Civil Engineering Research Journal
ISSN: 2575-8950

Juniper Publishers
key to the Researchers

Review Article
Volume 15 Issue 4 - August 2026
DOI: 10.19080/CERJ.2026.14.555925

Civil Eng Res J

Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance

Chunlin Liu*

K&C Protective Technologies Pte Ltd /AIS Communications Pte Ltd, Singapore

Submission: August 19, 2026; **Published:** August 28, 2026

***Corresponding author:** Chunlin Liu, K&C Protective Technologies Pte Ltd /AIS Communications Pte Ltd, Singapore

Abstract

Cybersecurity has traditionally focused on protecting systems, networks and information assets. However, contemporary digital threats increasingly emerge from the interaction of technology with human emotion, behaviour, social influence and online environments. This paper extends the Security & Happiness by Design (SHBD) paradigm and its Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS) from the physical environment into cyberspace. It proposes a human-centric digital governance framework in which security is designed not only to prevent, detect and respond to malicious activity, but also to strengthen trust, psychological safety, constructive connection and social resilience. The established CONNECT–SENSE–RESPONSE trinity is reinterpreted as a continuous digital governance cycle: CONNECT establishes trusted participation, positive human connection and contextual understanding; SENSE combines affective computing, behavioural analytics, social sensing and human reporting to identify meaningful trajectories of risk; and RESPONSE enables proportionate interventions ranging from supportive engagement to formal security action and rehabilitation. The framework is illustrated through three unrelated cases of self-radicalised Singaporean youths reported by Singapore's Internal Security Department in July 2026, demonstrating how cyberspace may function as an incubator, amplifier and operational enabler of physical-world threats. The paper argues that SHBD can complement conventional cybersecurity and online-safety controls by shifting intervention upstream, from responding to manifested harm towards identifying and disrupting harmful trajectories before they mature. Such an approach, however, requires privacy by design, fairness, proportionality, contextual validity and accountable human oversight to ensure that behavioural intelligence supports human security without becoming pervasive surveillance.

Keywords: Security & Happiness by Design; SHBD; HIBLISS; Affective Computing; Human-Centred Cybersecurity; Online Safety; Digital Governance; Behavioural Intelligence; Online Radicalisation; CONNECT-SENSE-RESPONSE

Introduction

The digital environment is no longer isolated from the physical world. It has become a social environment in which people learn, work, form identities, seek belonging and experience conflict. Consequently, security incidents in cyberspace increasingly emerge from interactions among technology, information, emotion, behaviour and social relationships. Traditional cybersecurity remains essential for protecting confidentiality, integrity and availability, but these objectives alone do not fully address harms such as cyberbullying, online harassment, scams, manipulation, hate speech, extremist recruitment and the escalation of online grievances into offline violence.

K&C Protective Technologies Pte Ltd has been implementing the concept of Security & Happiness by Design (SHBD) since 2008. This concept was first developed by founder Chunlin LIU on September 11, 2008, drawing on his experience working with and engaging various stakeholders through the years. The concept aimed to integrate security, human behaviour, and environmental considerations into the design of protective systems. The concept was subsequently published in the Civil Engineering Research Journal in 2021 as Security & Happiness by Design for Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS) [1]. HIBLISS proposed that security should move beyond an exclusively preventive and resistance-oriented approach by creating environments that encourage positive human behaviour, enhance well-being, and strengthen resilience. Its operational philosophy is expressed through three core functions: CONNECT, SENSE, and RESPONSE [1].

The original SHBD concept was developed primarily within the physical and built environment, integrating environmental design with sensors, video analytics, artificial intelligence, robotics

and smart infrastructure. This reflected both the protective-security origins of SHBD and the technological environment in which the concept emerged. Since then, cyberspace has assumed an increasingly consequential role in shaping human behaviour, relationships, identity formation and security risk.

The COVID-19 pandemic accelerated this transition. Lockdowns, remote working and increased dependence on social media and digital communication demonstrated that security and well-being in digital environments are closely interconnected. Misinformation, online hostility, social isolation, scams and other digital harms further demonstrated that vulnerabilities may arise not only from technological weaknesses but also from interactions among emotion, behaviour, information and social influence. Concurrent advances in artificial intelligence, affective computing and behavioural analytics have created new possibilities for understanding and responding to these human-centred risks.

Despite growing interest in human-centred cybersecurity, online safety and affective computing, a gap remains between technical cybersecurity controls and frameworks that systematically integrate human connection, affective and behavioural sensing, proportionate intervention and recovery within a unified security-by-design architecture. This paper addresses that gap by extending SHBD and HIBLISS into cyberspace.

The paper makes three principal contributions. First, it extends SHBD from physical protective environments to digital environments. Second, it operationalises CONNECT–SENSE–RESPONSE as a continuous human-centric digital governance cycle incorporating affective, behavioural and contextual intelligence. Third, it proposes a layered governance architecture that integrates technological sensing with human judgement, proportionality, privacy safeguards, intervention and rehabilitation.

This paper therefore extends Security & Happiness by Design from the physical environment into cyberspace. The fundamental SHBD philosophy remains unchanged, but the environment now includes digital platforms, networks, content, online communities, algorithms and human-computer interactions. Applying CONNECT–SENSE–RESPONSE to this environment provides a framework for recognising harmful behavioural trajectories earlier and enabling supportive and proportionate interventions. Consistent with the development of human-centred cybersecurity [2], SHBD in cyberspace seeks not to create pervasive emotional surveillance, but to design digital environments in which security, trust, well-being and resilience reinforce one another.

From Security by Design to Security & Happiness by Design in Cyberspace

Security by Design generally seeks to incorporate protection into a system from the outset rather than adding controls after construction. In cyberspace, this principle is commonly implemented through authentication, access control, encryption, secure coding, network segmentation, monitoring and incident response. These controls are important, but they are predominantly concerned with the technical aspects of the system. SHBD introduces a second design question: what psychological and behavioural conditions are being created for the people who inhabit the system?

A digital environment may be technically secure while still producing frustration, distrust, isolation or hostility. Conversely, a platform designed only for engagement and convenience may unintentionally reward outrage, polarisation or repeated exposure to harmful material. Security & Happiness by Design therefore treats digital well-being, trust, dignity and social resilience as security-relevant design outcomes. In this paper, 'happiness' is not used to mean continuous positive emotion. It refers more broadly to a condition in which users can participate with reasonable confidence, psychological safety and social connection, while harmful behaviour is discouraged and legitimate security intervention remains available.

This framing preserves the central idea of HIBLISS: security can be strengthened not only by resisting threats at the point of attack, but also by shaping the environment so that the manifestation of harmful behaviour is reduced earlier in the attack pathway [1] (Figure 1). In cyberspace, that pathway may include exposure to harmful narratives, emotional reinforcement, entry into closed communities, repeated consumption of violent material, identity crisis, acquisition of attack knowledge, financing terrorism, and finally operational preparation. Not every user who displays anger, distress or controversial beliefs presents a security risk. The design challenge is therefore to combine behavioural and affective indicators with context, escalation patterns and human judgement rather than relying on simplistic emotion labels.

Hence, progression is neither inevitable nor necessarily linear. Individuals may disengage, regress or enter the trajectory at different points.

Affective Computing as an Enabling Capability

Within SHBD, affective computing is therefore an enabling capability rather than the decision-making authority.

Affective computing refers to computational methods that recognise, interpret or respond to human affections. Contemporary approaches may analyse text, speech, facial expression, interaction patterns and other contextual signals. Research has demonstrated that emotion analysis can move beyond a simple positive-versus-negative sentiment classification. For example, multidimensional systems have differentiated fear, anger, sadness, happiness and overall emotional valence in social-media text [3,4]. Large-scale studies of public discourse during COVID-19 further showed that changes in emotional expression can be tracked over time and related to changing events and concerns [5].

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

Figure 1: Cyber-to-Physical Harm Trajectory.

Such capabilities are relevant to SHBD because emotions often influence attention, interpretation, decision-making and social behaviour. Emotion-aware analysis may help distinguish, for example, fear from anger, or vulnerability from hostility, enabling different forms of response. Recent research also shows the value of examining more complex emotional patterns in online harms such as cyberbullying [6], while multimodal emotion-recognition studies indicate that combining modalities can improve recognition but that performance varies by context [7]. These findings support a central SHBD principle: sensing should be contextual and adaptive rather than binary.

At the same time, affective computing introduces serious ethical and technical risks. Emotion inference is probabilistic, culturally and contextually dependent, and vulnerable to bias. Researchers have therefore called for explicit risk assessment, limitations on high-stakes use, data minimisation, transparency and careful consideration of misuse [8,9]. SHBD in cyberspace must consequently reject the idea of an omniscient 'emotion surveillance' system. Its purpose should be to create better opportunities for early support and proportionate security intervention, with humans retaining responsibility for consequential decisions.

Operational Framework: CONNECT-SENSE-RESPONSE for Cyberspace

The original HIBLISS framework identifies CONNECT, SENSE and RESPONSE as the trinity through which Behavioural Lead Intelligence is generated [1]. For cyberspace, these domains can be operationalised as a continuous governance cycle rather than a linear technical pipeline (Figure 2).

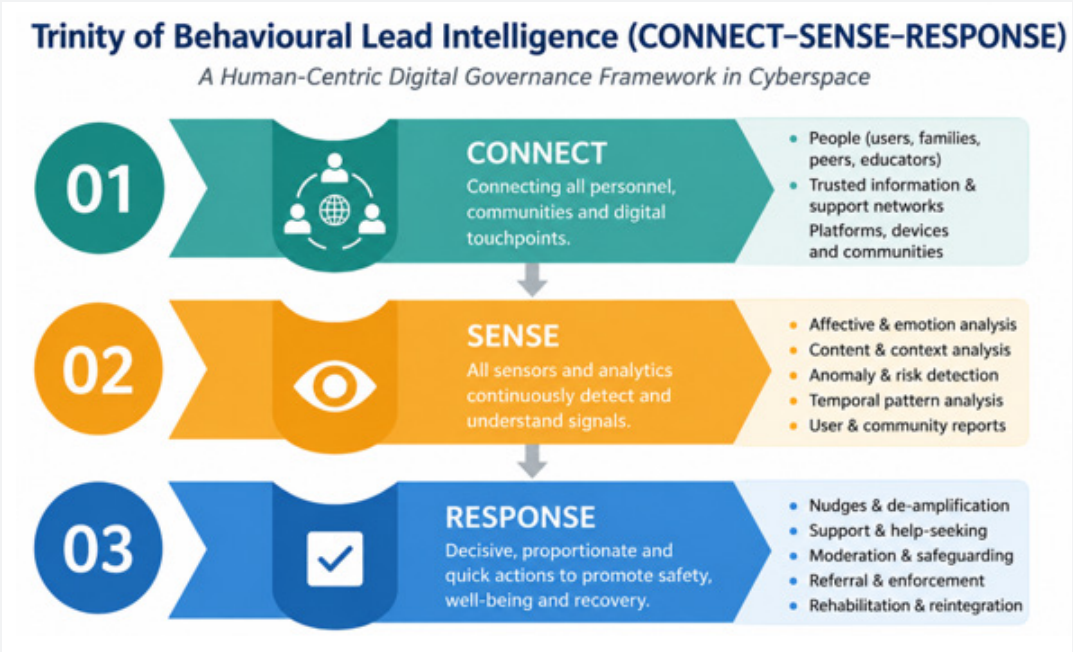

Figure 2: Trinity of Behavioral Lead Intelligence.

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

CONNECT

CONNECT concerns the quality, context and safety of digital participation. In the physical HIBLISS model, connectivity allows individuals to obtain information, maintain contact and interact smoothly with their environment. In cyberspace, CONNECT includes access to trustworthy information, healthy communities, credible support networks, digital literacy resources and channels for seeking help. It also includes the contextual links needed to understand behaviour: what content is being consumed, how interaction patterns are changing, whether a user is moving into increasingly closed or extremist spaces, and whether online activity is becoming disconnected from constructive family, school or community relationships.

CONNECT should therefore be designed in two directions. The first is protective connection: making credible information, counselling, community support and pro-social participation easy to find. The second is contextual connection: integrating signals across content, behaviour and reporting channels so that isolated indicators are not interpreted without context. Privacy-preserving design, purpose limitation and clear governance are essential at this stage.

SENSE

SENSE is the detection and analytical layer. It seeks to identify meaningful changes in affect, behaviour and interaction before harm is fully manifested. Potential indicators include sustained increases in hostility or fear, fascination with violence, repeated engagement with extremist propaganda, glorification of attackers, explicit dehumanisation, abrupt changes in online communities, attempts to recruit others, searches associated with attack preparation, or the convergence of grievance, violent intent and operational research. Affective computing can enrich this layer by distinguishing emotional trajectories rather than treating all negative expressions as equivalent.

Risk significance increases not because a single indicator becomes more intense, but because multiple independent indicators begin to converge across affect, behaviour, content, persistence, capability and intent (Table 1).

Table 1: Matrix of Indicators and Concerns.

Indicator 1	Indicator 2	Indicator 3	Indicator 4	Indication 5	Concerns
Emotion alone					Low evidential significance
Emotion	+ behavioural change				Contextual concern
Emotion	+ behavioural change	+ violent content persistence			Elevated concern
Emotion	+ behavioural change	+ violent content persistence	+ capability acquisition		Serious concern
Emotion	+ behavioural change	+ violent content persistence	+ capability acquisition	+ Target/Intent/Preparation	Intervention threshold

The purpose is not to simply infer threats and risks from emotion. Anger, sadness and fear are normal human experiences. SENSE becomes security-relevant only when affective signals are interpreted alongside behaviour, content, persistence, escalation and credible contextual indicators. A SHBD system should therefore favour multi-factor thresholds, temporal patterns and human review. It should also measure positive signals such as re-engagement, reduction of hostility, help-seeking and restoration of social connection, because the objective is not merely threat detection but movement toward a safer and healthier state.

RESPONSE

RESPONSE translates intelligence into proportionate action. Responses can range from low-friction digital interventions to formal security action. At an early stage, the platform may offer contextual information, counter-narratives, digital-literacy prompts, supportive resources, or opportunities to connect with trusted people. At a higher level of concern, trained moderators, counsellors, educators, community partners or guardians may be engaged. Where there are credible indicators of violence or criminal conduct, escalation to competent authorities may be necessary. The response must be calibrated to the level of risk, because an overly punitive intervention may deepen alienation and distrust while an insufficient response may allow harm to progress or materialize (Table 2).

Table 2: SHBD Response Ladder.

Level of Risk	Actions
Level 1 – Enable	Trusted information and positive connection
Level 2 – Nudge	Digital friction, prompts and counter information
Level 3 – Support	Trusted adult, educator, counsellor or community intervention
Level 4 – Assess	Human multidisciplinary review
Level 5 – Protect	Formal safeguarding and security intervention where credible risk exists

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

This reflects the original HIBLISS emphasis on combining technology with people, processes and procedures [1]. In cyberspace, the equivalent is a Human-Centred Digital Response Framework: defined escalation thresholds, trained reviewers, multidisciplinary case assessment, auditable decisions, appeal mechanisms where appropriate, and pathways for rehabilitation and reintegration.

Illustrative Application: Cyber-to-Physical Threat Trajectories in Three Singapore Self-Radicalisation Cases

On 27 July 2026, Singapore's Internal Security Department (ISD) announced that three unrelated male Singaporean youths, aged 15, 19 and 14, had been issued Orders of Detention under the Internal Security Act in April, May and June 2026 respectively. ISD stated that all three had been self-radicalised online by violent extremist ideologies and had made preparations to conduct attacks in Singapore [10]. These cases provide a contemporary illustration of why cyberspace must be treated as part of the security environment rather than only as a communications medium.

The 15-year-old's radicalisation developed through extensive exposure to online content relating to the Israeli-Palestinian conflict and violent extremist material. He expressed support for terrorist and militant groups, created online chat groups, disseminated pro-ISIS content, researched homemade explosives, searched for travel to Syria and overseas shooting ranges, and progressed toward plans for violence [10]. The 19-year-old, Tan Jun Jie, became a staunch ISIS supporter, planned knife attacks against SAF personnel and LGBTQ students, researched knife skills and a weapon, and had also attempted DDoS cyberattacks against websites of Muslim organisations he regarded as deviant [10]. The 14-year-old was radicalised by Composite Violent Extremism (CoVE), combining elements of ISIS support, far-right ideology and fascination with mass shooters. He prepared for a mass-casualty stabbing attack at his school, repeatedly consumed violent material, researched weapons and bomb-making, and drafted a 21-page manifesto [10].

ISD highlighted three characteristics particularly relevant to SHBD in cyberspace. First, repeated exposure to violent and extremist material can normalise violence and increase receptivity to narratives that legitimise violence. Second, the internet provides operational knowledge that can support attack planning. Third, the cyber dimension is expanding: the 19-year-old's attempted DDoS attacks represented the first self-radicalised individual dealt with under the ISA who had attempted cyberattacks in furtherance of radical beliefs [10]. The Ministry of Home Affairs separately acted on 27 July 2026 to disable or block access to online terrorism-related content, stating that investigations had established a direct nexus between such content and past self-radicalisation cases in Singapore [11].

Applying CONNECT-SENSE-RESPONSE to the Three Cases

Table 3: Adoption of SHBD to the 3 Cases.

Case	CONNECT	SENSE	RESPONSE
15-year-old	Map the pathway between mainstream social media, online religious groups, extremist content, chat groups, family/school support and credible counter-narratives. Strengthen access to trusted religious and civic guidance before extremist communities become the dominant source of meaning.	Detect sustained escalation from grievance-related content to support for violence, pro-ISIS dissemination, recruitment activity, bomb-making research, travel/shooting-range searches and attack-oriented intent. Affective signals such as anger or perceived injustice are contextual indicators, not stand-alone risk labels.	Use graduated interventions: platform friction and counter-messaging at early stages; trusted-adult/community engagement when persistent extremist identification emerges; rapid human review and referral to authorities when violent intent, recruitment or operational preparation becomes credible.
19-year-old	Identify the transition from online religious learning to extremist preachers, pro-ISIS material, closed ideological reinforcement and acquisition of cyber/physical attack knowledge. Preserve constructive connections with credible religious teachers, peers and institutions.	Sense convergence of ideological rigidity, dehumanisation of out-groups, violent ideation, weapon research, attack-target selection and attempted DDoS activity. Cross-domain indicators are important because cyber aggression and physical violence may reflect the same underlying extremist trajectory.	Combine cyber incident handling with behavioural risk assessment. Early response may include credible theological correction and psychosocial support; explicit attack planning or cyber offences require formal investigation and security intervention, followed by rehabilitation.
14-year-old	Recognise the fragmented online ecosystem of CoVE: extremist propaganda, mass-shooter culture, violent games/gore, grievance communities and social-media identity performance. Strengthen school, family and peer reporting channels and safe opportunities for belonging.	Look for multi-ideology escalation rather than a single ideological signature: repeated violent-content consumption, fascination with mass shooters, weapon/bomb research, manifesto production, target selection, rehearsal/simulation and stated willingness to act. CoVE requires pattern-based sensing because beliefs may be contradictory and fluid.	Prioritise early school/community reporting, multidisciplinary assessment and rapid escalation where planning becomes operational. Rehabilitation should address ideology together with grievances, psychological vulnerabilities, social connection and future reintegration.

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

These cases are used illustratively rather than as empirical validation of SHBD. The retrospective analysis does not imply that implementation of SHBD would necessarily have predicted or prevented the cases. Instead, it demonstrates how CONNECT–SENSE–RESPONSE may provide a structured framework for interpreting escalating cyber-to-physical risk trajectories and identifying possible points of intervention (Table 3).

The table illustrates that CONNECT-SENSE-RESPONSE is not a proposal for automated detention or predictive policing. It is a design framework for organising prevention, early detection, support, escalation and recovery. The three cases also show why the framework must extend beyond platform moderation. Family members, friends, schools and community institutions are part of CONNECT; changes in behaviour and expressed intent contribute to SENSE; and reporting, counselling, moderation, law enforcement and rehabilitation form different levels of RESPONSE. ISD specifically emphasised the importance of early reporting and noted that the youths would undergo holistic rehabilitation addressing ideological misconceptions together with psychological and social vulnerabilities [10].

The case study also demonstrates the importance of designing for personalised radicalisation. MHA has observed that CoVE may combine Islamist extremism, far-right extremism, and grievance-fuelled narratives, and that the absence of a coherent ideology can make detection more difficult [12]. A human-centric system therefore cannot rely solely on static keyword lists in a single ideological category. It must focus on trajectories of harm: escalating grievance, normalisation of violence, social reinforcement, target identification, acquisition of capability and movement toward action.

A Human-Centric Digital Governance Architecture

Based on the preceding analysis, SHBD in cyberspace can be represented as a layered governance architecture (Figure 3). The first layer is the Digital Environment Layer: platform design, recommendation systems, community structures, access controls and user interfaces. The second is the Human Connection Layer: trusted information, family, peers, educators, community organisations and support resources. The third is the Affective and Behavioural Sensing Layer: multimodal emotion analysis, content analysis, anomaly detection, temporal pattern analysis and user/community reports. The fourth is the Human Judgement and Governance Layer: trained reviewers, risk assessment, legal and ethical checks, and multidisciplinary case management. The fifth is the Proportionate Response Layer: nudges, de-amplification, support, moderation, safeguarding, referral, enforcement and rehabilitation. Across all layers, privacy, transparency, accountability and security controls must operate as cross-cutting requirements.

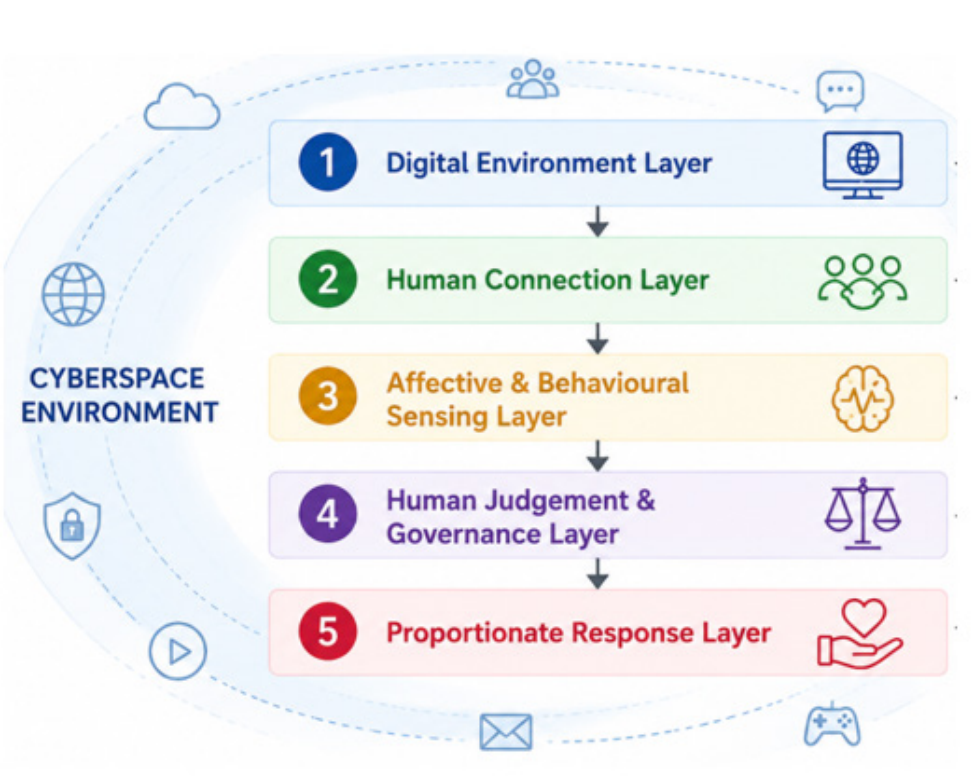

Figure 3: Five-layer Human-Centric Digital Governance.

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

The architecture differs from conventional 'detect-and-block' models in two ways. First, it explicitly values positive outcomes such as trust, agency, social connection and recovery. Second, it treats response as a spectrum. Binary account removal may be necessary for certain content or actors, but it should not be the only design instrument. In many cases, the most effective upstream intervention may be a credible human connection, a timely challenge to misinformation, an opportunity to seek help, or the interruption of an algorithmic pathway that repeatedly amplifies violent material.

Design Principles and Safeguards

Human well-being is a security objective. Security decisions should consider not only technical containment but also their effects on trust, dignity, psychological safety and social cohesion.

Emotion is a signal, not a verdict. No adverse decision should be based solely on inferred emotion. Emotion analytics should be combined with behavioural, contextual and temporal evidence.

Intervene at the lowest effective level. Use the least intrusive response capable of reducing risk, while escalating rapidly when credible violence or criminal conduct is present.

Design for positive connection. Platforms should make trusted information, constructive communities and help-seeking pathways easier to reach, especially when users show signs of vulnerability, isolation or radicalisation.

Require human oversight for high-impact decisions. Automated systems may prioritise or flag cases, but consequential security actions should require accountable human assessment.

Protect privacy by design. Collect only data necessary for defined purposes, apply retention limits, sensitize privacy information, access controls and audit trails, and avoid secondary use of emotional data without legitimate justification.

Test for bias and contextual validity. Affective and behavioural models should be evaluated across languages, cultures, age groups and communication styles, with documented limitations.

Measure recovery as well as detection. Success should include reduced hostility, restored connection, successful rehabilitation and safer participation, not only the number of accounts blocked or alerts generated.

Behaviour is not identity. Risk assessment should focus on observable trajectories, context and credible indicators rather than permanently categorising individuals according to inferred beliefs, emotions or identities.

Safety without pervasive surveillance. SHBD should seek sufficient situational awareness to enable proportionate intervention while avoiding indiscriminate collection, continuous emotional monitoring or secondary use of behavioural data beyond legitimate and defined purposes.

Discussion

The three Singapore cases underline a fundamental cyber-physical reality: online harms can develop into offline security threats. In each case, cyberspace contributed more than ideological exposure. It provided social reinforcement, identity formation, violent exemplars, technical knowledge and opportunities for rehearsal or dissemination. This makes online safety relevant to protective security, education, community resilience and national security simultaneously.

SHBD provides a useful conceptual bridge because it does not separate security from the human condition that produces or mitigates risk. The framework asks not only how to stop a harmful act, but how the environment can reduce the probability that the harmful trajectory matures. Affective computing is potentially valuable in this role because it can help systems recognise changes in emotional expression and distinguish different forms of negative affect. However, the scientific and ethical limitations of emotion recognition require caution. Emotion cannot be reliably reduced to a facial expression, a word or a score in all contexts, and models may perform differently across populations and settings [8,9].

For this reason, the strongest application of affective computing within SHBD may be at the aggregate, assistive and triage levels rather than as an autonomous decision-maker. Aggregate social sensing can reveal emerging patterns of fear, anger or hostility; assistive tools can help human reviewers understand context; and triage systems can prioritise cases where affective change coincides with behavioural escalation. This is consistent with research showing that emotion-level analysis can provide actionable distinctions in public communication and online interaction [3-7].

Future empirical research should test the framework in specific digital environments. Possible studies include longitudinal analysis of escalation patterns in online communities; evaluation of whether supportive interventions reduce harmful engagement; controlled testing of different forms of digital friction; measurement of trust and perceived fairness after security interventions; and comparative evaluation of human-only, algorithm-only and human-in-the-loop approaches. Research should also examine whether CONNECT variables - such as access to trusted communities and help-seeking pathways - can serve as protective factors that reduce progression from grievance to violent intent.

Four key research propositions would be recommended as follows:

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

a. Proposition 1: Stronger protective CONNECT factors are associated with reduced progression along harmful digital trajectories.

b. Proposition 2: Multi-factor behavioural and affective convergence provides more useful risk triage than single-signal emotion classification.

c. Proposition 3: Graduated human-centred interventions produce greater perceived fairness and trust than binary enforcement-only interventions.

d. Proposition 4: Human-in-the-loop SHBD models provide better contextual validity than algorithm-only approaches.

Conclusion

Security & Happiness by Design in Cyberspace extends the HIBLISS philosophy from smart physical environments into the digital spaces where human relationships, identities and security risks increasingly develop. The proposed model retains the original CONNECT-SENSE-RESPONSE logic but reinterprets it for human-centric digital governance. CONNECT creates safe participation, trusted relationships and contextual understanding. SENSE combines affective computing, behavioural analytics and human reporting to identify meaningful trajectories of risk. RESPONSE provides a graduated pathway from supportive intervention to formal security action and rehabilitation.

The July 2026 detention of three self-radicalised youths in Singapore demonstrates the urgency of this approach. Their cases show how online exposure and interaction can progress into recruitment, cyberattack attempts, weapon research, attack planning and intended physical violence [10]. Conventional cybersecurity remains necessary, but it is not sufficient for threats that emerge through human emotion, social influence and behaviour. A more complete security architecture must protect systems and people together.

SHBD should therefore not be understood as a call for pervasive emotional surveillance or predictive policing. It proposes a different security philosophy: situational awareness without universal surveillance, behavioural understanding without deterministic profiling, and early intervention without automated punishment.

The future of cybersecurity cannot be secured by protecting machines while neglecting the human environments in which threats emerge. Security & Happiness by Design consequently extends the security-by-design principle from securing systems alone towards designing digital environments in which security, trust, human well-being and resilience become mutually reinforcing conditions. In doing so, the objective shifts from responding only after harm has materialised towards shaping cyberspace so that harmful trajectories are less likely to mature in the first place.

References

1. Liu C (2021) Security & Happiness by Design for Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS). Civil Engineering Research Journal 12(2): 555832.
2. National Institute of Standards and Technology (NIST) (2026) Human-Centered Cybersecurity. Computer Security Resource Center, U.S. Department of Commerce.
3. A*STAR Institute of High Performance Computing (2021) CrystalFeel and multidimensional emotion analytics: fear, anger, happiness, sadness and emotional valence. A*STAR research/publicity materials.
4. Gupta RK, Vishwanath A, Yang Y (2020) COVID-19 Twitter Dataset with Latent Topics, Sentiments and Emotions Attributes. arXiv:2007.06954.
5. Lwin MO, Lu J, Sheldenkar A, Schulz PJ, Shin W, Gupta R, Yang Y (2020) Global Sentiments Surrounding the COVID-19 Pandemic on Twitter: Analysis of Twitter Trends. JMIR Public Health and Surveillance 6(2): e19447.
6. Zhong J, Mo Y, Zhang J, Liu P, Luo X, Ding R, et al. (2025) Beyond anger: uncovering complex emotional patterns between cyberbullying roles through affective computing and epistemic network analysis. Humanities and Social Sciences Communications 12: 1281.
7. Bhattacharya P, Gupta RK, Yang Y (2020) Exploring the contextual factors affecting multimodal emotion recognition in videos. arXiv:2004.13274.
8. Hernandez J, Lovejoy J, McDuff D, Suh J, O'Brien T, Sethumadhavan A, Greene G, Picard R, Czerwinski M (2021) Guidelines for Assessing and Minimizing Risks of Emotion Recognition Applications. International Conference on Affective Computing & Intelligent Interaction (ACII).
9. Mohammad SM (2021) Ethics Sheet for Automatic Emotion Recognition and Sentiment Analysis. arXiv:2109.08256.
10. Internal Security Department, Singapore (2026) Issuance of Orders of Detention under the Internal Security Act (ISA) against three self-radicalised Singaporean youths.
11. Ministry of Home Affairs, Singapore (2026) Issuance of directions under the Online Criminal Harms Act against online entities disseminating terrorism-related content.
12. Ministry of Home Affairs, Singapore (2026) Assessing emergence of composite violent extremism and other personalised forms of online radicalisation. Written Reply to Parliamentary Question.

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925

DOI: 10.19080/CERJ.202.15.555925

How to cite this article: Chunlin L. Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Eng Res J. 2026; 15(5): 555925. DOI:10.19080/CERJ.202.15.555925