four boundary equilibria corresponding to combinations of attack/no attack and defence/no defence, together with a potential internal equilibrium [8]. This provides a direct example of how local strategic interactions can generate stable or unstable system-level states.

The resulting phase portraits, in Figure 2, further illustrate this co-evolutionary process. The phase portraits illustrate qualitatively different outcomes, including a defence-dominated state, a contested state in which attack and defence remain simultaneously active, and an unstable internal state that separates evolutionary trajectories. In the published analysis, the internal point $(\beta, \alpha) = (0.84, 0.39)$ has eigenvalues of opposite signs, indicating saddle behaviour, with trajectories converging towards boundary equilibria depending on their initial conditions [8]. These equilibria depend on the underlying payoff parameters, which may vary across cybersecurity scenarios; changes in attack cost, attack benefit, or defence effectiveness can therefore reshape the equilibrium structure and evolutionary regime. These findings highlight a key principle of social physics: cybersecurity outcomes can emerge as collective evolutionary regimes rather than being determined by isolated actions.

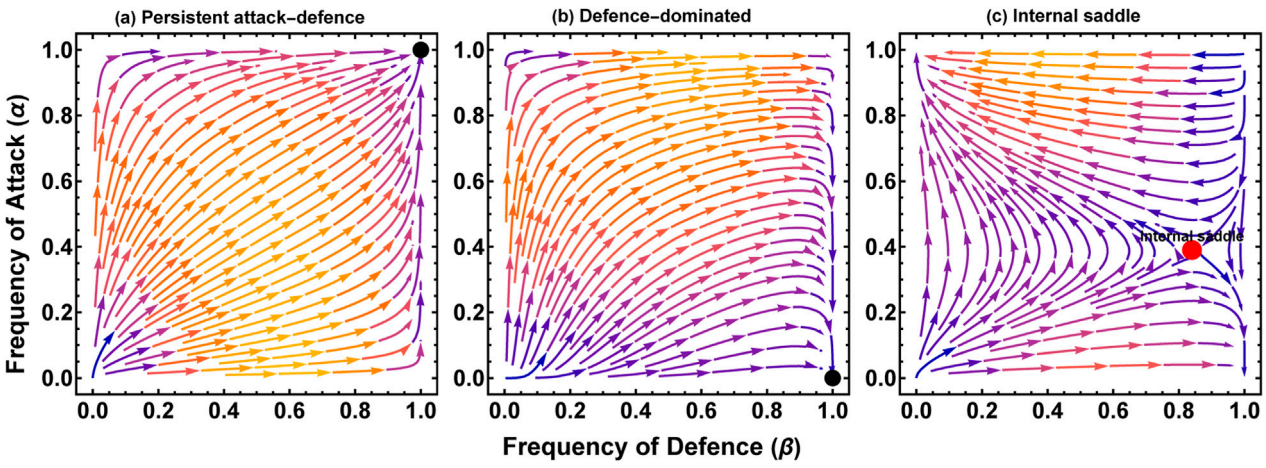


FIGURE 2
Evolutionary regimes in an attacker-defender cyber ecosystem obtained from replicator dynamics. Phase portraits illustrate convergence towards a persistent attack-defence competition in **(a)**, defence-dominated state in **(b)**, and an unstable internal equilibrium in **(c)**, acting as a saddle point. The trajectories demonstrate how population-level interactions can produce qualitatively different cybersecurity regimes. Regenerated from the evolutionary model in [8].

4.2.1 Beyond binary attacker-defender strategies

The binary attack/no-attack and defence/no-defence formulation provides a tractable baseline for illustrating co-evolutionary dynamics. However, real cyber ecosystems involve multiple competing strategies, such as exploitation, evasion, and persistence for attackers, and authentication, intrusion detection, or moving-target defence for defenders [48–53]. Extending EGT to multi-strategy populations would allow these alternatives to evolve simultaneously and could reveal richer dynamics, including larger number of stable equilibria, strategy coexistence, invasion of rare strategies, replacement, and cycling or other non-convergent evolutionary trajectories [54, 55]. Such extensions provide a natural pathway for studying strategic diversity and long-term attacker-defender co-adaptation in cyber ecosystems.

4.3 Finite and structured populations

Many evolutionary cybersecurity models consider large, well-mixed populations in which all agents interact equally with one another. Real cyber ecosystems, however, are finite, heterogeneous, and highly structured. Organisations differ substantially in resources and capabilities, users exhibit diverse security behaviours, and interactions occur through complex network topologies rather than random mixing. Finite-population evolutionary models provide a framework for studying these realities. Rather than focusing exclusively on average behaviour, such models account for stochastic effects that become important in realistic settings. Moran processes and related stochastic evolutionary models allow researchers to analyse fixation probabilities, estimate the likelihood that a strategy spreads throughout a population, and identify conditions under which rare behaviours become dominant [27]. These approaches are particularly relevant to cybersecurity because important defensive innovations often begin as minority strategies. Examples include the early adoption of multi-factor authentication [56, 57], zero-trust architectures [58, 59], or coordinated vulnerability disclosure practices [60]. Understanding whether such behaviours can spread throughout a population requires analysing finite-population dynamics rather than relying solely on deterministic approximations.

Finite populations also introduce stochastic strategy updating. A commonly used pairwise comparison rule is the Fermi function, as given in Equation 3 which assigns a probability to adopting a neighbouring strategy according to the payoff difference:

$$P(X \to Y) = \frac{1}{1 + \exp\left[-\kappa\left(f_Y - f_X\right)\right]}, \tag{3}$$

where κ controls the strength of selection. When selection is weak, strategy updating is close to random, whereas stronger selection favours strategies with higher payoffs. This provides a simple link between individual social learning and stochastic population-level change. Repeated stochastic updates can stimulate transitions between population states. In the rare-mutation limit, as given in Equation 4 these transitions form a Markov chain, whose stationary distribution $\boldsymbol{\pi}$ satisfies

$$\boldsymbol{\pi} M = \boldsymbol{\pi}, \qquad \sum_i \pi_i = 1, \tag{4}$$

where M is the transition matrix. Each π_i represents the long-run probability of observing a particular cyber state. This connects individual stochastic updating to the persistence of collective security states.

Beyond population size and stochasticity, network structure can introduce an additional layer of complexity. Organisations, devices, and users are embedded within communication and dependency networks whose topology can strongly influence cyber outcomes. Scale-free networks contain highly connected hubs that can accelerate both attack propagation and defensive information sharing. Small-world networks can facilitate rapid diffusion while maintaining local clustering. Enterprise environments frequently

exhibit layered and hierarchical structures that shape the movement of attackers and defenders. Evolutionary dynamics on structured populations reveal that network topology can fundamentally alter strategic outcomes [15, 61, 62].

Static network topology, however, captures only one dimension of cyber-system structure. Real cyber ecosystems are temporal: users and devices join or leave, communication links appear and disappear, software dependencies change, and attack surfaces are repeatedly reconfigured. Temporal network models can therefore represent how the timing and ordering of interactions influence attack propagation, defensive information sharing, and the persistence of secure behaviour. This extension is particularly relevant because temporality can alter the accessibility and controllability of dynamical processes compared with static network representations [63].

Cyber interactions can also extend beyond pairwise relationships. Organisation-wide security coordination, supply-chain defence, collaborative incident response, and multi-agent AI systems may involve groups of actors whose joint actions cannot be represented adequately by independent pairwise links. Higher-order networks, including hypergraphs and related representations, provide a way to model such multi-agent interactions explicitly. Recent evolutionary game research shows that higher-order interactions can alter the conditions and pathways through which collective strategies emerge and persist [64]. Incorporating higher-order interactions into evolutionary cybersecurity models could therefore reveal collective defensive behaviours and coordination effects that remain invisible in pairwise attacker-defender games.

Certain network structures can promote the spread of secure behaviours by enabling cooperative defence and information sharing [65]. Others can facilitate the persistence of insecure practices by creating isolated communities or concentrating vulnerabilities within critical hubs. Consequently, the question is not simply whether a defensive strategy is effective, but whether the surrounding network structure supports its adoption and persistence. Recent evolutionary cybersecurity results show that local interactions can promote defensive clustering through network reciprocity, suppress persistent attacks, and expand the region of secure outcomes [65]. These insights connect cybersecurity to a rich literature on evolutionary dynamics in structured populations and suggest promising opportunities for integrating network science and cyber risk analysis.

4.4 Evolutionary tipping points in cybersecurity

One of the most powerful contributions of social physics to cybersecurity is the concept of tipping points. Complex systems often exhibit critical transitions in which gradual changes accumulate until a threshold is reached, triggering abrupt shifts in system behaviour [66]. Similar phenomena are increasingly evident in cyber ecosystems [67]. The adoption of security technologies provides a clear example. Multi-factor authentication (MFA) often delivers limited benefits when adopted by only a small fraction of users. However, once adoption exceeds a critical threshold, attackers may find credential-based attacks substantially less profitable, leading to rapid reductions in successful compromises. Similar dynamics can emerge in the uptake of security patches, where collective adoption can dramatically reduce opportunities for exploitation. Conversely, cyber threats may also exhibit tipping-point behaviour. Ransomware campaigns frequently rely on network effects and behavioural contagion. Small increases in attacker capabilities, automation, or vulnerability prevalence may trigger rapid transitions from isolated incidents to widespread outbreaks. Once critical thresholds are crossed, attacks can propagate through interconnected systems at a scale that overwhelms traditional defensive mechanisms. A simple payoff comparison in [65] illustrates how such thresholds can arise. For example, as shown in Equation 5 when the expected benefit of attacking a defended system is lower than its cost, attack becomes evolutionarily unattractive:

$$c_a > b_a(1 - p_d), \tag{5}$$

where c_a is the attack cost, b_a is the attack benefit, and p_d is defence effectiveness. The condition illustrates how changes in defence effectiveness or attack incentives can shift the population from attack persistence towards non-attacking behaviour. Thus, the threshold is scenario-dependent: changes in these payoff parameters can shift the conditions for a critical transition. Under fixed parameters, the unstable internal equilibrium separates evolutionary basins of attraction, while changes in the underlying payoffs can reshape these basins and the resulting system-level regime.

These observations highlight the importance of non-linear dynamics in cybersecurity. Security is not merely the sum of individual decisions but an emergent property of collective behaviour. Small changes in defensive adoption, user awareness, attacker adaptation, or network structure can generate disproportionate system-level consequences. Identifying such critical thresholds remains an important research challenge. Integrating EGT with models of contagion, percolation, and cascading failures offers a promising way for understanding when cyber systems approach critical transitions and how interventions can shift them toward more resilient states. From this perspective, cybersecurity becomes not only a problem of defence but also a problem of managing the evolutionary and collective dynamics that shape digital societies.

5 Behavioural cybersecurity and Human-AI cyber ecosystems

Cybersecurity outcomes are shaped not only by technical mechanisms but also by how people, organisations, and AI systems adapt to changing threats. From a social-physics perspective, these behaviours are interconnected as individual decisions influence others through social and organisational networks, while repeated interactions generate collective patterns of trust, adaptation, and resilience. This section examines these behavioural and human-AI dynamics, focusing on social learning, trust, delegation, co-evolution, and collective intelligence.

5.1 Behavioural dynamics in cybersecurity

While technical vulnerabilities remain important, many cybersecurity incidents originate from human behaviour

[68]. Users make security decisions under uncertainty, often balancing convenience, trust, perceived risk, and cognitive effort. Consequently, cybersecurity outcomes depend not only on technological capabilities but also on how individuals and organisations adapt their behaviour in response to evolving threats [69, 70].

From a social-physics perspective, security behaviour emerges through interactions among individuals embedded within social and organisational networks. Security awareness campaigns, phishing attacks, password practices, and technology adoption are all influenced by social learning, imitation, and peer effects [17, 71]. As a result, secure and insecure behaviours can spread through populations in ways similar to information, opinions, and infectious diseases [72]. Behavioural cybersecurity therefore exhibits many of the characteristics of complex adaptive systems [73]. Individual decisions aggregate into collective patterns, feedback loops shape future behaviour, and local interactions can generate system-wide consequences [74]. Understanding these dynamics is essential for explaining why security interventions succeed in some environments but fail in others. Cybersecurity awareness and training can therefore be viewed as interventions that modify behavioural adaptation and the diffusion of secure strategies within a population rather than as static educational activities.

5.2 Trust and delegation in Human-AI cyber systems

The increasing deployment of AI is transforming cybersecurity from a purely human-centred activity into a hybrid human-AI ecosystem [75]. AI systems now assist with threat detection, vulnerability analysis, incident response, and security monitoring [76]. At the same time, attackers increasingly employ AI to automate reconnaissance, generate phishing content, and identify vulnerabilities at scale [77].

This growing reliance on AI introduces new questions regarding trust, delegation, and decision-making [78, 79]. Security analysts must determine when AI recommendations should be accepted, challenged, or overridden. Excessive trust may result in automation bias, while insufficient trust can prevent organisations from fully benefiting from AI capabilities [80, 81]. Consequently, effective cybersecurity increasingly depends on achieving an appropriate balance between human judgement and automated decision support [82, 83]. From an evolutionary perspective, trust in AI is not static [34, 84–87]. It evolves through repeated interactions and feedback from previous outcomes. Successful AI-assisted decisions strengthen confidence in automated systems, whereas failures may reduce trust and encourage greater human oversight. Understanding these adaptive trust dynamics is becoming a central challenge for future cybersecurity research.

5.3 Human-AI Co-evolutionary dynamics

The introduction of AI therefore extends the traditional attacker-defender evolutionary setting to a multi-population environment. The integration of AI into cybersecurity creates a new layer of co-evolutionary dynamics [88]. Attackers adapt to defensive AI systems by developing new evasion strategies, while defensive systems continuously learn from emerging attack patterns [89, 90]. Simultaneously, human operators adapt their behaviour in response to both adversarial activity and AI-generated recommendations [75]. As a result, cybersecurity increasingly involves three interacting populations: attackers, defenders, and AI agents [91]. Changes in one population influence the behaviour of the others, generating complex feedback loops that can amplify or suppress cyber risk [92, 93]. These interactions resemble broader complex adaptive systems in which multiple adaptive agents continuously respond to changing environmental conditions. The increasing autonomy of AI systems does not necessarily imply the displacement of human actors. Rather, it changes the distribution of decision-making, coordination, and adaptation across the cyber ecosystem. As AI systems become faster, more scalable, and more autonomous, some operational tasks may shift from human operators to artificial agents, while humans may increasingly concentrate on oversight, contextual judgement, governance, and high-impact decisions.

From a social-physics perspective, the relevant question is therefore not whether humans or AI will dominate, but how changes in autonomy, delegation, and human oversight reshape the interactions and feedback loops through which cyber outcomes emerge. This also raises the possibility that human agents may become less central to some operational processes while remaining essential at organisational and governance levels. Understanding this changing distribution of agency therefore requires moving beyond traditional attacker-defender models towards frameworks capable of capturing human-AI co-adaptation. Evolutionary dynamics, agent-based modelling, and network-based approaches provide promising tools for analysing these emerging ecosystems.

5.4 Collective intelligence and cyber resilience

One of the most promising opportunities created by human-AI ecosystems is the emergence of collective intelligence. Human expertise provides contextual reasoning, creativity, and strategic judgement, while AI systems contribute speed, scalability, and data-processing capabilities. Together, these complementary strengths can improve threat detection, incident response, and organisational resilience [94–96]. However, collective intelligence is not always guaranteed. Poor coordination, biased decision-making, over-reliance on automation, and misinformation can reduce the effectiveness of both human and AI agents. Consequently, cyber resilience should be viewed as an emergent property arising from interactions among individuals, organisations, technologies, and AI systems rather than as a feature of any single component. From a social-physics perspective, resilience emerges when adaptive interactions enable cyber ecosystems to absorb disturbances, recover from attacks, and maintain essential functionality despite changing threats.

6 Economic and regulatory dynamics of cyber ecosystems

Cybersecurity is influenced not only by technical capabilities but also by economic incentives, institutional policies, and regulatory decisions. Organisations, governments, and individuals continuously balance the costs of security investments against

the risks of cyber attacks. Consequently, cyber resilience emerges from the interaction of technological, behavioural, economic, and governance factors rather than from technical solutions alone.

6.1 Cybersecurity economics, incentives and externalities

Cybersecurity investments are often constrained by limited resources and competing organisational priorities. Decisions regarding security technologies, employee training, and infrastructure protection therefore depend on balancing expected costs against potential losses. Because attackers and defenders respond strategically to these investment decisions, cybersecurity naturally exhibits economic dynamics that evolve over time. Evolutionary and game-theoretic models provide useful tools for analysing how security investments influence long-term cyber resilience [97, 98]. Rather than identifying a single optimal investment, these approaches explain how defensive strategies adapt as attackers modify their behaviour and new threats emerge.

Security decisions rarely affect only the organisation making them. Weak security in one organisation may increase risks for connected partners, customers, or critical infrastructures. These interdependencies create security externalities in which local decisions generate system-wide consequences [99]. Such environments often encourage free-riding, where organisations rely on others to invest in cybersecurity while limiting their own expenditure [100]. Social-physics approaches provide a population-level perspective for understanding how incentives, cooperation, and collective behaviour influence the adoption of secure practices across interconnected cyber ecosystems. Evolutionary analysis in cybersecurity also shows that improving security does not automatically maximise collective welfare. Defence effectiveness, attack costs, and the cost of security investment must be considered together, highlighting an important social-physics principle: resilient cyber ecosystems must balance security outcomes with the incentives that sustain secure behaviour [8]. Finite-population analysis further shows that unequal access to advanced defence capabilities can change evolutionary outcomes. High-cost defensive strategies may remain difficult to adopt even when they provide stronger protection, while committed defenders and targeted subsidies can shift the population towards safer states [27]. This illustrates how economic incentives and policy interventions can reshape collective cyber behaviour.

6.2 Cyber insurance, systemic risk and governance

Cyber insurance has emerged as an important mechanism for managing financial losses associated with cyber attacks [101]. However, insurance does not eliminate cyber risk; instead, it redistributes risk across organisations and markets. As cyber incidents become increasingly interconnected, correlated attacks may produce simultaneous losses that challenge the stability of insurance systems [102]. Understanding these dynamics requires moving beyond individual organisations to consider systemic cyber risk. Combining evolutionary dynamics with network science and risk modelling offers new opportunities for analysing how cyber risk propagates through interconnected digital economies.

Governments and regulatory bodies play an increasingly important role in shaping cybersecurity behaviour. Security standards, privacy regulations, reporting requirements, and international cooperation can influence how organisations allocate resources and respond to cyber threats. From a social-physics perspective, regulation acts as an external force that influences the evolution of cyber ecosystems. Effective governance should therefore encourage adaptive learning, cooperation, and information sharing while maintaining sufficient flexibility to respond to rapidly evolving threats. Understanding how regulatory interventions reshape collective cyber behaviour remains an important challenge for future research [103].

7 A social physics synthesis of cybersecurity

As discussed in the preceding sections, cybersecurity outcomes emerge from interactions across multiple organisational and temporal scales. Social physics provides a unifying perspective for connecting these scales, as illustrated in Figure 1. The framework begins with the foundational perspectives of evolutionary game theory, complex systems science, network science, behavioural science, cyber economics, and AI-driven multi-agent systems, and traces how these perspectives explain the evolution of cyber ecosystems from individual interactions to system-wide outcomes.

At the *micro level*, the dynamics begin with heterogeneous cyber ecosystem actors, including attackers, defenders, users, organisations, regulators, and AI agents. These actors continuously learn, adapt, cooperate, and compete under uncertainty, generating co-evolutionary interactions shaped by strategic adaptation, learning and imitation, trust and delegation, incentives, and human-AI co-adaptation. As these local interactions become embedded within communication, organisational, and technological networks, they give rise to *meso-level adaptive social dynamics*. Network structure influences the diffusion of information, attacks, trust, and security practices, while feedback loops, collective adaptation, and self-organization amplify or constrain these processes. Temporal and higher-order network structures naturally extend the meso-level of this framework. Temporal networks capture when interactions occur and how changing connectivity reshapes the evolution of strategies, while higher-order networks capture collective interactions among groups of actors rather than only pairwise relationships. These structures can mediate the pathway from micro-level adaptation to macro-level phenomena such as contagion, cascading failures, and critical transitions.

These interconnected dynamics can then produce *macro-level emergent cyber phenomena* that extend beyond the behaviour of individual actors or networks. Attack propagation, cyber-risk contagion, cascading failures, and self-organization may develop through the accumulation of local interactions and network effects. As these processes evolve, cyber ecosystems can approach critical transitions and tipping points, leading to different system states ranging from vulnerability and transition to resilience or systemic collapse. Thus, the framework captures a fundamental multi-scale pathway in cybersecurity where individual incentives

10.3389/fphy.2026.1984375

TABLE 1 Research directions in the Social Physics of Cybersecurity.

Research area	Key research questions	Potential methodologies
Level 1 (micro) – Adaptive actors and strategies: How do individual and population-level strategies adapt?		
Evolutionary attacker-defender dynamics	(1) How do attack and defence strategies co-evolve over time? (2) under what conditions do defensive strategies become evolutionarily stable? (3) how does strategic adaptation influence cyber resilience?	EGT, replicator dynamics, stochastic evolutionary processes, agent-based simulations, empirical cyber data
Behavioural cybersecurity and collective adaptation	(1) How do secure behaviours emerge and spread? (2) how do trust and social learning influence cyber resilience? (3) what drives long-term adoption of secure practices?	Behavioural experiments, social learning models, evolutionary dynamics, longitudinal user studies
Human-AI cyber ecosystems	(1) How do humans and AI agents co-adapt under cyber threats? (2) how does trust evolve in AI-assisted cybersecurity? (3) how should responsibility be shared between humans and AI?	Human-AI interaction experiments, evolutionary trust models, LLM-based societies, multi-agent simulations
Level 2 (meso) – Interactions and network structure: How do connectivity, population structure, and collective interactions shape adaptation?		
Finite and structured cyber populations	(1) How does population structure affect cyber defence? (2) when can secure behaviours invade vulnerable populations? (3) what role do network topology and stochasticity play?	Moran processes, fixation analysis, graph-based evolutionary games, structured population models
Temporal and higher-order network dynamics	(1) How do attacks and defensive information diffuse across changing networks? (2) how do temporal network structure and interaction timing affect cyber contagion and cascading failures? (3) how do higher-order interactions and group coordination reshape evolutionary cyber dynamics?	Temporal network analysis, higher-order networks, hypergraph models, contagion models, evolutionary games, statistical physics, resilience analysis
Level 3 (Macro)– Emergent system behaviour and resilience: How do collective dynamics produce critical transitions and systemic outcomes?		
Critical transitions and cyber resilience	(1) What tipping points separate resilient and vulnerable cyber ecosystems? (2) which indicators provide early warning of cyber crises? (3) how can interventions steer systems towards resilient states?	Complex systems modelling, dynamical systems, resilience metrics, early-warning signal detection
Cross-level mechanisms: How do incentives and governance influence adaptation across all levels?		
Cybersecurity economics and incentives	(1) How do economic incentives influence cybersecurity investment? (2) how do security externalities shape collective outcomes? (3) how can free-riding be reduced?	Evolutionary economics, game theory, cyber insurance models, interdependent security analysis
Governance and regulatory dynamics	(1) How do regulations influence cyber behaviour? (2) which governance mechanisms promote adaptive resilience? (3) how can policy reduce systemic cyber risk?	Governance frameworks, policy simulations, evolutionary population models, scenario analysis
Integrating framework: How can these levels be unified to explain emergent cyber-system behaviour?		
Social physics of cybersecurity	(1) How can evolutionary dynamics, network science, and behavioural models be unified? (2) how can cyber ecosystems be modelled across micro-, meso-, and macro-levels? (3) how can empirical data validate real-world cyber datasets?	Integrated social-physics framework, statistical physics, complex systems modelling, AI-enabled cyber simulations, interdisciplinary empirical studies

shape behaviour, repeated interactions generate population dynamics, network structure modifies the spread of behaviour, and collective dynamics produce system-level resilience or vulnerability.

Viewed collectively, these levels illustrate the central principle of social physics: cybersecurity is an emergent property of interacting populations rather than a static property of individual technologies. Integrating evolutionary dynamics, complex systems science, network interactions, behavioural cybersecurity, economics, and AI-enabled multi-agent systems therefore provides a unified basis for understanding, predicting, and governing the evolution of increasingly interconnected cyber ecosystems.

8 Implications of a social physics perspective

Viewing cybersecurity through the lens of social physics shifts attention from isolated technical incidents towards the collective dynamics through which cyber ecosystems evolve. This perspective provides a basis for identifying feedback loops, critical transitions, systemic risk, and emergent resilience, while integrating insights from evolutionary dynamics, network science, behavioural research, economics, and human-AI systems. Such a framework can inform adaptive defence, resilient digital infrastructures, and evidence-based governance. Table 1 summarises the resulting research agenda, organised according to the micro–meso–macro framework rather than as independent priorities. Together, these directions connect adaptive actors and strategies to networked interactions and emergent system-level outcomes.

9 Future research directions

Despite significant progress, several challenges remain. A major priority is the development of empirically validated evolutionary models that connect theoretical predictions with real-world cybersecurity data. Such validation should include both parameter calibration against observed cyber behaviour and out-of-sample evaluation of predicted evolutionary regimes. Greater attention is also needed for finite and structured population models that better represent the heterogeneity of modern cyber ecosystems.

Future research should investigate cyber contagion, cascading failures, critical transitions, and systemic cyber risk using integrated models that combine EGT, network science, statistical physics, and agent-based simulations. An important extension is to move beyond static pairwise networks towards temporal and higher-order network representations. Such models would extend the micro–meso–macro framework by making the structure and timing of interactions explicit rather than treating them as fixed background conditions. Another important direction is the emergence of autonomous AI agents and large-scale multi-agent cyber environments. Understanding how humans and AI systems cooperate, compete, and co-adapt under evolving cyber threats will be essential for designing trustworthy and resilient digital infrastructures. Future models should examine how delegation, oversight, human intervention, and AI autonomy alter evolutionary dynamics, organisational decision-making, and cyber resilience. Rather than assuming either human dominance or AI replacement, such models can treat the distribution of agency itself as an evolving property of the cyber ecosystem.

Heterogeneous adaptation timescales represent another important research direction. Attackers, AI systems, human users, organisations, and regulators may respond to cyber events at very different rates. Rapidly adapting AI agents can therefore interact with slower organisational decision processes, creating delays between threat emergence, detection, decision-making, and intervention. Future models should incorporate heterogeneous adaptation rates and organisational response delays to investigate whether timescale mismatches amplify cyber risk, destabilise otherwise resilient systems, or create opportunities for adaptive intervention. Finally, the Social Physics of Cybersecurity requires closer collaboration across cybersecurity, physics, AI, economics, and behavioural science. Developing common datasets, shared modelling frameworks, and empirical validation methods will be critical for establishing this interdisciplinary field and translating theoretical advances into practical cyber resilience.

10 Conclusion

Cybersecurity is no longer solely a technical problem. It is a complex adaptive socio-technical system in which attackers, defenders, users, organisations, regulators, and increasingly autonomous AI agents continuously interact, learn, and evolve. These interactions generate collective behaviours, feedback loops, and systemic risks that cannot be fully explained through traditional security models. This review has argued that Social Physics provides a unifying framework for understanding these dynamics. By integrating insights from EGT, finite and structured population dynamics, complex systems science, network science, behavioural cybersecurity, cyber economics, and human-AI interaction, we have shown that cyber resilience emerges from the collective behaviour of interconnected populations rather than from individual technologies or isolated defensive mechanisms.

Viewing cybersecurity through this interdisciplinary lens shifts the focus from preventing individual attacks to understanding how cyber ecosystems evolve, adapt, and respond to changing conditions. Such a perspective provides new opportunities for analysing systemic cyber risk, identifying critical transitions, and designing adaptive security strategies for increasingly autonomous digital environments. Ultimately, we argue that cybersecurity should be understood as a *social-physical phenomenon*, whose behaviour emerges from interacting populations of human and artificial agents embedded within complex socio-technical networks. Establishing the Social Physics of Cybersecurity as an interdisciplinary research paradigm offers a promising foundation for understanding, predicting, and governing the resilient digital societies of the future.

Author contributions

AB: Visualization, Writing – original draft, Validation, Formal Analysis, Conceptualization, Writing – review and editing,

Methodology, Investigation, Software. ZS: Writing – review and editing, Validation, Supervision, Investigation, Methodology, Conceptualization, Writing – original draft. MP: Supervision, Conceptualization, Writing – original draft, Investigation, Validation, Writing – review and editing. TH: Methodology, Supervision, Conceptualization, Validation, Investigation, Funding acquisition, Writing – review and editing, Resources, Writing – original draft, Project administration.

Funding

The author(s) declared that financial support was received for this work and/or its publication. TH is supported by EPSRC (grant EP/Y00857X/1). MP was supported by the Slovenian Research and Innovation Agency (Grant No. P1-0403).

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

The authors MP, TH declared that they were an editorial board member of Frontiers at the time of submission. This had no impact on the peer review process and the final decision.

Generative AI statement

The author(s) declared that generative AI was used in the creation of this manuscript. Generative AI was used for improving clarity of the paper.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Shiva S, Roy S, Dasgupta D. Game theory for cyber security. In: *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (2010). p. 1–4. doi: 10.1145/1852666.1852704

2. Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, et al. Game theory for cyber security and privacy. *ACM Comput Surv (Csur)* (2017) 50:1–37. doi: 10.1145/3057268

3. Michael K, Vogel KM, Pitt J, Zafeirakopoulos M. Artificial intelligence in cybersecurity: a socio-technical framing. *IEEE Trans Technology Soc* (2024) 6:15–30. doi: 10.1109/TTS.2024.3460740

4. Taddeo M, Jones P, Abbas R, Vogel K, Michael K. Socio-technical ecosystem considerations: an emergent research agenda for ai in cybersecurity. *IEEE Trans Technology Soc* (2023) 4:112–8. doi: 10.1109/TTS.2023.3278908

5. Alsharida RA, Al-rimy BAS, Al-Emran M, Zainal A. A systematic review of multi perspectives on human cybersecurity behavior. *Technology Society* (2023) 73:102258. doi: 10.1016/j.techsoc.2023.102258

6. AlQadheeb A, Bhattacharyya S, Perl S. Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. *Array* (2022) 14:100146. doi: 10.1016/j.array.2022.100146

7. Wessels M, van den Brink P, Verburgh T, Cadet B, van Ruijven T. Understanding incentives for cybersecurity investments: development and application of a typology. *Digital Business* (2021) 1:100014. doi: 10.1016/j.digbus.2021.100014

8. Bashir A, Shamszaman ZU, Song Z, Han TA. Co-evolutionary dynamics of attack and defence in cybersecurity. *Knowledge-Based Syst* (2026) 340:115750. doi: 10.1016/j.knosys.2026.115750

9. Jusup M, Holme P, Kanazawa K, Takayasu M, Romić I, Wang Z, et al. Social physics. *Phys Rep* (2022) 948:1–148. doi: 10.1016/j.physrep.2021.10.005

10. Quang LA, Jung N, Cho ES, Choi JH, Lee JW. Agent-based models in social physics. *J Korean Phys Soc* (2018) 72:1272–80. doi: 10.3938/jkps.72.1272

11. Paul S, Mukherjee D, Mitra A, Mitra A, Dutta PK. Unravelling the complex networks of social physics: exploring human behavior, big data, and distributed systems. *J Social Comput* (2024) 5:165–79. doi: 10.23919/JSC.2024.0014

12. Perc M, Jordan JJ, Rand DG, Wang Z, Boccaletti S, Szolnoki A. Statistical physics of human cooperation. *Phys Rep* (2017) 687:1–51. doi: 10.1016/j.physrep.2017.05.004

13. Han TA, Baronchelli A, Leibo JZ, Lenaerts T, Rahwan I, Santos FP, et al. Social physics in the age of artificial intelligence. *Philosophical Trans R Soc* (2026) A. In press. doi: 10.48550/arXiv.2603.16900

14. Tsarev D, Trofimova A, Alodjants A, Khrennikov A. Phase transitions, collective emotions and decision-making problem in heterogeneous social systems. *Scientific Reports* (2019) 9:18039. doi: 10.1038/s41598-019-54296-7

15. Szabó G, Fath G. Evolutionary games on graphs. *Phys Reports* (2007) 446:97–216. doi: 10.1016/j.physrep.2007.04.004

16. Veksler VD, Buchler N, Hoffman BE, Cassenti DN, Sample C, Sugrim S. Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. *Front Psychology* (2018) 9:691. doi: 10.3389/fpsyg.2018.00691

17. McAlaney J, Benson V. Cybersecurity as a social phenomenon. In: *Cyber Influence and Cognitive Threats*. Elsevier (2020). p. 1–8. doi: 10.1016/B978-0-12-819204-7.00001-4

18. Adeyemi DS. Human-ai collaboration in cybersecurity decision-making: a systematic review of literature. *Commun In Phys Sci* (2026) 13:403–21.

19. Saeri AK, Graham J, Noetel M, Slattery P, Ah-King D, Aittokallio E, et al. *Prioritization of Risks from Artificial Intelligence: A Delphi Study of 272 International Experts* (2026). *Pre-print available arXiv:2606.04490*.

20. Bates E, Mavroudis V, Hicks C. Reward shaping for happier autonomous cyber security agents. In: *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security* (2023). p. 221–32. doi: 10.1145/3605764.3623916

21. Kacheru G. Autonomous ai agents for cybersecurity: detecting and responding to threats in real time. In: *International Conference on Intelligent Computing and Communication*. Springer (2025). p. 53–64. doi: 10.1007/978-3-032-18349-1_6

22. Moisan F, Gonzalez C. Security under uncertainty: adaptive attackers are more challenging to human defenders than random attackers. *Front Psychology* (2017) 8:982. doi: 10.3389/fpsyg.2017.00982

23. Zhang Y, Malacaria P. Dealing with uncertainty in cybersecurity decision support. *Comput and Security* (2025) 148:104153. doi: 10.1016/j.cose.2024.104153

24. Willard GN. Understanding the co-evolution of cyber defenses and attacks to achieve enhanced cybersecurity. *J Inf Warfare* (2015) 14:16–30.

25. Kianpour M, Kowalski SJ, Øverby H. Advancing the concept of cybersecurity as a public good. *Simulation Model Pract Theor* (2022) 116:102493. doi: 10.1016/j.simpat.2022.102493

26. Kianpour M, Øverby H, Kowalski SJ, Frantz C. Social preferences in decision making under cybersecurity risks and uncertainties. In: *International Conference on Human-Computer Interaction*. Springer (2019). p. 149–63. doi: 10.1007/978-3-030-22351-9_10

27. Bashir A, Shamszaman ZU, Song Z, Perc M, Han TA. Strategic commitments shape collective cybersecurity under ai inequality. *Chaos, Solitons and Fractals* (2026) 210:118728. doi: 10.1016/j.chaos.2026.118728

28. La RJ. Role of network topology in cybersecurity. *53rd IEEE Conf on Decis and Control (Ieee)* (2014) 5290–5. doi: 10.1109/CDC.2014.7040216

29. Pandey S, Singh RK, Gunasekaran A, Kaushik A. Cyber security risks in globalized supply chains: conceptual framework. *J Glob Operations Strateg Sourcing* (2020) 13:103–28. doi: 10.1108/JGOSS-05-2019-0042

30. Tan Z, Parambath SP, Anagnostopoulos C, Singer J, Marnerides AK. Advanced persistent threats based on supply chain vulnerabilities: challenges, solutions, and future directions. *IEEE Internet Things J* (2025) 12:6371–95. doi: 10.1109/JIOT.2025.3528744

31. Huynh PHT, Vinh DT, Lam KDA, Truong ANN, Bui UNT, Dinh KN, et al. Reputation-driven cooperation in lattice-based decentralized federated learning through evolutionary game theory (2026). Pre-print arxiv.org/abs/2608.01197.

32. Bandyopadhyay T, Jacob V, Raghunathan S. Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *Inf Technology Management* (2010) 11:7–23. doi: 10.1007/s10799-010-0066-1

33. Azmat H. Cybersecurity in supply chains: protecting against risks and addressing vulnerabilities. *Int J Digital Innovation* (2025) 6.

34. Bashir A, Song Z, Ogbo NB, Balabanova N, Smit M, Leung C, et al. *Trust as Monitoring: Evolutionary Dynamics of User Trust and Ai Developer Behaviour* (2026). arXiv preprint arXiv:2603.24742.

35. Alalawi Z, Bova P, Cimpeanu T, Di Stefano A, Duong MH, Domingos EF, et al. Trust ai regulation? Discerning users are vital to build trust and effective ai regulation. *Appl Mathematics Comput* (2026) 508:129627. doi: 10.1016/j.amc.2025.129627

36. Wang Z, Wang L, Szolnoki A, Perc M. Evolutionary games on multilayer networks: a colloquium. *The Eur Physical Journal B* (2015) 88:124. doi: 10.1140/epjb/e2015-60270-7

37. Pawlick J, Colbert E, Zhu Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Comput Surv (Csur)* (2019) 52:1–28. doi: 10.1145/3337772

38. Douha NYR, Sasabe M, Taenaka Y, Kadobayashi Y. An evolutionary game theoretic analysis of cybersecurity investment strategies for smart-home users against cyberattacks. *Appl Sci* (2023) 13:4645. doi: 10.3390/app13074645

39. Yang P, Gao F, Zhang H. Multi-player evolutionary game of network attack and defense based on system dynamics. *Mathematics* (2021) 9:3014. doi: 10.3390/math9233014

40. Etesami SR, Başar T. Dynamic games in cyber-physical security: an overview. *Dynamic Games Appl* (2019) 9:884–913. doi: 10.1007/s13235-018-00291-y

41. Miao F, Zhu Q, Pajic M, Pappas GJ. A hybrid stochastic game for secure control of cyber-physical systems. *Automatica* (2018) 93:55–63. doi: 10.1016/j.automatica.2018.03.012

42. Zhang H, Mi Y, Fu Y, Liu X, Zhang Y, Wang J, et al. Security defense decision method based on potential differential game for complex networks. *Comput and Security* (2023) 129:103187. doi: 10.1016/j.cose.2023.103187

43. Zhang Y, Malacaria P. Bayesian stackelberg games for cyber-security decision support. *Decis Support Syst* (2021) 148:113599. doi: 10.1016/j.dss.2021.113599

44. Boudko S, Abie H. Adaptive cybersecurity framework for healthcare internet of things. In: *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE (2019). p. 1–6. doi: 10.1109/ISMICT.2019.8743905

45. D'Orsogna MR, Perc M. Statistical physics of crime: a review. *Phys Life Reviews* (2015) 12:1–21. doi: 10.1016/j.plrev.2014.11.001

46. Song Z, Anh Han T. Emergence of cooperation and commitment in optional prisoner's dilemma. *Appl Math Model* (2026) 155:116603. doi: 10.1016/j.apm.2025.116603

47. Qu X, Kurokawa S, Han TA. The evolution of cooperation and tolerance under conditional dissociation in cohesive population. *Chaos, Solitons and Fractals* (2026) 208:118214. doi: 10.1016/j.chaos.2026.118214

48. Huang H, Li T, Li B, Wang W, Sun Y. A bidirectional differential evolution based unknown cyberattack detection system. *IEEE Trans Evol Comput* (2024) 29:459–73. doi: 10.1109/TEVC.2024.3365101

49. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* (2019) 2:1–22. doi: 10.1186/s42400-019-0038-7

50. Ferdous J, Islam R, Mahboubi A, Islam MZ. A review of state-of-the-art malware attack trends and defense mechanisms. *IEEE Access* (2023) 11:121118–41. doi: 10.1109/ACCESS.2023.3328351

51. Yan S, Ren J, Wang W, Sun L, Zhang W, Yu Q. A survey of adversarial attack and defense methods for malware classification in cyber security. *IEEE Commun Surv and Tutorials* (2022) 25:467–96. doi: 10.1109/COMST.2022.3225137

52. Sengupta S, Chowdhary A, Sabur A, Alshamrani A, Huang D, Kambhampati S. A survey of moving target defenses for network security. *IEEE Commun Surv and Tutorials* (2020) 22:1909–41. doi: 10.1109/COMST.2020.2982955

53. Griffioen P, Weerakkody S, Sinopoli B. A moving target defense for securing cyber-physical systems. *IEEE Trans Automatic Control* (2020) 66:2016–31. doi: 10.1109/TAC.2020.3005686

54. Gokhale CS, Traulsen A. Evolutionary games in the multiverse. *Proc Natl Acad Sci* (2010) 107:5500–4. doi: 10.1073/pnas.0912214107

55. Duong MH, Han TA. Analysis of the expected density of internal equilibria in random evolutionary multi-player multi-strategy games. *J Math Biol* (2016) 73:1727–60. doi: 10.1007/s00285-016-1010-8

56. Ometov A, Petrov V, Bezzateev S, Andreev S, Koucheryavy Y, Gerla M. Challenges of multi-factor authentication for securing advanced iot applications. *IEEE Netw* (2019) 33:82–8. doi: 10.1109/MNET.2019.1800240

57. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: a survey. *Cryptography* (2018) 2:1. doi: 10.3390/cryptography2010001

58. Gambo ML, Almulhem A. Zero trust architecture: a systematic literature review. *J Netw Syst Management* (2026) 34:25. doi: 10.1007/s10922-025-09998-x

59. Fernandez EB, Brazhuk A. A critical analysis of zero trust architecture (zta). *Computer Stand and Inter* (2024) 89:103832. doi: 10.1016/j.csi.2024.103832

60. Walshe T, Simpson AC. Coordinated vulnerability disclosure programme effectiveness: issues and recommendations. *Comput and Security* (2022) 123:102936. doi: 10.1016/j.cose.2022.102936

61. Nowak MA, Tarnita CE, Antal T. Evolutionary dynamics in structured populations. *Philosophical Trans R Soc B: Biol Sci* (2010) 365:19–30. doi: 10.1098/rstb.2009.0215

62. Cimpeanu T, Santos FC, Pereira LM, Lenaerts T, Han TA. Artificial intelligence development races in heterogeneous settings. *Scientific Rep* (2022) 12:1723. doi: 10.1038/s41598-022-05729-3

63. Li A, Cornelius SP, Liu YY, Wang L, Barabási AL. The fundamental advantages of temporal networks. *Science* (2017) 358:1042–6. doi: 10.1126/science.aai7488

64. Guo J, Meng Y, Li A. *Evolutionary Game Dynamics for higher-order Interactions* (2025).*arXiv Preprint arXiv:2501.06411*

65. Bashir A, Shamszaman ZU, Song Z, Han TA. Network reciprocity shapes evolutionary cybersecurity dynamics. *arXiv Preprint arXiv:2607.25568* (2026).

66. Kurahashi S, Chappin E, Jager W, Takahashi H. Editorial: tipping points in societies. *Front Phys* (2023) 11:1227555. doi: 10.3389/fphy.2023.1227555

67. Edwards CM, Nilchiani RR, Ganguly A, Vierlboeck M. Evaluating the tipping point of a complex system: the case of disruptive technology. *Syst Eng* (2025) 28:69–81. doi: 10.1002/sys.21782

68. van Steen T. Developing a behavioural cybersecurity strategy: a five-step approach for organisations. *Computer Stand and Inter* (2025) 92:103939. doi: 10.1016/j.csi.2024.103939

69. Przymus Z, Małagocka K, Przybyszewski K. The human factor in cybersecurity: from risk profiles to resilience. *Proced Computer Sci* (2024) 246:1437–45. doi: 10.1016/j.procs.2024.09.587

70. Maalem Lahcen RA, Caulkins B, Mohapatra R, Kumar M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* (2020) 3:10. doi: 10.1186/s42400-020-00050-w

71. Bishop LM, Asquith PM, Morgan PL. The employee cybersecurity awareness framework. *Hum Behav Emerging Tech* (2025) 2025:1025045. doi: 10.1155/hbe2/1025045

72. Moustafa AA, Bello A, Maurushat A. The role of user behaviour in improving cyber security management. *Front Psychol* (2021) 12:561011. doi: 10.3389/fpsyg.2021.561011

73. Burns A, Posey C, Courtney JF, Roberts TL, Nanayakkara P. Organizational information security as a complex adaptive system: insights from three agent-based models. *Inf Syst Front* (2017) 19:509–24. doi: 10.1007/s10796-015-9608-8

74. Montasari R, Hosseinian-Far A, Hill R. Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. *Cyber Criminology* (2018) 71–93. doi: 10.1007/978-3-319-97181-0_4

75. Malatji M. Augmented intelligence framework for human–artificial intelligence teaming in cybersecurity. *Human-Centric Intell Syst* (2025) 5:151–80. doi: 10.1007/s44230-025-00103-8

76. Cohen D, Te'eni D, Yahav I, Zagalsky A, Schwartz D, Silverman G, et al. Human–ai enhancement of cyber threat intelligence. *Int J Inf Security* (2025) 24:99. doi: 10.1007/s10207-025-01004-4

77. Van Hoang N. Human expertise and machine learning in collaborative intelligence frameworks for robust cybersecurity solutions. *J Appl Cybersecurity Analytics, Intelligence, Decision-Making Syst* (2023) 13:1–12.

78. Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nat Machine Intelligence* (2019) 1:557–60. doi: 10.1038/s42256-019-0109-1

79. Powers ST, Linnyk O, Guckert M, Hannig J, Pitt J, Urquhart N, et al. The stuff we swim in: regulation alone will not lead to justifiable trust in ai. *IEEE Technology Soc Mag* (2024) 42:95–106. doi: 10.1109/mts.2023.3341463

80. Hagen RA, Øverlier L, Helkala K. Human factors in ai-driven cybersecurity: cognitive biases and trust issues. *Digital Threats: Res Pract* (2025) 6:1–20. doi: 10.1145/3759260

81. Dalal A. Cybersecurity and artificial intelligence: how ai is being used in cybersecurity to improve detection and response to cyber threats. *Turkish J Computer Mathematics Education (Turcomat)* (2018) 9:1704–9. doi: 10.61841/turcomat.v9i3.14670

82. Malatji M. A cybersecurity ai agent selection and decision support framework. *arXiv Preprint arXiv:2510.01751* (2025).

83. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge Inf Syst* (2025) 67:6969–7055. doi: 10.1007/s10115-025-02429-y

84. Duan W, Zhou S, Scalia MJ, Yin X, Weng N, Zhang R, et al. Understanding the evolvement of trust over time within human-ai teams. *Proc ACM Human-Computer Interaction* (2024) 8:1–31. doi: 10.1145/3687060

85. Regona M, Yigitcanlar T, Hon C, Teo M. Building trust in artificial intelligence: a systematic review through the lens of trust theory. *ACM Comput Surv* (2026). 1–39. doi: 10.1145/3789256

86. Han TA, Perret C, Powers ST. When to (or not to) trust intelligent machines: insights from an evolutionary game theory analysis of trust in repeated games. *Cogn Syst Res* (2021) 68:111–24. doi: 10.1016/j.cogsys.2021.02.003

87. Andras P, Esterle L, Guckert M, Han TA, Lewis PR, Milanovic K, et al. Trusting intelligent machines: deepening trust within socio-technical systems. *IEEE Technology Soc Mag* (2018) 37:76–83. doi: 10.1109/mts.2018.2876107

88. Akhtar ZB, Rawol AT. Enhancing cybersecurity through ai-powered security mechanisms. *IT Journal Research Development* (2024) 9:50–67. doi: 10.25299/itjrd.2024.16852

89. Shahana A, Hasan R, Farabi SF, Akter J, Al Mahmud MA, Johora FT, et al. Ai-driven cybersecurity: balancing advancements and safeguards. *J Computer Sci Technology Stud* (2024) 6:76–85. doi: 10.32996/jcsts.2024.6.2.9

90. Malatji M, Tolah A. Artificial intelligence (ai) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive ai. *AI and Ethics* (2025) 5:883–910. doi: 10.1007/s43681-024-00427-4

91. Abou El Houda Z. Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape. In: *Cyber Security for Next-Generation Computing Technologies*. Boca Raton, FL: CRC Press (2024). p. 84–101.

92. Agrawal A, Nadeem M, Al Nuaim A, Al Nuaim A. Artificial intelligence driven multi agent framework for adaptive cyber attack simulation and automated incident response in cyber range environments. *Scientific Rep* (2026). doi: 10.1038/s41598-026-45937-9

93. Bashir A, Han TH, Shamszaman ZU. *Many-To-One Adversarial Consensus: Exposing multi-agent Collusion Risks in ai-based Healthcare* (2025). *arXiv preprint arXiv:2512.03097*.

94. Peeters MM, Van Diggelen J, Van Den Bosch K, Bronkhorst A, Neerincx MA, Schraagen JM, et al. Hybrid collective intelligence in a human–ai society. *AI and Society* (2021) 36:217–38. doi: 10.1007/s00146-020-01005-y

95. Gupta P, Nguyen TN, Gonzalez C, Woolley AW. Fostering collective intelligence in human–ai collaboration: laying the groundwork for cohumain. *Top Cognitive Science* (2025) 17:189–216. doi: 10.1111/tops.12679

96. Akinwalere S, Chang K. The symbiotic roles of artificial intelligence and human intelligence in advancing knowledge ecosystem. *J Knowledge Management* (2026) 1–42. doi: 10.1108/jkm-03-2025-0362

97. Fielder A, Panaousis E, Malacaria P, Hankin C, Smeraldi F. Decision support approaches for cyber security investment. *Decis Support Systems* (2016) 86:13–23. doi: 10.1016/j.dss.2016.02.012

98. Chronopoulos M, Panaousis E, Grossklags J. An options approach to cybersecurity investment. *IEEE Access* (2017) 6:12175–86. doi: 10.1109/access.2017.2773366

99. Jeong S, Rogers Z, Choi TY. Strange dance partners: supply chain cyberattacks and chained vulnerability. *J Operations Management* (2025) 71:763–85. doi: 10.1002/joom.1374

100. Simon J, Omar A. Cybersecurity investments in the supply chain: coordination and a strategic attacker. *Eur J Oper Res* (2020) 282:161–71. doi: 10.1016/j.ejor.2019.09.017

101. Tsohou A, Diamantopoulou V, Gritzalis S, Lambrinoudakis C. Cyber insurance: state of the art, trends and future directions. *Int J Inf Security* (2023) 22:737–48. doi: 10.1007/s10207-023-00660-8

102. Palsson K, Gudmundsson S, Shetty S. Analysis of the impact of cyber events for cyber insurance. *The Geneva Pap Risk Insurance-Issues Pract* (2020) 45:564–79. doi: 10.1057/s41288-020-00171-w

103. Marotta A, Madnick S. Analyzing and categorizing emerging cybersecurity regulations. *ACM Comput Surv* (2025) 58:1–36. doi: 10.1145/3757318