Civil Engineering Research Journal
ISSN: 2575-8950

Juniper Publishers
key to the Researchers

Review Article
Volume 16 Issue 1 - September 2026
DOI: 10.19080/CERJ.2026.16.555926

Civil Eng Res J

Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE

Chunlin Liu*

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

Submission: September 06, 2026; **Published:** September 11, 2026

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

Abstract

Security & Happiness by Design (SHBD) proposes that security should not be treated only as resistance against threats, but as an environmental and human-centred design problem in which security, trust, well-being and resilience can reinforce one another. The Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS) operationalises this philosophy through the trinity of CONNECT, SENSE and RESPONSE. This paper develops the algorithmic logic of that trinity while retaining its original closed-loop structure and builds explicitly on two bodies of work: the extension of SHBD into cyberspace and the comparison of Security by Design (SbD) and Privacy by Design (PbD) in Shielding Software Systems. The latter is especially relevant because its discussion of techno-regulation shows that technological design can encode behavioural possibilities and constraints. HIBLISS takes this design logic further: rather than relying only on fixed prevention, it creates an adaptive cycle in which the environment is connected, meaningful behavioural and affective changes are sensed and interpreted, and proportionate responses are selected according to context. CONNECT establishes the data, contextual and protective relationships needed to understand the environment. SENSE transforms multi-modal information into behavioural and contextual intelligence through feature fusion, affective and behavioural analysis, trajectory assessment and human interpretation. RESPONSE translates that intelligence into proportionate interventions and feeds the resulting outcomes back into the system for adaptation. The resulting architecture is not an autonomous decision-maker, but a human-centred adaptive security-governance loop constrained by privacy, fairness, proportionality and accountable human oversight.

Keywords: Security & Happiness by Design; SHBD; HIBLISS; CONNECT-SENSE-RESPONSE; Security by Design; Privacy by Design; Techno-regulation; Affective Computing; Behavioural Intelligence; Human-Centred Security

Introduction

To bridge the gap between abstract human psychology and functional engineering, the Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS) operationalises the Security & Happiness by Design (SHBD) methodology through three interdependent phases: CONNECT, SENSE and RESPONSE. Together, they form a continuous closed-loop system in which information about people, technology and environment is acquired, interpreted and translated into proportionate action, with the effects of that action returned to the system as new information.

The original SHBD concept was developed in the physical and built environment and subsequently extended into cyberspace. The cyberspace formulation retains the original CONNECT-SENSE-RESPONSE logic but broadens it into a human-centric governance cycle. CONNECT establishes trusted participation, positive human connection and contextual understanding; SENSE combines affective computing, behavioural analytics, social sensing and human reporting; and RESPONSE provides graduated intervention ranging from supportive engagement to formal security action and rehabilitation [1,2].

This development is consistent with the broader principle of Security by Design (SbD), which seeks to incorporate security from the outset rather than adding protection after a system has been developed. Del-Real, De Busser and van den Berg [3], in their systematic comparison of SbD and Privacy by Design (PbD), observe that software design has a central role in preventing cybersecurity harm and that SbD would benefit from a more interdisciplinary and human-centred foundation.

The comparison with PbD is also significant. Del-Real et al. [3] found that PbD is more strongly anchored in recognised rights and an interdisciplinary perspective, while SbD definitions are less uniform and more often centred on the technical product.

They argue that both approaches should protect individuals and organisations, be implemented early in the development process, and take account of broader human and organisational concerns. HIBLISS builds on this design orientation by treating human behaviour, affect, trust and well-being not as external matters surrounding a security system, but as conditions that can influence security outcomes and should therefore be considered within the design logic itself.

Within SHBD, happiness should not be understood simply as positive emotion or pleasure. Rather, it represents protective human conditions such as psychological safety, dignity, trust, agency, constructive social connection and resilience. Happiness is therefore treated as a human-centred security condition rather than an emotional score to be maximized.

Of particular relevance is the discussion of techno-regulation in Shielding Software Systems. Del-Real et al. [3] write: "An alternative approach, summarized under the heading of techno-regulation, seeks to solve this issue by taking things in a different direction: it aims to code (im)possibilities into technological systems, so that end users can no longer intentionally or accidentally engage in insecure or unsafe behaviour." This observation is central to the argument developed in this paper. It shows that security can be produced not only by instructing users or detecting violations, but by designing the technological environment itself so that particular actions are enabled, discouraged, constrained or prevented.

HIBLISS builds on this insight but does not reduce human-centred security to technological prohibition. Its distinctive proposition is that the environment can be designed as an adaptive behavioural interface. CONNECT establishes the relationship between people, systems and context; SENSE identifies meaningful changes and convergence among signals; and RESPONSE modifies the environment or initiates human intervention at a level proportionate to the assessed concern. In this sense, techno-regulation supplies an important design premise for HIBLISS, while CONNECT-SENSE-RESPONSE extends that premise from static coded constraint towards continuous adaptive regulation and support.

The purpose of this paper is therefore not to replace the original HIBLISS structure, but to develop its algorithmic logic. The organising architecture remains CONNECT-SENSE-RESPONSE, with governance and human judgement operating across the cycle.

The contribution of this paper lies in making explicit the computational and governance logic implicit within the original HIBLISS trinity. It conceptualizes HIBLISS as an adaptive closed-loop architecture in which CONNECT establishes contextual and protective relationships, SENSE identifies meaningful convergence across multimodal indicators, and RESPONSE selects the least intrusive effective intervention before returning observed outcomes to the next cycle through adaptive tuning.

As we remember the lives lost on 11 September 2001, the tragedy remains a solemn reminder that security and vigilance can never be taken for granted. More than two decades on, the threat landscape continues to evolve, becoming increasingly complex and sophisticated. In today's highly digitalized and interconnected world, threats are no longer confined to physical infrastructure. Disruption to digital infrastructure can equally affect essential services, economies and communities, with significant consequences for human lives. The lessons of 9/11 therefore remain relevant today. We must continue to stay vigilant, anticipate emerging threats and strengthen our resilience across both the physical and digital environments on which society increasingly depends.

The HIBLISS Closed-Loop Algorithmic Architecture

The HIBLISS trinity should be understood as a feedback system rather than three independent modules. The basic operational sequence is as follows:

Figure 1 shows the algorithmic architecture of HIBLISS. CONNECT performs data acquisition and produces multi-modal input data for SENSE. SENSE identifies potentially significant or anomalous patterns and passes them through the Feature Fusion Layer. RESPONSE acts on the fused interpretation through ambient or other proportionate feedback. The effects of RESPONSE then return through Adaptive Tuning to CONNECT, changing the conditions for the next acquisition cycle. This feedback path is fundamental: HIBLISS is not a linear detect-and-react sequence, but a continuously recalibrating closed loop.

Figure 2 provides the expanded human-centric interpretation used in this paper. Environment, interpretation and behavioural adaptation make explicit what is already implicit in the original closed loop: CONNECT operates within an environment, SENSE requires contextual interpretation, and RESPONSE is evaluated by the behavioural and environmental state that follows. Figure 2 therefore expands Figure 1; it does not replace it.

In computational terms, CONNECT provides inputs and establishes context; SENSE extracts and fuses features and estimates the significance of changing patterns; INTERPRETATION places those patterns within operational, social and human context; RESPONSE selects the lowest effective intervention; and BEHAVIOURAL ADAPTATION produces a changed state that becomes the next input to CONNECT. The system therefore repeatedly asks: What is happening? What does it mean? What should be done? Did it work? What is happening now?

Viewed through the lens of techno-regulation, each HIBLISS phase performs a different design function. CONNECT determines what relationships, information and protective pathways are made

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

available; SENSE determines how changes in those conditions are interpreted; and RESPONSE determines how the environment changes what becomes easier, harder, supported, delayed, restricted or escalated. The closed loop therefore operationalises the proposition that security architecture can influence behaviour, while avoiding the assumption that every human-centred security problem can be solved through a fixed allow/deny rule.

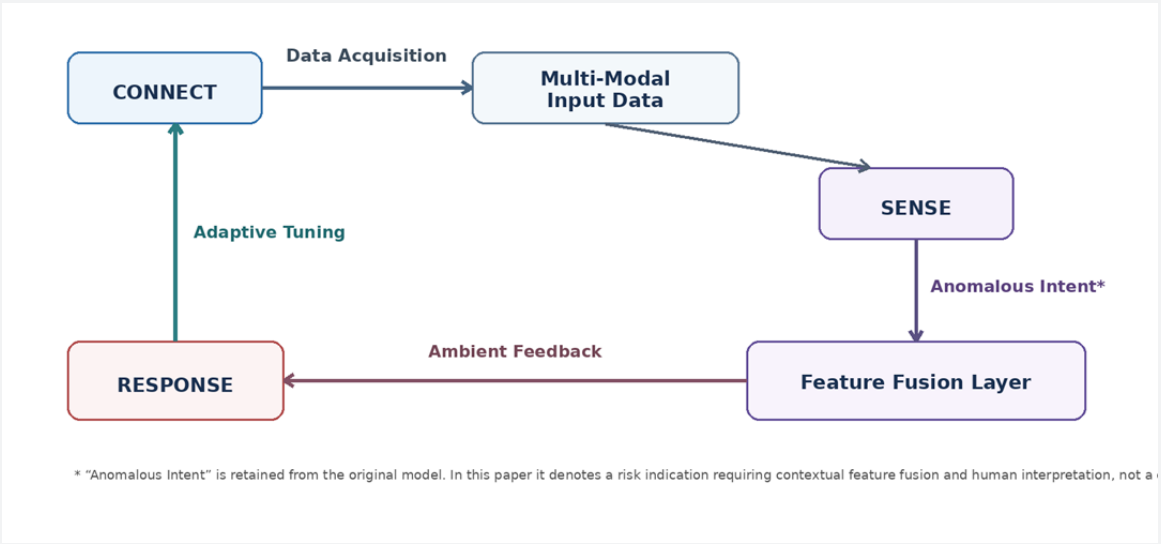

Figure 1: Algorithmic Logic of the HIBLISS Trinity (CONNECT-SENSE-RESPONSE).

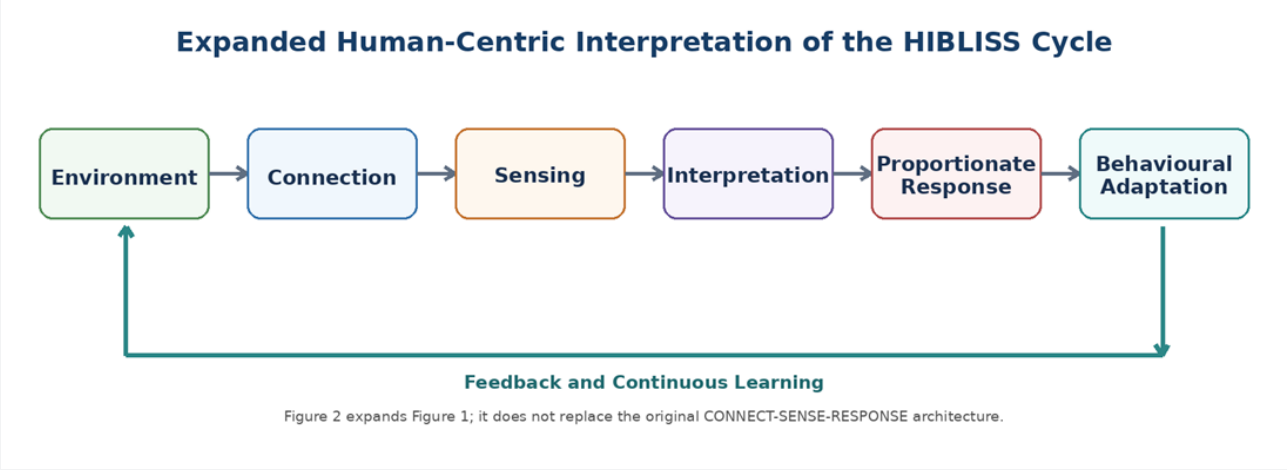

Figure 2: Expanded Human-Centric HIBLISS Cycle.

The "CONNECT" Phase (Data Acquisition & Feature Extraction)

The algorithmic foundation relies on multi-modal data ingestion. Unlike an architecture that depends primarily on explicit identification, CONNECT should prioritise contextual, relational and privacy-preserving information sufficient to establish the state of the environment and meaningful changes within it. In HIBLISS, however, CONNECT is broader than data acquisition. It also concerns the quality and safety of human participation and the protective relationships that can reduce the likelihood that a harmful trajectory develops.

Ingestion Architecture

In a physical environment, parallel data pipelines may ingest information from optical systems such as CCTV and video analytics, spatial sensors such as LiDAR, acoustic sensors, access-control systems, crowd-density measurements and environmental

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

or operational metadata. Relevant contextual variables may include passenger or pedestrian flow, queue length, scheduling bottlenecks, time, weather, lighting and the operational state of facilities.

In cyberspace, CONNECT may draw from a different combination of signals: content interaction, changes in communication or participation patterns, human reports, platform events, help-seeking activity and other contextual indicators. The objective is not indiscriminate collection. Data should be purpose-limited and proportionate to the security question being addressed.

Vectorisation

Raw telemetry is not itself intelligence. The CONNECT phase therefore transforms selected observations into features that can be analysed. Physical examples may include movement velocity, trajectory, dwell time, directional change, crowd density or acoustic characteristics. Digital examples may include temporal interaction patterns, changes in engagement, persistence, frequency and relationships among content, behaviour and reports.

Where direct identification is unnecessary, personally identifiable information should be removed, minimised, pseudonymised or processed at the edge. This is consistent with Privacy by Design: privacy safeguards should constrain the architecture from the beginning rather than being added after behavioural data have been collected.

Contextual and Protective Connection

The extension of SHBD into cyberspace adds an important second meaning to CONNECT. Connection is not only a technical link between sensors and an analytical engine. It also includes access to trustworthy information, healthy communities, credible support networks, digital literacy resources and channels for seeking help [2].

This produces two complementary forms of connection. Contextual connection links signals across environment, behaviour, content and reporting so that isolated observations are not interpreted without context. Protective connection strengthens relationships and resources that may themselves reduce risk. A person who remains connected to credible information, supportive communities and trusted human relationships may have greater opportunity to disengage from a harmful trajectory before formal security intervention is required.

Algorithmic Goal

The immediate algorithmic goal of CONNECT is to establish a real-time and dynamic baseline of the relevant environment. The baseline is not a permanent definition of 'normal' behaviour. It is a contextual reference that allows the system to identify meaningful change. This distinction is important because human behaviour varies across time, culture, location and circumstance. CONNECT therefore supplies SENSE with both observations and the context required to interpret them.

In relation to SbD, PbD and techno-regulation, CONNECT is the stage at which design choices define the field of possible interaction. Access mechanisms, information architecture, support channels, privacy settings and environmental affordances all influence what users can see, reach and do. HIBLISS therefore treats connection architecture itself as a security intervention: the design should make legitimate, safe and constructive pathways easy to reach while limiting unnecessary exposure to harmful or insecure conditions.

The "SENSE" Phase (Cognitive Analytics & Feature Fusion)

Once relevant features and contextual baselines are established, SENSE analyses whether observed changes represent ordinary variation, operational friction, vulnerability, distress, emerging risk or a potentially harmful trajectory. The purpose is not to label a person from a single behaviour or emotion, but to identify meaningful convergence among independent indicators.

Feature Fusion Layer

The algorithmic core of SENSE is multi-modal feature fusion. Instead of allowing one sensor or one behavioural indicator to determine the result, the system correlates multiple sources. In a physical environment, a sudden directional deviation may be considered together with dwell time, crowd conditions, access events and environmental stress. In a digital environment, changes in affect may be considered together with behaviour, content, persistence, capability indicators, human reporting and contextual information.

This is a central SHBD principle: risk significance should increase because several independent indicators converge across time and context, not merely because one signal becomes intense.

No single affective, behavioural or environmental indicator should ordinarily determine security intent or trigger a consequential response. Significance increases where multiple independent indicators converge across context and time. Such convergence should increase the priority for contextual assessment rather than automatically determine intent or guilt.

Affective and Behavioural Computing

Affective computing can enrich SENSE by helping identify changes in emotional expression and distinguish, for example, fear from anger or vulnerability from hostility. However, emotion is a signal, not a verdict. Anger, sadness, anxiety and fear are ordinary human experiences and should not independently trigger adverse security decisions.

Accordingly, affective information should be used primarily for aggregate awareness, assistance and triage, and interpreted alongside behavioural, contextual and temporal evidence. This

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

reduces the risk that probabilistic emotion inference becomes deterministic profiling.

Predictive Intent Modelling

The original HIBLISS algorithm can be expressed probabilistically as P(Incident | Vectors), where the system estimates the likelihood of an unfolding event given the available features. For human-centred applications, it is more appropriate to interpret this as trajectory or risk estimation rather than as a machine claim that it has discovered a person's intent.

The term "Anomalous Intent" is retained from the original HIBLISS diagram because it describes the transition between SENSE and the Feature Fusion Layer. It should not, however, be read as a claim that the system can directly know a person's intention. In the expanded model, it represents an algorithmically derived indication that observed patterns may be significant enough to require fusion with additional behavioural, environmental, affective and contextual evidence. Only after this fusion should the system determine whether further human assessment or response is justified.

$$R = f(A, B, C, P, K, I, X)$$

This formulation is conceptual rather than a validated predictive equation. It identifies categories of information whose relationships may inform contextual risk assessment. Their weighting, interaction effects and thresholds would require empirical development and validation for specific applications and environments.

where A represents affective indicators; B behavioural indicators; C content or environmental context; P persistence and temporal pattern; K capability indicators; I credible intent or preparation indicators; and X wider contextual factors. The output should support triage and human judgement rather than automated punishment.

The "Anxiety" Matrix Counterbalance

A distinctive feature of the original draft is that HIBLISS does not assume the human subject is always the source of abnormality. The SENSE layer should also examine whether the security architecture itself is creating friction, anxiety or unsafe conditions.

For example, if crowd stress rises at a security checkpoint, the cause may be excessive queueing, confusing routing or an access-control bottleneck rather than hostile behaviour. Likewise, repeated failure of a digital security process may indicate poor usability rather than user negligence. An Environmental Stress Index (ESI), if empirically developed and validated for a particular deployment, could therefore serve as a counterbalance by measuring whether system conditions are contributing to stress. At this stage ESI is best treated as a conceptual metric requiring operational validation rather than as an established universal measure.

Interpretation and Human Judgement

SENSE should culminate in interpretation, not automatic conviction. Algorithms are well suited to detecting patterns, ranking cases and identifying convergence across large volumes of information. They are less suited to resolving ambiguity involving culture, motivation, irony, vulnerability, legitimate dissent or rapidly changing context.

This is where HIBLISS deliberately departs from a purely deterministic form of techno-regulation. A fixed rule can encode a clear prohibition, but ambiguous behavioural situations require contextual interpretation. SENSE therefore acts as the mediating layer between observation and regulation. It determines whether a coded constraint is appropriate, whether a lower-friction intervention is sufficient, or whether the apparent anomaly is actually produced by the system itself. This preserves the value of design-based prevention without converting probabilistic behavioural inference into automatic enforcement.

Human judgement should therefore increase as the consequence of the decision increases. Low-impact environmental adjustments may be automated. Triage may be semi-automated. Decisions that materially affect a person's rights, access, reputation or liberty should require accountable human assessment.

The "RESPONSE" Phase (Ambient Countermeasures & Feedback Loops)

The unique differentiator of HIBLISS lies not only in what it senses but in how it responds. When a vulnerability, threat or high-anxiety condition is detected, RESPONSE should not default immediately to abrasive alarms, aggressive physical barriers or binary enforcement. The system should select an intervention proportionate to the nature, confidence and consequence of the assessed risk.

HIBLISS should select the least intrusive intervention reasonably capable of addressing the assessed condition. Response intensity should increase only as the confidence, consequence and immediacy of the concern increase.

Dynamic Spatial Alteration

In the physical environment, RESPONSE can alter conditions rather than merely confront individuals. If a crowd bottleneck creates stress and physical risk, routing displays may be adjusted, alternative paths opened, staffing changed, queue information improved, lighting modified or other environmental measures introduced to disperse flow and reduce uncertainty.

The key principle is behavioural adaptation through environmental design. The response changes the conditions influencing behaviour and then observes whether the resulting state is safer.

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

Acoustic, Informational and Digital Intervention

Ambient response can also include acoustic or informational measures where there is evidence that these interventions are suitable for the specific environment. Such interventions should not be assumed to have universal psychological effects; their effectiveness should be tested in context.

In cyberspace, the same logic may involve contextual information, counter-narratives, digital-literacy prompts, interruption of repeated harmful recommendations, friction before sharing high-risk content, access to help-seeking resources, trusted-human engagement, moderation or restriction. The intervention selected depends on the trajectory and level of concern.

This adaptive selection of interventions is what transforms a fixed regulatory mechanism into an adaptive security-governance cycle.

Adaptive Feedback Loop

In the original architecture, the return path is specifically labelled Adaptive Tuning. This means that RESPONSE does more than close an incident: it changes the parameters, environmental conditions or operational assumptions that CONNECT uses in the next cycle. Ambient Feedback is therefore both an intervention and a source of new evidence. The system learns whether the response reduced risk, reduced anxiety, improved flow or restored constructive behaviour, and then tunes subsequent acquisition and sensing accordingly.

RESPONSE is not the end of the algorithm. The outcome of an intervention is returned to CONNECT and becomes part of the next sensing cycle. If a routing change reduces crowd density and stress, the intervention provides evidence of effectiveness. If conditions worsen, the system should adjust, escalate or select a different intervention.

In human-centred applications, success should therefore include recovery indicators as well as detection indicators: reduced hostility, restored connection, successful help-seeking, safer participation, reduced environmental stress and successful rehabilitation.

Governance, Privacy and Human Oversight

The ability to collect and interpret behavioural and affective information creates a corresponding governance obligation. Without safeguards, an adaptive security architecture could become pervasive surveillance. SHBD explicitly rejects this outcome. The objective is situational awareness without universal surveillance, behavioural understanding without deterministic profiling, and early intervention without automated punishment [2].

Behaviour is not identity. HIBLISS should assess observable changes, conditions and trajectories within context rather than assign permanent risk identities to individuals based on inferred emotion, belief or behaviour. Behavioural Lead Intelligence should support contextual understanding and proportionate human assessment, not deterministic classification.

Privacy by Design is therefore not external to the HIBLISS algorithm. It constrains CONNECT through data minimisation and purpose limitation; constrains SENSE through contextual validity, bias testing and limits on emotion inference; and constrains RESPONSE through proportionality, human review, auditability and limits on secondary use.

Privacy by Design and Data Protection by Design in HIBLISS

The consideration of privacy within HIBLISS did not begin with its extension into cyberspace. In the HIBLISS Framework: Security & Happiness by Design, privacy was already incorporated as one of the measurable criteria within the broader Happiness Rating used to assess security-system design [4]. The framework proposed a five-level Privacy Rating ranging from “Very Low” to “Very High”. At the highest rating, the system analyses real-time behaviour without requiring or storing personal data. Where personal data are required, the rating decreases progressively according to the amount of personal information collected, the level of protection provided and the period for which the data are retained.

This earlier HIBLISS privacy model can be understood more clearly when considered alongside Privacy by Design (PbD) and Data Protection by Design (DPbD). Del-Real, De Busser and van den Berg (2024) distinguish privacy from data protection while recognising their close relationship. Privacy is a broader and more context-dependent concept, whereas data protection concerns the principles and safeguards activated when personal data are processed. They further note that the GDPR concepts of “data protection by design” and “data protection by default” are rooted in the broader principle of Privacy by Design.

Viewed from this perspective, the HIBLISS Privacy Rating already contains elements of both PbD and DPbD. Its highest privacy condition seeks to achieve the security objective without collecting or retaining personal data in the first place. Where this is not practicable, HIBLISS progressively considers the minimum amount of personal data required, how securely those data are protected and how long they should be retained. The assessment criteria therefore move beyond a general statement that privacy should be respected and translate privacy into concrete security-system design choices involving body capture, data minimisation, storage, protection and retention (Liu, 2024).

There is, however, an important distinction between the HIBLISS rating approach and PbD/DPbD. The HIBLISS Privacy Rating is primarily an assessment mechanism: it evaluates how privacy-sensitive a proposed security arrangement is. PbD and DPbD are primarily design principles: they require privacy and

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

data-protection requirements to be embedded proactively into the architecture and throughout the lifecycle of the system. Del-Real et al. (2024) found that PbD is comparatively well developed in this respect, encompassing not only technological design but also organisational practices, system operation and management.

The algorithmic HIBLISS model developed in this paper therefore builds upon the 2024 Privacy Rating by moving privacy considerations upstream from assessment into the CONNECT–SENSE–RESPONSE architecture itself. Privacy is no longer considered only when the completed security design is rated; it becomes a constraint governing how the algorithm operates. CONNECT should acquire the minimum information necessary for the defined security purpose and, where practicable, favour non-identifying, anonymised, pseudonymised or edge-processed information. SENSE should avoid unnecessary re-identification and should not convert behavioural or affective indicators into persistent personal profiles without justification. RESPONSE should similarly avoid exposing or retaining personal information beyond what is necessary for a proportionate intervention.

In this sense, the algorithmic HIBLISS model does not replace the earlier Privacy Rating. Rather, it builds upon and operationalises it. The five-level rating remains useful as an assessment measure, while PbD and DPbD provide the design principles through which a higher privacy rating can be achieved. This also strengthens the relationship between security and happiness within SHBD: the objective is not merely to increase security capability, but to obtain the necessary security outcome with the least privacy intrusion and minimum necessary processing of personal data.

Discussion: From Security by Design to Adaptive Human-Centric Security

Del-Real et al. [3] found that SbD and PbD share the principle of early integration but differ in conceptual development and orientation. PbD is more strongly anchored in rights and interdisciplinary thinking, whereas SbD has frequently concentrated on the technical product. HIBLISS supports the argument that security design should also consider the human and social environment in which technology operates.

The relationship can be summarised as a progression in design emphasis rather than a replacement of one framework by another. Security by Design asks how security can be embedded into the system from the outset. Privacy by Design asks how privacy and associated rights can be protected through technological and organisational design. Techno-regulation demonstrates that design can encode behavioural possibilities and constraints. SHBD/HIBLISS adds an adaptive human-centred layer: how can a human-technology environment continuously CONNECT, SENSE and RESPOND so that security, constructive behaviour, trust and well-being reinforce one another?

This progression also helps clarify the theoretical contribution of HIBLISS. The key innovation is not that software or infrastructure can restrict behaviour; techno-regulation already establishes that proposition. The contribution is the closed-loop logic by which the degree and form of behavioural influence can change in response to sensed context and observed outcomes. HIBLISS therefore moves from "security rules embedded in technology" towards "security and well-being objectives embedded in an adaptive human-technology system."

This reframes the security question. The objective is not for an algorithm to determine whether a person is 'dangerous'. It is to determine what observable conditions are changing, whether independent indicators are converging, what level of concern is justified, and what is the least intrusive effective action that can improve the situation.

The architecture presented in this paper is conceptual and requires empirical validation before deployment in consequential applications. Affective inference remains probabilistic and sensitive to cultural, linguistic and situational context. Behavioural baselines may change over time, while convergence among indicators does not itself establish harmful intent. Future validation should therefore examine multimodal feature fusion, contextual baselines, convergence thresholds, environmental stress measures and graduated response strategies across different environments. Evaluation should consider not only detection performance, but also false positives, proportionality, privacy impact, perceived fairness, recovery and unintended behavioural effects.

Conclusion

The algorithmic logic of HIBLISS remains grounded in its original trinity. CONNECT establishes the relationship among people, technology and environment and transforms selected observations into contextual features. SENSE combines those features to identify meaningful patterns, trajectories and environmental stress while retaining human interpretation for consequential judgements. RESPONSE translates intelligence into proportionate action and feeds the effects of intervention back into the system.

The original algorithmic path is CONNECT -> Data Acquisition -> Multi-Modal Input Data -> SENSE -> Anomalous Intent indication -> Feature Fusion Layer -> RESPONSE -> Adaptive Tuning -> CONNECT. The expanded human-centric interpretation can therefore be understood as Environment -> Connection -> Sensing -> Interpretation -> Proportionate Response -> Behavioural Adaptation -> Feedback. The second formulation makes explicit the human and governance logic of the first; it does not replace the original HIBLISS architecture.

The techno-regulation passage identified by Del-Real et al. [3] is therefore more than a supporting observation. It provides a conceptual starting point for understanding why HIBLISS can influence security through design. If technological systems can code (im)possibilities so that unsafe behaviour is prevented,

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926

then an adaptive system can also shape the conditions under which behaviour develops. HIBLISS adds sensing, interpretation, proportionality and feedback to that design logic. It can make unsafe behaviour difficult or impossible where firm constraint is justified, but it can also make safe, constructive and resilient behaviour easier and more likely where support, connection or environmental adjustment is the better response.

Accordingly, HIBLISS should be viewed as an adaptive human-centred security architecture: one that seeks to protect systems and people together while ensuring that technological intelligence remains bounded by privacy, fairness, proportionality and accountable human oversight.

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. Liu C (2026) Security & Happiness by Design in Cyberspace: A Human-Centric Framework for Affective, Behavioural and Digital Security Governance. Civil Engineering Research Journal. 15(5): 555925.
3. Del-Real C, De Busser E, van den Berg B (2024) Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review. Computer Law & Security Review 52: 105933.
4. Liu CL (2024) HIBLISS framework: Security & happiness by design. Journal of Infrastructure, Policy and Development 8(9): 5297.

DOI: 10.19080/CERJ.202.16.555926

How to cite this article: Chunlin L. Algorithmic Logic of the HIBLISS Trinity: CONNECT–SENSE–RESPONSE. Civil Eng Res J. 2026; 16(1): 555926. DOI:10.19080/CERJ.202.16.555926