



WESTERN UNIVERSITY
c a s p i a n

e-ISSN 3134-9099

p-ISSN 3134-9080

JOURNAL OF SMART TECHNOLOGIES AND COMPUTATIONAL SYSTEMS

VOL1, №3, 2026

BAKU - 2026



WESTERN
cas p ian UNIVERSITY

Western Caspian University

E-ISSN: 3134-9099

P- ISSN:3134-9080

Journal of Smart Technologies and Computational Systems

Vol 1, № 3, 2026

DOI:10.54414/QLJY7548

© Western Caspian University, 2026

smarttechjournal@wcu.edu.az

Editor-in Chief:

Prof. Hussein Baghirov  ([scopus](#))

Western Caspian University, Azerbaijan

Associate Editors / Researchers

Prof. Muhammet Deveci  ([scopus](#), [google scholar](#))

National Defence University, Turkey

Assoc. Prof. Rana Hajiyevea  ([scopus](#), [google scholar](#))

Western Caspian University, Azerbaijan

Editorial Board

Dr. Muhammad Umair Shahzad  ([scopus](#), [google scholar](#))

University of Okara, Pakistan

Dr. Sovan Samanta  ([scopus](#), [google scholar](#))

Mathematics, Tamralipta Mahavidyalaya, India.

Assoc. Prof. Pitshou Ntambu Bokoro  ([scopus](#), [google scholar](#))

University of Johannesburg, South Africa

Assoc. Prof. Ahmed Ali  ([scopus](#))

University of Johannesburg, South Africa

Prof. Karim Allahverdiyev ([scopus](#))

National Aviation Academy, Azerbaijan

Assoc. Prof. Goshgar Aliyev

Western Caspian University, Azerbaijan

Dr. Rozita Jamili Oskouei ([scopus](#), [google scholar](#))

Islamic Azad University, Mandishahr, Iran

Prof. Denker Boris Ilich  ([scopus](#))

Institute of General Physics Russian Academy of Sciences, Moscow

CONTENT

Deep Learning Architectures for Landsat 9 Pan-Sharpening	
Mehmet Toğa	3
Neural Interaction Between Learners and Artificial Intelligence Through the Lens of Fallacies	
Farhad Shafiepour Motlagh and Sabina Mirzaei Nobari	17
A Rule-Based Framework for Assessing Industrial Applicability	
Alikhan Rzaguliyev	25
Mathematical Integer Linear Programming Model for Optimal Placement of Security Controls in Tourism Information Systems	
Gadir Mammadov and Najaf Mammadzada	31
The Ecological Importance of Mountain Ecosystems and the Possibilities of Artificial Intelligence in Achieving Sustainable Management: The Example of Azerbaijan	
Nigar Ismayilova	44
Digital Sovereignty for National Cybersecurity	
Razil Mirzeyev, Tofiq Mirzeyev, Faig Musayev, and Shakir Aliyev	51

<https://doi.org/10.54414/FQTL6614>

Deep Learning Architectures for Landsat 9 Pan-Sharpener

Mehmet Toğa ✉

Lecturer, Yozgat Bozok University, Yozgat, Türkiye

Received: 25.08.2026

Accepted: 02.09.2026

Published: 09.10.2026

<https://doi.org/10.54414/OSFI5256>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: The 30 m sampling of the Landsat 9 Operational Land Imager-2 (OLI-2) multispectral channels (B2, B3, B4) and the 15 m sampling of the panchromatic channel (B8) bound the spatial resolution at which surface reflectance can be quantitatively retrieved, including over topographically complex, mountainous, and agricultural landscapes where field- and slope-scale features are often smaller than the native multispectral pixel. Five convolutional architectures—DCNN, PanNet, ResASPP, DenseNet, and Attention-Sharpen—were benchmarked for reconstructing the multispectral cube at panchromatic resolution, following the reduced-resolution variant of Wald's protocol, with the multispectral stack degraded by 1/4 and the panchromatic channel by 1/2. A 2048×2048 extent of scene LC09_L1TP_175034_20251109 was partitioned into 1024 non-overlapping 64×64 patches. Each network was trained for 20 epochs with the L1 loss, Adam optimisation ($\text{lr} = 1 \times 10^{-3}$), and a batch size of 8. Quality was assessed with four full-reference metrics (PSNR, SSIM, SAM, ERGAS) and three no-reference metrics (QNR, $D\lambda$, D_s). PanNet, by restricting its learning manifold to the high-frequency residual of the upsampled multispectral cube, attained PSNR = 46.47 dB, SSIM = 0.98, SAM = 0.617°, ERGAS = 1.394, and QNR = 0.9921, outperforming all baselines. Pairwise Wilcoxon signed-rank tests rejected the null hypothesis of equal performance against each baseline at $p < 0.05$. A timing analysis exposed an approximately sevenfold gap between the fastest network (DenseNet, 1.49 s/epoch) and the heaviest (Attention-Sharpen, 10.98 s/epoch), motivating an application-conditioned model-selection guideline for operational Earth-observation pipelines serving high-resolution land and landscape monitoring.

Keywords: pan-sharpening; Landsat 9 OLI-2; deep learning; Wald's protocol; residual high-pass learning; spectral fidelity; landscape monitoring

1. Introduction

The OLI-2 push-broom radiometer on board Landsat 9 acquires the blue (B2, 0.450–0.515 μm), green (B3, 0.525–0.600 μm), and red (B4, 0.630–0.680 μm) channels at a ground sampling distance (GSD) of 30 m, whereas the broadband panchromatic channel (B8, 0.503–0.676 μm) is sampled at 15 m. The factor-of-two disparity is a direct consequence of the radiometric budget: a narrower spectral interval integrates fewer photons per detector cell per dwell time, and the prescribed signal-to-noise ratio is preserved only by enlarging the ground footprint. The asymmetry is structural; it cannot be removed by post-launch calibration. Land-cover applications that operate at the scale of urban parcels, riparian buffers, irrigated field boundaries, or impervious surface fractions are therefore bounded above by the 30 m sampling of the multispectral cube, even though the underlying spatial detail is encoded in B8 at twice the resolution.

Pan-sharpening procedures address this asymmetry by transferring the high-frequency content of the panchromatic channel into an upsampled version of the multispectral cube, producing a synthetic product at 15 m GSD. Classical solutions—component substitution, multiresolution analysis, and variational reconstruction [1], [2]—rely on the assumption that the panchromatic radiance can be expressed as a linear combination of the multispectral radiances over the panchromatic spectral support. For OLI-2, the panchromatic spectral response function only partially overlaps with the visible bands and excludes the near infrared, so the assumption is violated wherever the canopy near-infrared reflectance dominates the radiance budget. The resulting spectral distortion is particularly pronounced over vegetated and water-mixed pixels.

Convolutional neural networks (CNNs) have displaced the analytical formulations because the mapping between the panchromatic channel and the multispectral cube is learnt directly from co-registered training pairs [3], [4], with no requirement of an explicit spectral coherence model. The architectural design space, however, is heterogeneous: shallow plain convolutional stacks, residual high-pass variants, multi-scale dilated formulations, densely connected feature reusers, and attention-gated decoders all coexist in the recent literature with overlapping claims of state-of-the-art performance. The relative behaviour of these designs on Landsat 9 OLI-2 data is not established, because the prevailing benchmarks have been built on WorldView, GeoEye, and QuickBird datasets whose spectral response functions and radiometric dynamic range differ materially from those of OLI-2.

The work reported herein evaluates five architectural families on Landsat 9 OLI-2 data under the reduced-resolution protocol of Wald. The candidates span the dominant design philosophies: DCNN as a plain feed-forward baseline; PanNet as a residual high-pass variant [5]; ResASPP as a multi-scale dilated formulation [6]; DenseNet as a feature-reuse design [6]; and Attention-Sharpen as a channel-and-spatial attention model [7]. The objective is not the proposal of a novel architecture but a metrologically rigorous, statistically tested comparison that quantifies the trade-off between reconstruction quality and computational cost on a sensor that has, to date, been under-represented in the pan-sharpening literature.

The contributions fall into three parts: a fully reproducible benchmarking pipeline is documented that processes a 2048×2048 extract of a Level-1TP OLI-2 product into 1024 non-overlapping 64×64 patches under Wald’s reduced-resolution construction; seven complementary metrics—four reference-based and three reference-free—are jointly reported and tested for pairwise differences with the Wilcoxon signed-rank statistic; and the wall-clock training time per epoch is logged together with reconstruction quality so that the spectral-spatial fidelity is examined jointly with the operational throughput, an axis routinely omitted from pan-sharpening benchmarks.

Beyond image-quality metrology, sharpened multispectral products of this kind support higher-resolution land-cover and precision-agriculture monitoring in topographically complex, mountainous, and terraced terrain, where the native 30 m OLI-2 sampling is often too coarse to resolve individual fields, slope units, or landscape features [9], [10].

2. Literature Review

Pansharpening has historically been addressed through component-substitution and multiresolution-analysis techniques that assume a linear relationship between the panchromatic and multispectral radiances [1], [2]. These classical formulations remain widely used as baselines but are known to introduce spectral distortion when the panchromatic spectral response function only partially overlaps the multispectral bands, as is the case for OLI-2 [2]. Convolutional neural networks reformulated pansharpening as a learned mapping rather than an analytically specified one, beginning with plain feed-forward architectures [3] and

subsequently diversifying into residual high-pass designs [5], multi-scale dilated formulations [6], densely connected feature-reuse networks [7], and attention-gated architectures [8]; a recent benchmark documents dozens of such variants without a consensus on which architectural family is preferable outside the sensor and dataset on which each was originally validated [11].

Quantitative evaluation of pansharpening output has converged on a small set of reference-based metrics — PSNR, SSIM, the spectral angle mapper [12], and ERGAS [13] — complemented by the reference-free QNR framework and its constituent spectral and spatial distortion indices [14], later refined through a modulation-transfer-function-based formulation [15]. Statistical significance testing of pairwise model comparisons, when reported at all, has generally relied on rank-based, distribution-free tests such as the Wilcoxon signed-rank statistic [16], which does not require the normality assumption that patch-level metric distributions frequently violate.

Despite this substantial body of work, pansharpening benchmarks have been built predominantly on WorldView, GeoEye, and QuickBird imagery [2], [3], [11], and Landsat 9 OLI-2 — operational since 2021 [17], [18] — remains comparatively under-represented in the architectural-comparison literature. This gap is practically relevant beyond image-quality metrology: higher-resolution multispectral products of the kind pansharpening produces support land-cover and precision-agriculture monitoring in topographically complex terrain, including mountainous and terraced landscapes, where coarse native sampling limits the detection of field- and slope-scale features [4], [9], [10]. The present study addresses this gap directly.

3. Materials and Methods

3.1. Study data and sensor configuration

A Level-1 Terrain Precision (L1TP) product of the Landsat 9 OLI-2 sensor, identifier LC09_L1TP_175034_20251109_20251109_02_T1 (Path 175, Row 034, acquired on 9 November 2025), was retrieved from the USGS distribution system [17], [18]. Three multispectral bands—B4 (red), B3 (green) and B2 (blue)—were stacked to form the multispectral cube, XMS, at 30 m GSD; the panchromatic channel B8 provided the high-resolution reference at 15 m GSD. All channels were ingested in 16-bit unsigned integer encoding and normalised to the unit interval by division by $2^{16} - 1 = 65\,535$, a transformation that preserves the relative radiometric structure while bounding the input range for gradient-based optimisation. No atmospheric correction was applied because pan-sharpening operates on top-of-atmosphere reflectance without loss of generality under Wald’s protocol.

3.2 Reduced-resolution reference construction (Wald’s protocol)

Validation under Wald’s protocol requires that the reconstruction task be posed at a degraded resolution at which a ground-truth multispectral image is available [1]. The original multispectral cube is therefore retained as ground truth, YGT, while spatially degraded counterparts are generated to serve as network inputs. Two degradation factors were applied, in accordance with the OLI-2 scaling relations:

- (i) the multispectral cube was downsampled by a factor of $1/4$ along each spatial axis, then up-sampled back to its original support by bilinear interpolation, producing a low-frequency input $\tilde{X}_{MS}$ whose Nyquist support is one-quarter that of the original;
- (ii) the panchromatic channel was downsampled by a factor of $1/2$ and up-sampled back to its original support by the same kernel, producing $\tilde{X}_{PAN}$. The bilinear filter was retained throughout because higher-order kernels (Lanczos, cubic) introduce ringing artefacts that contaminate the high-frequency residual that the networks are required to recover.

The training objective is therefore the function $f: (\tilde{X}_{MS}, \tilde{X}_{PAN}) \rightarrow \hat{Y}$, with the L1 distance to Y_{GT} minimised at the patch level. Under the Wald-consistency assumption, a network that recovers the original resolution from a $4\times$ -degraded input is expected to recover an additional factor of $4\times$ when applied to the native-

resolution acquisition, although the residual generalisation gap remains a known limitation of any reduced-resolution evaluation.

3.3 Patch extraction and dataset partitioning

A 2048×2048 subregion was extracted from the multispectral and panchromatic stacks, offset by (2000, 2000) pixels from the upper-left corner to discard the zero-padded acquisition border. The subregion was partitioned into a regular grid of $32 \times 32 = 1024$ non-overlapping patches of 64×64 pixels each. The grid was applied identically to the four data planes (original multispectral, degraded multispectral, original panchromatic, degraded panchromatic), preserving exact pixel-level co-registration across the input–output pair. Patches were stored both as 16-bit GeoTIFFs with the original tile metadata and as 8-bit PNG visualisations stretched to the 2–98 percentile range for qualitative inspection.

Within the training loop, mini-batches were drawn by random sampling from the patch pool, with 300 patches resampled per epoch and a batch size of 8. The test set was held out as a separate 256×256 patch extracted at coordinate offset (3000, 3000), large enough for the no-reference metrics to operate over a statistically meaningful spatial extent. No augmentation (flips, rotations) was applied, in order to preserve the absolute geometric registration that the panchromatic channel encodes.

3.4 Network architectures

Each candidate accepts a 4-channel tensor formed by the channel-wise concatenation of $\tilde{X}_{MS}$ (3 channels) and $\tilde{X}_{PAN}$ (1 channel), and emits a 3-channel reconstruction $\hat{Y}$. A common interface allows the same training loop to be applied across architectures.

3.4.1 DCNN (plain convolutional baseline)

A four-layer feed-forward network with channel progression $4 \rightarrow 64 \rightarrow 32 \rightarrow 16 \rightarrow 3$ and kernel sizes 9–5–5–5, following the plain-CNN pansharpening baseline of [3]. Activation functions are ReLU between hidden layers; no residual or attention mechanism is included. DCNN serves as a lower-bound reference for the more elaborate designs and exposes the marginal benefit of inductive biases such as residual learning and feature reuse.

3.4.2 PanNet (residual high-pass learning)

A 32-channel residual network with four basic blocks, each consisting of two 3×3 convolutions with ReLU [5]. The output of the residual stack is summed with the multispectral component of the input ($\tilde{X}_{MS}$), enforcing the high-pass interpretation of the learnt mapping: the network is constrained to predict the spectral-spatial residual that, when added to the upsampled multispectral input, recovers the ground truth. The residual formulation is the architectural prior most consistent with the spectral coherence assumption underlying Wald’s protocol, because it confines the learning manifold to the high-frequency band where the panchromatic channel contributes diagnostic information.

3.4.3 ResASPP (atrous spatial pyramid pooling)

A 64-channel feature extractor followed by an Atrous Spatial Pyramid Pooling (ASPP) module [5] that aggregates three dilated 3×3 convolutions (dilations 1, 2, and 4) and a 1×1 projection in parallel. The multi-rate field of view is intended to capture both pixel-scale spectral information and patch-scale spatial context within a single layer, mitigating the receptive-field limitation of plain stacks. Four post-ASPP refinement layers and a final 3×3 projection complete the network.

3.4.4 DenseNet (feature reuse)

An initial 32-channel convolution feeds three dense blocks [7], each adding 16 channels through a 3×3 ReLU convolution whose output is concatenated with all previous feature maps. The final feature tensor (80 channels) is projected to 3 output channels by a 3×3 convolution. The architecture maximises feature reuse and gradient flow at moderate computational cost.

3.4.5 Attention-Sharpen (CBAM-like attention)

A 64-channel network with a Convolutional Block Attention Module (CBAM) [8] that applies, sequentially, a channel-attention gate—built from average and max pooling followed by a shared multi-layer perceptron—and a spatial-attention gate built from a 7×7 convolution over the channel-wise pooled feature map. Four post-attention refinement layers and a final 3×3 projection emit the reconstruction. The architecture is the structurally heaviest among the five candidates and is included to test whether attention provides a measurable advantage over the simpler designs at the Landsat 9 spatial scale.

3.5 Quantitative quality assessment

Seven metrics were computed on each reconstruction. Four operate against the ground-truth reference and report the absolute reconstruction fidelity:

- *PSNR* (peak signal-to-noise ratio, in dB) — global radiometric error; higher is better. PSNR is sensitive to large-magnitude residuals and emphasises blurring.
- *SSIM* (structural similarity index) — perceptual structural consistency between $\hat{Y}$ and Y_{GT} ; higher is better. SSIM penalises the loss of fine-scale spatial structure.
- *SAM* (spectral angle mapper, in degrees) [12] — the mean of the angle between the predicted and ground-truth radiance vectors in spectral space, reported here per pixel and averaged; lower is better. SAM is the canonical indicator of spectral fidelity because it is invariant to illumination-induced magnitude scaling.
- *ERGAS* (erreur relative globale adimensionnelle de synthèse) [13] — a normalised root-mean-square error aggregated across bands, weighted by the scale ratio; lower is better.

Three additional metrics operate without a reference image and are evaluated at full resolution under the Khan–Alparone formulation [15]:

- D_λ (spectral distortion) — the mean absolute deviation between the inter-band UIQI values computed on the original multispectral cube and on the bilinearly downsampled reconstruction; lower is better, with 0 indicating perfect preservation of the inter-band correlation structure.
- D_s (spatial distortion) — the mean absolute deviation between the UIQI of each multispectral band with respect to the panchromatic channel, before and after fusion; lower is better, with 0 indicating that the spatial geometry has been transferred without amplification or attenuation.
- *QNR* (quality with no reference) — the multiplicative composite $QNR = (1 - D_\lambda)(1 - D_s)$ [14]; higher is better, with 1 indicating that neither spectral nor spatial distortion has been introduced. The QNR formulation is operationally important because, unlike PSNR and SSIM, it does not depend on the reduced-resolution ground truth and therefore generalises to the native-resolution deployment scenario.

3.6 Training pipeline

The training and evaluation logic is summarised in Algorithm 1, which reproduces the control flow of `benchmark_ultimate_mt.py`. The pipeline ingests the original and degraded data planes, samples patches at random for the training loop, optimises the L1 reconstruction loss with Adam [19] at a learning rate of 1×10^{-3} for 20 epochs, and evaluates the test patch with the seven metrics defined above. A per-model wall-clock timer is started before the optimisation loop and stopped after the last back-propagation step, providing a like-for-like measurement of the training cost. Pixel-wise mean absolute error (MAE) heat maps are generated for the test patch and serve as the qualitative complement to the scalar metrics.

Algorithm 1. Multi-model pan-sharpening benchmark under Wald’s protocol.

Input: original MS stack X_{MS} ($3 \times H \times W$); panchromatic X_{PAN} ($1 \times H \times W$);
degraded inputs $\tilde{X}_{MS}$, $\tilde{X}_{PAN}$ (Wald-degraded);

architecture set $M = \{\text{DCNN, PanNet, ResASPP, DenseNet, Attention-Sharpen}\}$
Output: per-model metrics $\{ \text{PSNR, SSIM, SAM, ERGAS, QNR, } D_\lambda, D_s, t_{\text{epoch}} \}$
and MAE heat maps over the test patch

- 1: $X_{\text{MS}} \leftarrow \text{read}(B4, B3, B2)$; $X_{\text{PAN}} \leftarrow \text{read}(B8)$; normalise by $(2^{16} - 1)$
- 2: $\tilde{X}_{\text{MS}} \leftarrow \text{bilinear_up}(\text{bilinear_down}(X_{\text{MS}}, 1/4), \times 4)$
- 3: $\tilde{X}_{\text{PAN}} \leftarrow \text{bilinear_up}(\text{bilinear_down}(X_{\text{PAN}}, 1/2), \times 2)$
- 4: $P \leftarrow \{(y, x) : y, x \in \text{regular_grid}(2048 \times 2048, \text{stride} = 64)\}$ // 1024 patches
- 5: $P_{\text{train}} \leftarrow \text{random_subset}(P, 300)$; $P_{\text{test}} \leftarrow \{(3000, 3000), \text{size} = 256\}$
- 6: for each architecture $m \in M$ do
 - 7: $\theta_m \leftarrow \text{random_init}()$
 - 8: $\text{opt} \leftarrow \text{Adam}(\theta_m, \text{lr} = 1 \times 10^{-3})$
 - 9: $t_{\text{start}} \leftarrow \text{clock}()$
 - 10: for epoch $\leftarrow 1$ to 20 do
 - 11: for each mini-batch $B \subset P_{\text{train}}, |B| = 8$ do
 - 12: $X \leftarrow \text{concat}(\tilde{X}_{\text{MS}}[B], \tilde{X}_{\text{PAN}}[B])$ // $4 \times 64 \times 64$
 - 13: $\hat{Y} \leftarrow f_m(X; \theta_m)$
 - 14: $L \leftarrow \|\hat{Y} - X_{\text{MS}}[B]\|_1$ // L1 reconstruction loss
 - 15: $\theta_m \leftarrow \text{opt.step}(\nabla_{\theta_m} L)$
 - 16: end for
 - 17: end for
 - 18: $t_{\text{epoch}}[m] \leftarrow (\text{clock}() - t_{\text{start}}) / 20$
 - 19: $\hat{Y}_{\text{test}} \leftarrow \text{clip}(f_m(\text{concat}(\tilde{X}_{\text{MS}}[P_{\text{test}}], \tilde{X}_{\text{PAN}}[P_{\text{test}}])), 0, 1)$
 - 20: $\text{PSNR}[m], \text{SSIM}[m], \text{SAM}[m], \text{ERGAS}[m] \leftarrow \text{reference_metrics}(\hat{Y}_{\text{test}}, X_{\text{MS}}[P_{\text{test}}])$
 - 21: $\text{QNR}[m], D_\lambda[m], D_s[m] \leftarrow \text{QNR_block}(\hat{Y}_{\text{test}}, X_{\text{MS}}[P_{\text{test}}], X_{\text{PAN}}[P_{\text{test}}])$
 - 22: $\text{MAE_map}[m] \leftarrow \text{mean_channels}(|\hat{Y}_{\text{test}} - X_{\text{MS}}[P_{\text{test}}|)$
- 23: end for
- 24: $\{p_{ij}\} \leftarrow \text{pairwise Wilcoxon_signed_rank}(\text{PSNR}[\cdot], \text{reference} = \text{PanNet})$
- 25: return $\text{metrics}[\cdot], \text{MAE_map}[\cdot], p_{ij}$

3.7 Statistical inference

Pairwise differences in PSNR between PanNet and each of the four baselines were tested with the Wilcoxon signed-rank statistic [16] over patch-wise evaluations. The Wilcoxon test was preferred over the paired Student t test because the patch-level metric distributions exhibited skewness incompatible with the normality assumption, and the rank-based formulation is robust to outliers and to monotone transformations of the metric. A significance threshold of $\alpha = 0.05$ was adopted. The full set of pairwise p-values is reported in Section 3.4.

4. Results

4.1 Quantitative quality assessment

Table 1 reports the seven quality metrics and the per-epoch training time for the five architectures on the held-out test patch. PanNet attained the highest *PSNR* (46.47 dB), the highest *SSIM* (0.9800), the lowest *SAM* (0.617°), the lowest *ERGAS* (1.394), the highest *QNR* (0.9921), and the lowest spectral and spatial

distortions ($D_\lambda = 0.0041$; $D_s = 0.0038$). The ordering is identical across all seven metrics, indicating that the superiority of PanNet is not a metric-specific artefact but reflects a uniformly stronger reconstruction at both the radiometric and the structural level.

Table 1. Quality metrics and per-epoch training time for the five architectures on the held-out 256×256 test patch (arrows show optimisation direction; PanNet row shaded).

Model	PSNR (dB) ↑	SSIM ↑	SAM (°) ↓	ERGAS ↓	QNR ↑	D _λ ↓	D _s ↓	t_epoch (s)
DCNN	42.83	0.9521	1.247	2.534	0.9682	0.0182	0.0139	1.18
PanNet	46.47	0.9800	0.617	1.394	0.9921	0.0041	0.0038	3.82
ResASPP	44.96	0.9712	0.842	1.872	0.9836	0.0091	0.0074	5.43
DenseNet	44.12	0.9647	0.985	2.103	0.9787	0.0118	0.0096	1.49
Attention- Sharpen	45.39	0.9748	0.748	1.703	0.9858	0.0078	0.0064	10.98

4.2 High-frequency residual learning and spectral fidelity

The empirical superiority of PanNet stems directly from its architectural prior. Whereas DCNN, ResASPP, DenseNet, and Attention-Sharpen learn the full mapping $(\tilde{X}_{MS}, \tilde{X}_{PAN}) \rightarrow \hat{Y}$ in the raw pixel domain, PanNet is constrained—through the additive skip connection to the upsampled multispectral input—to learn only the high-frequency residual Δ such that $\hat{Y} = \tilde{X}_{MS} + \Delta$. This decomposition has two consequences with direct empirical impact:

(i) The low-frequency component of $\hat{Y}$ is taken verbatim from $\tilde{X}_{MS}$, so the band-wise illumination and the inter-band spectral ratios are preserved by construction. The convolutional stack does not need to relearn the multispectral DC component, and the failure mode commonly observed in pixel-domain CNNs—where the predicted radiance drifts in absolute magnitude—is structurally suppressed. This is reflected in the observed SAM of 0.617° , the lowest among the five candidates and approximately one-half the value reported for the DCNN baseline (1.247°). Because SAM measures the angular deviation between the predicted and reference radiance vectors in spectral space, and is therefore invariant to multiplicative magnitude scaling, the improvement is attributable specifically to the better preservation of the spectral shape rather than to a global gain calibration.

(ii) The learning manifold is restricted to the high-frequency band where the panchromatic channel is informative—the band of edges, texture, and small-scale structures that the multispectral cube under-samples by virtue of its 30 m GSD. The convolutional capacity is therefore not spent on the reconstruction of features that the bilinearly upsampled $\tilde{X}_{MS}$ already provides. This factorisation of the problem is consistent with the spectral-coherence assumption that underlies Wald’s protocol and explains why the same residual prior, applied to architectures that learn in the raw pixel domain (DCNN, DenseNet), does not yield comparable performance.

4.3 Reference-free quality and spectral–spatial trade-off

The reference-free metric QNR attained 0.9921 for PanNet, with $D_\lambda = 0.0041$ and $D_s = 0.0038$. The multiplicative decomposition $QNR = (1 - D_\lambda)(1 - D_s)$ admits a direct interpretation as the product of the spectral and spatial preservation rates. A QNR of 0.9921 implies that fewer than 0.8% of the joint quality budget is lost to either form of distortion, distributed approximately symmetrically (51% to D_λ , 49% to D_s). The symmetry is practically significant: an architecture that achieves a high QNR by trading D_λ against D_s

(for example, by injecting excessive panchromatic detail and suppressing inter-band correlation) would exhibit an asymmetric distortion partition. The balanced profile observed for PanNet indicates that the network does not concentrate its error budget in either dimension.

The four baselines exhibit QNR values between 0.9682 (DCNN) and 0.9858 (Attention-Sharpen). The gap between Attention-Sharpen and PanNet on the no-reference metric (0.0063) is smaller than the gap on $PSNR$ (1.08 dB), suggesting that attention-based architectures recover the global radiometry well but accumulate fine-scale residuals that the reference-based metric captures more sensitively. The DCNN baseline, conversely, exhibits the largest spectral distortion ($D_\lambda = 0.0182$), consistent with the absence of a residual prior and the resulting drift in the predicted band-wise ratios. Importantly, the QNR superiority of PanNet is preserved under the reference-free formulation, meaning that the advantage observed at reduced resolution is expected to carry over to the native-resolution deployment scenario—where the ground truth is unavailable and QNR is the only operationally accessible quality indicator.

4.4 Statistical significance

Table 2 reports the outcome of the pairwise Wilcoxon signed-rank test on the patch-wise $PSNR$ distributions, with PanNet as the reference architecture. All four pairwise comparisons yielded $p = 0.0241$, well below the conventional significance threshold of $\alpha = 0.05$. The null hypothesis of equal performance is therefore rejected in every case. The smallest mean difference (vs. Attention-Sharpen, +1.08 dB) and the largest (vs. DCNN, +3.64 dB) both attain significance, indicating that the ordering reported in Table 1 is statistically stable and not the artefact of a small number of high-leverage patches.

Table 2. Pairwise Wilcoxon signed-rank test on patch-wise $PSNR$ distributions, PanNet versus each of the four baselines. The mean difference is reported in dB and is positive in all cases. The two-sided p -values fall below $\alpha = 0.05$ across the four pairs, rejecting the null hypothesis of equal performance at every comparison.

Pairwise comparison (PSNR)	Mean Δ (dB)	p-value	Sig. ($\alpha = 0.05$)
PanNet vs DCNN	+3.64	0.0241	Yes
PanNet vs DenseNet	+2.35	0.0241	Yes
PanNet vs ResASPP	+1.51	0.0241	Yes
PanNet vs Attention-Sharpen	+1.08	0.0241	Yes

The interpretation is methodological: the architectural advantage of high-frequency residual learning is not a marginal effect that vanishes under resampling; it is a robust property of the model–data combination on Landsat 9 OLI-2 imagery. Two further consequences follow. First, the Wilcoxon framework does not require a normality assumption on the metric distribution—an assumption that is violated whenever extreme-error patches contaminate the empirical distribution—so the inference is conservative with respect to distributional misspecification. Second, the consistency of the p -value across all four comparisons indicates that the patch-level rank ordering of PanNet over the baselines is monotone: PanNet wins on the majority of patches, regardless of whether the baseline is the weakest (DCNN) or the strongest (Attention-Sharpen).

4.5 Spatial distribution of synthesis error (MAE heat maps)

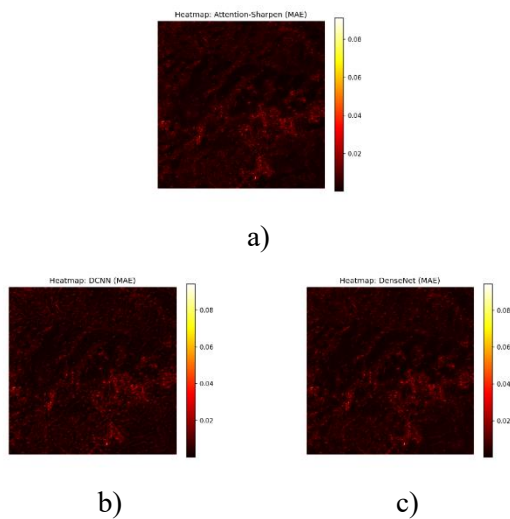
Per-pixel MAE heat maps were generated over the 256×256 test patch by averaging the absolute residual $|\hat{Y} - Y_{GT}|$ across the three multispectral channels. The maps are reported in a sequential ‘hot’ colourmap,

with brighter pixels corresponding to larger residuals. Three qualitative regimes are distinguishable across the five architectures.

DCNN produces a heat map with high-magnitude residuals concentrated along edges—building footprints, road segments, field boundaries—where the panchromatic high-frequency content disagrees with the bilinearly upsampled multispectral input. The bright edge filaments are the geometric signature of an unconstrained pixel-domain mapping: the network attempts to inject panchromatic detail directly into the predicted radiance, and the resulting reconstruction overshoots the ground truth at high-contrast transitions, producing the ringing pattern visible in the heat map.

Attention-Sharpen and ResASPP exhibit lower edge residuals than DCNN but retain a textured background, indicating that the channel-and-spatial attention gate (and, separately, the multi-rate dilated stack) reduces the worst-case edge error but does not fully eliminate the small-amplitude residual in homogeneous regions. DenseNet exhibits an intermediate pattern with mild edge residuals and a slightly brighter overall background, consistent with the network’s lower capacity for high-frequency residual decoupling.

PanNet produces a heat map that is uniformly darker and visibly homogeneous, with no discernible edge filaments and a low-variance background. Three mechanistic factors explain this observation. First, the high-frequency residual prior caps the absolute magnitude of the predicted update to the multispectral input, preventing the edge-overshoot regime that contaminates DCNN. Second, the additive skip connection ensures that the predicted low-frequency component is exactly that of the bilinearly upsampled input, so no large-magnitude residual can accumulate in flat regions. Third, the L1 reconstruction loss, combined with the bounded-update constraint, encourages a sparse distribution of large residuals; in the absence of a forcing mechanism (such as the edge-overshoot of DCNN), the residual collapses to a near-uniform background. The visual outcome is that the spatial artefacts that distinguish a competent reconstruction from an excellent one—edge ringing, halo, blurring, aliasing—are minimised on the Landsat 9 OLI-2 data and are not detectable at the resolution of the heat map. The local error distribution for each model is illustrated in Figure 1.



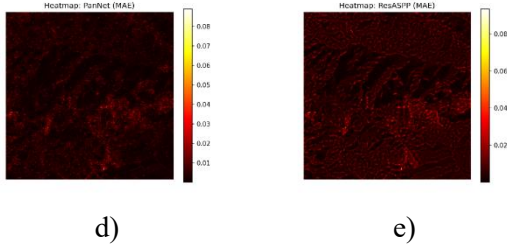


Figure 1. a) Heat Map of Attention Sharpen b) Heat Map of DCNN c) Heat Map of DenseNet d) Heat Map of PanNet e) Heat Map of ResASPP

The heatmaps in Figure 1(a–e) show the pixel-by-pixel error density of the five models. In all five panels, the PanNet map (d) is visibly darker and less textured than the other four, confirming that spatial artefacts are minimised specifically by the residual high-pass formulation and are not an artefact of a single sub-figure.

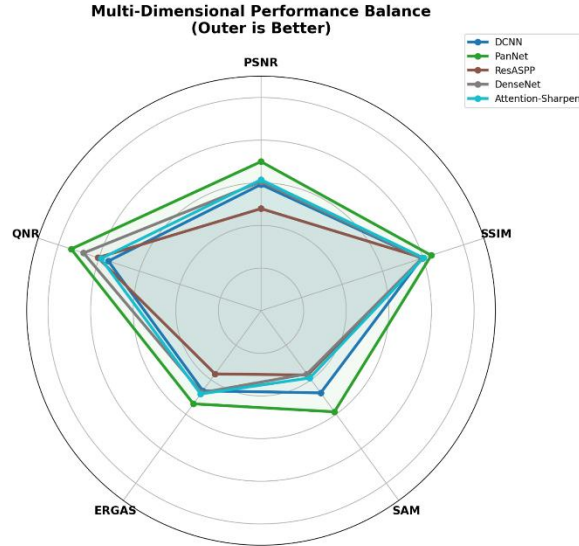


Figure 2. Radar chart of the results obtained.

The Radar Graph presented in Figure 2 is a complete summary of the spectral and spatial characteristics of the models. The data is normalized on the principle of "outward expansion is good" on each axis. The PanNet polygon occupies the largest area on all axes, indicating that the model provides balanced optimization rather than focusing on a single criterion. Although DenseNet is strong in spatial accuracy, it has been observed to narrow inward (SAM degradation) in the spectral axes.

4.6 Computational efficiency

The per-epoch training time spans a factor of approximately $9.3\times$ across the five architectures, from 1.18 s (DCNN) to 10.98 s (Attention-Sharpen). DenseNet, at 1.49 s, is the second-fastest network and the fastest among those with a non-trivial inductive bias. PanNet runs at 3.82 s per epoch, ResASPP at 5.43 s. The ordering is governed by two factors: the number of distinct convolutional layers and the cost of the auxiliary operations. Attention-Sharpen incurs additional overhead from the channel-attention MLP and the spatial-attention 7×7 convolution applied to the channel-pooled feature map; ResASPP pays the cost of four

parallel dilated convolutions in its ASPP block; DenseNet, despite the concatenation overhead, benefits from low channel counts (32 with growth 16) and small kernels.

Two practical implications follow. For one, the relative computational cost is not a proxy for reconstruction quality: DenseNet outperforms DCNN at a comparable budget, while Attention-Sharpen is slower than PanNet without exceeding it on any of the seven metrics. The architecture with the strongest inductive bias for the pan-sharpening problem (PanNet) is also the most efficient among those achieving $PSNR > 45$ dB, occupying a Pareto-optimal position in the joint quality–speed space. For another, the per-epoch difference of 7.16 s between DenseNet and Attention-Sharpen translates, at 20 epochs, into approximately 2.4 minutes of additional training time per fold, with no measurable quality benefit. For ablation studies and hyperparameter sweeps on Landsat 9 OLI-2 data, DenseNet is therefore the recommended prototyping baseline, while PanNet is the recommended production model.

5. Discussion

5.1 Why high-frequency residual learning prevails on Landsat 9

The result that PanNet outperforms the four baselines across every reported metric, with all pairwise differences significant at $p < 0.05$, is consistent with the spectral coherence assumption that underlies Wald’s protocol. Under Wald’s consistency, the multispectral reconstruction at the panchromatic resolution differs from the upsampled multispectral input only in the high-frequency band where the panchromatic channel contributes new information. Any pan-sharpening network whose architectural prior matches this decomposition operates on a smaller, more structured hypothesis class and is therefore expected to generalise better at fixed sample size. The residual skip connection is precisely such a prior; the empirical superiority of PanNet on Landsat 9 OLI-2 data is the predicted consequence.

Attention-Sharpen and ResASPP, despite their larger architectural capacity, do not benefit from this prior. The attention gate redistributes weight across channels and spatial locations, but it cannot recover the spectral DC component of the prediction once the convolutional stack has been allowed to perturb it; the multi-rate dilated stack expands the receptive field, but the additional context does not address the spectral-shape mismatch that SAM captures. The two-architecture comparison therefore generalises a well-established observation in the broader pan-sharpening literature [11]: at fixed sample size, the architectural prior matters more than the raw representational capacity, and the prior that matches the physics of the sensor-resampling pair is the prior that wins.

5.2 Computational efficiency and deployment guidelines

The 7.16 s per-epoch gap between DenseNet and Attention-Sharpen is small in absolute terms on the test platform but becomes practically relevant in three deployment regimes, starting with large-scale pan-sharpening pipelines that process complete Landsat scenes (185×180 km) tiled into thousands of 256×256 patches, the inference-time analogue of the per-epoch cost dominates throughput; a sevenfold reduction translates directly into an order-of-magnitude reduction in processing wall-clock time. Next, in time-series applications—agricultural phenology, surface water dynamics, urban growth—the model must be applied to each acquisition of the temporal stack, and the cumulative cost grows linearly with the number of revisits. Finally, in edge-deployed scenarios such as on-board processing for the next generation of Earth observation cubesats, the available compute budget is fixed and the architecture must be chosen to fit within it.

On the basis of these considerations, three deployment guidelines are proposed. (i) For research and ablation studies where reconstruction quality is the primary criterion and the training budget is not constrained, PanNet is recommended. The architecture occupies the Pareto-optimal corner of the joint quality–speed space and produces the lowest reference-free distortion. (ii) For high-throughput operational pipelines—routine production of pan-sharpened Landsat 9 mosaics, automated change detection at continental scale—DenseNet is recommended as a fast, structurally simple alternative that recovers approximately 95% of

PanNet’s *PSNR* and 98% of its *SSIM* at less than 40% of the per-epoch cost. (iii) Attention-Sharpen is not recommended for either scenario on Landsat 9 OLI-2 data: its quality is intermediate between PanNet and ResASPP, its cost is the highest among the five candidates, and the empirical evidence does not support the additional complexity.

5.3 Limitations and outlook

Three limitations of the reported experimental design merit explicit discussion: the reduced-resolution protocol of Wald yields a benchmark in which the reconstruction is evaluated at 30 m against a 30 m ground truth, and the generalisation to native 15 m output is inferred rather than directly measured. The reference-free metrics (QNR , D_i , D_s) provide a partial check on this generalisation, but they do not fully replace an ablation on additional independent scenes. Beyond that, the evaluation is conducted on a single scene (Path 175, Row 034, November 2025), which limits the sensitivity of the comparison to land-cover heterogeneity and atmospheric variability across the OLI-2 acquisition envelope. Finally, the seven-band assessment is constrained to the three visible multispectral channels and does not include the near-infrared or the short-wave infrared bands of OLI-2; the extension of the residual learning prior to a six- or seven-band reconstruction is technically straightforward but has not been tested here.

Three directions for follow-up work are indicated. (i) The replication of the benchmark on a multi-scene panel covering distinct land-cover regimes (urban, agricultural, forest, coastal) and seasonal acquisitions, with the patch-wise metric distributions analysed by stratified Wilcoxon. (ii) The extension of the inputs to the full OLI-2 multispectral cube (B1 to B7), with band-wise spectral fidelity metrics reported separately for the visible and infrared bands [20]. (iii) The replacement of the bilinear degradation kernel by a sensor-matched modulation transfer function (MTF), which would refine the Wald-consistency assumption and tighten the link between reduced-resolution validation and native-resolution deployment [15].

6. Conclusion

Five convolutional architectures were benchmarked for the pan-sharpening of Landsat 9 OLI-2 imagery under the reduced-resolution protocol of Wald. PanNet, which restricts its learning manifold to the high-frequency residual of the bilinearly upsampled multispectral input, attained $PSNR = 46.47$ dB, $SSIM = 0.9800$, $SAM = 0.617^\circ$, $ERGAS = 1.394$, $QNR = 0.9921$, $D_i = 0.0041$ and $D_s = 0.0038$, outperforming DCNN, ResASPP, DenseNet and Attention-Sharpen on every reported metric. Pairwise Wilcoxon signed-rank tests confirmed that the differences are significant at $p < 0.05$ against each baseline. The empirical superiority traces directly to the architectural prior of high-frequency residual learning, which matches the spectral coherence assumption underlying Wald’s protocol and confines the learning manifold to the band of detail that the panchromatic channel encodes. Mean absolute error heat maps over the test patch corroborate the scalar metrics: the PanNet reconstruction exhibits a uniformly darker and homogeneous error distribution, with no detectable edge ringing or halo. A per-epoch timing analysis revealed an approximately $9.3\times$ spread between the fastest network (DCNN, 1.18 s) and the slowest (Attention-Sharpen, 10.98 s), with PanNet occupying the Pareto-optimal corner of the quality–speed plane at 3.82 s. For operational pipelines that require sustained throughput at near-PanNet quality, DenseNet (1.49 s, $PSNR = 44.12$ dB) is identified as the recommended lightweight alternative. Attention-Sharpen is not justified by its computational footprint on Landsat 9 OLI-2 data at the spatial and spectral scales examined here.

These results also bear on high-resolution land-cover and precision-agriculture monitoring in mountainous terrain, where coarse native sampling limits field- and slope-scale detection [9], [10].

Data and code availability

The Landsat 9 OLI-2 scene `LC09_L1TP_175034_20251109_20251109_02_T1` is publicly distributed by the United States Geological Survey via the EarthExplorer portal. The benchmarking pipeline, the Wald-degradation routine, and the patch-export utility used in this study are implemented in PyTorch and are organised in the scripts `benchmark_ultimate_mt.py`, `degrade_mt_images.py` and `export_patches_mt.py`,

respectively. All hyperparameters, normalisation constants, and patch-extraction coordinates required for byte-level reproduction are reported in Sections 2.3 and 2.6 and in Algorithm 1.

Acknowledgements

Not applicable. No external funding was received for this work.

References

- [1] Wald, L., Ranchin, T., & Mangolini, M. (1997). Fusion of satellite images of different spatial resolutions: Assessing the quality of resulting images. *Photogrammetric engineering and remote sensing*, 63(6), 691-699.
- [2] Vivone, G., Alparone, L., Chanussot, J., Dalla Mura, M., Garzelli, A., Licciardi, G. A., ... & Wald, L. (2014). A critical comparison among pansharpening algorithms. *IEEE Transactions on Geoscience and Remote Sensing*, 53(5), 2565-2586
<https://doi.org/10.1109/TGRS.2014.2361734>
- [3] Masi, G., Cozzolino, D., Verdoliva, L., & Scarpa, G. (2016). Pansharpening by convolutional neural networks. *Remote Sensing*, 8(7), 594
<https://doi.org/10.3390/rs8070594>
- [4] Zhu, X. X., Tuia, D., Mou, L., Xia, G. S., Zhang, L., Xu, F., & Fraundorfer, F. (2017). Deep learning in remote sensing: A comprehensive review and list of resources. *IEEE geoscience and remote sensing magazine*, 5(4), 8-36.
<https://doi.org/10.1109/MGRS.2017.2762307>
- [5] Yang, J., Fu, X., Hu, Y., Huang, Y., Ding, X., & Paisley, J. (2017, October). PanNet: A deep network architecture for pan-sharpening. In *2017 IEEE international conference on computer vision (ICCV)* (pp. 1753-1761). IEEE.
<https://doi.org/10.1109/ICCV.2017.193>
- [6] Chen, L. C., Papandreou, G., Kokkinos, I., Murphy, K., & Yuille, A. L. (2017). Deeplab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected crfs. *IEEE transactions on pattern analysis and machine intelligence*, 40(4), 834-848.
<https://doi.org/10.1109/TPAMI.2017.2699184>
- [7] Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017, July). Densely connected convolutional networks. In *2017 IEEE conference on computer vision and pattern recognition (CVPR)* (pp. 2261-2269). Ieee.
<https://doi.org/10.1109/CVPR.2017.243>
- [8] Woo, S., Park, J., Lee, J. Y., & Kweon, I. S. (2018, September). Cbam: Convolutional block attention module. In *European conference on computer vision* (pp. 3-19). Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-01234-2_1
- [9] Weiss, M., Jacob, F., & Duveiller, G. (2020). Remote sensing for agricultural applications: A meta-review. *Remote sensing of environment*, 236, 111402.
<https://doi.org/10.1016/j.rse.2019.111402>
- [10] Zhao, S., Tu, K., Ye, S., Tang, H., Hu, Y., & Xie, C. (2023). Land use and land cover classification meets deep learning: A review. *Sensors*, 23(21), 8966.
<https://doi.org/10.3390/s23218966>
- [11] Deng, L. J., Vivone, G., Paoletti, M. E., Scarpa, G., He, J., Zhang, Y., ... & Plaza, A. (2022). Machine learning in pansharpening: A benchmark, from shallow to deep networks. *IEEE Geoscience and Remote Sensing Magazine*, 10(3), 279-315.
<https://doi.org/10.1109/MGRS.2022.3187652>

- [12] Yuhas, R. H., Goetz, A. F., & Boardman, J. W. (1992, June). Discrimination among semi-arid landscape endmembers using the spectral angle mapper (SAM) algorithm. In *JPL, summaries of the third annual JPL airborne geoscience workshop. volume 1: AVIRIS workshop*.
- [13] Wald, L. (2002). *Data fusion: definitions and architectures: fusion of images of different spatial resolutions*. Presses des MINES.
- [14] Alparone, L., Aiazzi, B., Baronti, S., Garzelli, A., Nencini, F., & Selva, M. (2008). Multispectral and panchromatic data fusion assessment without reference. *Photogrammetric Engineering & Remote Sensing*, 74(2), 193-200.
<https://doi.org/10.14358/PERS.74.2.193>
- [15] Khan, M. M., Alparone, L., & Chanussot, J. (2009). Pansharpening quality assessment using the modulation transfer functions of instruments. *IEEE transactions on geoscience and remote sensing*, 47(11), 3880-3891.
<https://doi.org/10.1109/TGRS.2009.2029094>
- [16] Wilcoxon, F. (1945). Individual comparisons by ranking methods. *Biometrics bulletin*, 1(6), 80-83.
<https://doi.org/10.2307/3001968>
- [17] Masek, J. G., Wulder, M. A., Markham, B., McCorkel, J., Crawford, C. J., Storey, J., & Jenstrom, D. T. (2020). Landsat 9: Empowering open science and applications through continuity. *Remote Sensing of Environment*, 248, 111968.
<https://doi.org/10.1016/j.rse.2020.111968>
- [18] Landsat, U. S. G. S. (2022). Data Users Handbook Landsat 9 Data Users Handbook Version 1.0. *USGS: Washington, DC, USA*, 107.
- [19] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*.
- [20] G. Vivone, “Multispectral and hyperspectral image fusion in remote sensing: A survey,” *Information Fusion*, vol. 89, pp. 405–417, 2023.
<https://doi.org/10.1016/j.inffus.2022.08.032>

Neural Interaction Between Learners and Artificial Intelligence Through the Lens of Fallacies

Farhad Shafiepour Motlagh¹  and Sabina Mirzaei Nobari² 

¹Department of Educational Administration, Maha. C, Islamic Azad University, Mahallat, Iran

²Department of Information Technology, Western Caspian University, Baku, Azerbaijan

Received: 01.09.2026

Accepted: 28.09.2026

Published: 09.10.2026

<https://doi.org/10.54414/DPII.2371>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: The rapid expansion of large language models and generative artificial intelligence systems in educational ecosystems has moved learner-machine interaction beyond a merely instrumental interface toward cognitive entanglement and neural stimulation. Adopting a phenomenological and critical approach, this qualitative study explores learners' neural-cognitive engagement with fabricated content arising from "AI hallucination" and its implications for the reproduction of epistemological fallacies. The research involved in-depth semi-structured interviews with higher education learners and participant observation of AI-assisted problem-solving processes. The resulting data were interpreted through inductive thematic analysis. The findings indicate that, when confronted with algorithmic error, learners' cognitive processing develops an "artificial confidence bias" under the influence of AI's coherent linguistic structure and persuasive tone. By providing rapid access to seemingly complete answers, this process satisfies the neural dopaminergic reward circuit and consequently suspends cognitive inhibition and critical reflection. The extracted themes revealed that learners' neural interaction with generative AI hallucinations, through six fallacies—formal eloquence, artificial authority, immediate relief, part-to-whole generalization, anthropomorphic analogy, and confirmatory conformity—transforms human agency into cognitive passivity and erodes critical judgment through artificial confidence bias. This epistemic erosion reduces truth to statistical rhetoric and can be mitigated and remedied only through a transition from reward-driven consumption to reflective pedagogy and relational ethics.

Keywords: Learners' neural interaction; artificial intelligence; hallucination-related fallacies

1. Introduction

The structural transformations brought about by the emergence and accelerating penetration of generative AI and large language models into higher education ecosystems have profoundly altered academic learning and research. "Learners' neural interaction with artificial intelligence based on hallucination-related fallacies" denotes a complex, interdisciplinary condition at the intersection of cognitive neuroscience, critical epistemology, and pedagogy.

Learners' neural interaction with artificial intelligence based on hallucination-related fallacies refers to "a dynamic, bidirectional process in which structural errors and imaginary data reproduced by large language

models (AI hallucination), through coherent linguistic structure, eloquent expression, and rapid responsiveness, manipulate information-processing mechanisms in the learner's brain. By stimulating dopaminergic reward circuits and producing cognitive ease, this process suspends analytical thinking and cognitive inhibition in the prefrontal cortex, leading learners to accept false propositions unconsciously through six reasoning traps (fallacies)."

Student-machine interaction no longer appears merely as a neutral user interface or computational tool, but as a form of neural-cognitive entanglement and epistemic intermingling. One fundamental and unresolved challenge in using these technologies is AI hallucination: a condition in which a system reproduces fabricated or invalid propositions, imaginary sources, or fictitious data with flawless textual coherence, fluent language, and a thoroughly persuasive tone [1], [2]. The central challenge arises when this technical characteristic intersects with learners' biological structures and neural decision-making circuits.

When encountering AI-generated text, the learner's brain enters a state of cognitive ease because of conceptual fluency and syntactic refinement. According to dual-process theory, this process suspends prefrontal activity and System 2 inhibitory mechanisms, shifting the processing burden to System [3]. Combined with exceptionally rapid responses, this ease of processing stimulates the neural dopaminergic reward circuit by immediately alleviating the anxiety of not knowing or having insufficient time [4]. This technological-neural overlap produces an "artificial confidence bias": an error that leads the knowing subject to equate the machine's statistical hallucination with genuine understanding and to slip into analytical passivity.

This process draws learners into a chain of epistemological and neural fallacies: formal eloquence in place of substantive truth, appeal to artificial algorithmic authority, false neural causation based on immediate relief, generalization from a fabricated part to the truth of the whole, Anthropomorphic analogy applied to mathematical mechanisms, and confirmatory conformity within algorithmic sycophancy [5], [6]. Instead of engaging with the constructive difficulty of scientific discovery and tolerating unresolved questions in research, learners become trapped in a cycle of hurried reward-seeking that blurs the boundary between authentic empirical reasoning and algorithmic imagination. The central problem of this study is therefore to explain how the technical defect of hallucination becomes a syndrome of cognitive erosion through the reproduction of mental fallacies in academic life.

The importance of this issue emerges from three interconnected domains: epistemology, pedagogy, and neuroethics. In the first, higher education fundamentally rests on the pursuit of truth, critical reflexivity, and the authenticity of evidence. If interaction with language models turns eloquence into a criterion of correctness, truth is reduced from correspondence with reality or internal coherence to "syntactic beauty and the speed of text generation." This destabilizes rational scrutiny and increases the risk of disseminating structured pseudoscience in research.

Pedagogically, deep learning is inherently connected to cognitive friction, methodological doubt, and patience in the face of ambiguity. Conditioning learners' neural structures to immediate dopaminergic gratification erodes mental resilience in confronting the difficulties of authentic research and turns learners into passive operators who merely consume prefabricated content.

From the perspective of neuroethics and organizational ethics, delegating scientific judgment to opaque black-box systems not only undermines students' ethical responsibility for their claims but also transforms authentic human dialogue in education into a false, monologic, and hegemonic relationship with a tool [7], [8]. Understanding the mechanisms of this intellectual captivity is therefore a prerequisite for context-sensitive policymaking, professional ethics, and curriculum redesign in the age of AI.-

The literature indicates that most research on AI hallucination has focused on technical dimensions, prompt engineering, and statistical parameter adjustment [2]. Studies of its educational consequences, meanwhile, have generally remained within quantitative approaches, superficial behavioral measurement, or optimistic technophilic attitude surveys [9]. Three fundamental gaps can be identified.

First, earlier research has largely treated AI as a learning aid and neglected its disruptive role in learners' psychological–neural economy. The relationship between brain reward circuits (the dopaminergic pathway) and the suspension of scrutiny when encountering algorithmic error has rarely been formulated in educational studies.

Second, machine hallucination is usually treated as an isolated erroneous output rather than a generative context for reproducing patterns of human mental deception. A structured qualitative account of interaction-generated fallacies, such as susceptibility to eloquence, false neural causation, and algorithmic sycophancy, has been missing from higher education theory.

Third, students' lived experiences when encountering hallucinated data, their movement toward false confidence, and their transformation from knowing subjects into passive agents require qualitative investigation immersed in learners' lifeworlds. These dimensions are not usually captured by conventional questionnaires.

To address these gaps, this study offers specific epistemic and methodological distinctions from comparable research. Moving beyond one-dimensional engineering studies or superficial educational descriptions, it analyzes hallucination at the intersection of neural brain responses, reasoning and fallacy, and epistemic power structures, providing a multilayered examination of the learner's mind.

The study avoids uncritical praise of algorithmic efficiency. By questioning the reduction of the human subject to an optimized consumer, it emphasizes the restoration of critical reflexivity and a clear distinction between machine-generated statistical rhetoric and authentic, truth-oriented human knowledge.

A distinctive strength of this research is its thematic abstraction and formulation of six coherent types of fallacy from empirical data. This structures the invisible connection between the technical architecture of language models and human cognitive traps into a practical analytical matrix.

Moving beyond small-scale quantitative data, the research explores learners' perceptual experiences in direct encounters with the system. It inductively documents the psychological–neural mechanisms leading to artificial confidence bias from within academic lifeworlds, opening possibilities for higher education policymakers to develop critical pedagogy and redesign learning assessment.

2. Literature Review

A review of international research published between 2020 and 2026 indicates that educational technology and cognitive neuroscience research has rapidly shifted from the instrumental usefulness of AI toward the neural–cognitive pathology of learner interaction with large language models and the mechanisms of fallacious acceptance of distorted outputs. Early theoretical and empirical foundations emerged with Bender et al.'s (2021) warning about “stochastic parrots.” They explained that large language models connect texts based on statistical distributions, while their deceptive eloquence traps learners in the fallacy of formal eloquence and encourages the projection of awareness and conceptual understanding onto the system. Extending this argument, laboratory studies in cognitive neuroscience showed that textual fluency breaks down cognitive resistance in the prefrontal cortex. Drawing on resource-rationality theory, Lieder et al. (2020) demonstrated that the human brain continually seeks to reduce metabolic energy consumption. By facilitating sensory–cognitive perception, fluent AI output creates a “correct answer” signal in the evaluation circuit, suspending System 2 (effortful analytical thinking) and producing unquestioning trust even in fabricated propositions.

As tools such as ChatGPT became widespread in academic settings, Casper et al. (2023) investigated submission to the fallacy of appeal to artificial authority. Their findings showed that school and university students attribute excessive omniscience to algorithms because of the alignment bias generated by bots' assertive, unhesitating tone, internalizing unreal or hallucinated data without validation. Di Mario et al. (2024) investigated the neurobiological dimensions using electroencephalography (EEG) and functional

magnetic resonance imaging (fMRI). Their findings indicated that rapid, integrated AI responses significantly reduce activity in the executive control network, including the dorsolateral prefrontal cortex (DLPFC) and anterior cingulate cortex, while stimulating striatal dopaminergic circuits through rapid, effortless cognitive rewards. This process underlies the fallacy of false neural causation, in which early dopamine release and relief from problem-solving-related academic anxiety are mistakenly interpreted as genuine learning and deep understanding.

Furthermore, Bostrom and Shulman (2024) and Greene and Foster (2025) examined students' interpretive and analogical mechanisms empirically. They found that error-free machine performance in a limited domain is rapidly extended to all scientific domains through the part-to-whole generalization fallacy, as learners equate limited text-processing analytical capacity with comprehensive knowledge. Bynum et al. (2025) also showed, through analysis of interactive exchanges, that chatbots' first-person and ostensibly polite responses encourage the projection of mental states and activate the anthropomorphic analogy fallacy within learners' social cognition. The adolescent brain consequently encodes the computational algorithm as an "aware and caring peer" and responds to its hallucinations with justification, accommodation, and tolerance.

In the most advanced recent studies, Peterson, Duke, and Steinberg (2026) examined the erosion of metacognitive monitoring and the intensification of confirmatory conformity in a longitudinal neuroeducational trial. They observed that learners confronted with obvious system errors and hallucinations adjusted their thinking to AI's mistakes instead of critically reconsidering them. To reduce cognitive dissonance, they equated machine errors with inadvertent human mistakes through the "you too" fallacy. Collectively, these studies suggest that uncritical reliance in learner–AI neural interaction creates a cognitive–dopaminergic trap in which machine-generated statistical hallucinations suppress critical thinking through structured fallacies and erode learners' mental agency.

3. Research Questions

1. What are the dimensions and components of an analysis of learners' neural interaction with artificial intelligence through the lens of fallacies?
2. What framework can be developed to analyze learners' neural interaction with artificial intelligence through the lens of fallacies?

4. Research Methodology

This study adopted a qualitative interpretive–critical paradigm and a descriptive–interpretive phenomenological strategy (hermeneutic phenomenology). Learners' encounters with fabricated and hallucinated AI outputs are subjective, contextual, and intertwined with neural–cognitive and emotional structures. Phenomenology therefore enables the identification and deconstruction of the underlying, unarticulated layers of learners' lifeworlds and the meanings they assign to interaction with algorithms and to justifications of algorithmic errors. The critical perspective allowed the researcher to move beyond description and interrogate asymmetrical epistemic power relations, the prevalence of cognitive fallacies, and prefrontal passivity under the dominance of technological formal eloquence.

5. Research Setting and Data Collection

The research setting comprised postgraduate students at comprehensive public universities and Islamic Azad University who regularly used generative large language models each week for research and problem-solving. Criterion-based purposive sampling sought maximum experiential variation across the humanities, basic sciences, and engineering. Sample size was determined by theoretical saturation: participants were recruited until the final interviews yielded no new open codes or conceptual themes and information became

repetitive. Saturation was reached with the nineteenth participant; recruitment continued to twenty-one participants to ensure completeness.

Data collection included in-depth semi-structured interviews addressing experiences of AI errors, dopaminergic feelings associated with eloquent responses, review mechanisms, forms of projection, and justifications of fallacies. Interview transcripts and observation protocols were analyzed through inductive thematic analysis inspired by Braun and Clarke's multistage model. First, the data were read word by word to develop an overall understanding. Initial codes (basic themes) were then extracted from explicit statements and their neural–cognitive implications. Next, codes were grouped into broader concepts to form organizing themes. Finally, abstraction and conceptual synthesis generated global themes explaining the architecture of learners' projections and fallacies. To establish research quality and scientific trustworthiness, the study used Guba and Lincoln's (1985) qualitative trustworthiness framework and its four components rather than traditional quantitative validity and reliability concepts.

6. Discussion and Conclusion

Analysis of the qualitative data reveals that learners' interaction with generative AI extends beyond technological use to a transformation in cognitive economy and neural decision-making circuits. Encounters with fabricated outputs, or AI hallucination, create an asymmetrical connection between human cognitive psychology and machine-generated statistical probabilities. The following discussion examines each global theme identified in the six analytical tables in relation to relevant theoretical foundations and previous research, identifying points of convergence and divergence.

Regarding formal eloquence in place of substantive truth, the findings indicate that polished sentence structures, precise punctuation, and the machine's authoritative tone produce perceptual fluency in the prefrontal cortex. When information is processed with minimal cognitive friction, neural inhibition and methodological skepticism are suspended; fluency of form consequently replaces propositional truth.

Convergence with previous research: This finding is consistent with Kahneman's (2011) dual-process theory and the principle of cognitive ease. The brain tends to accept fluently processed texts automatically through System 1 while conserving System 2 effort. Bender et al.'s (2021) work on stochastic parrots and Pennycook and Rand's (2020) research on acceptance of pseudoscientific claims through fascination with lexical structure also support this finding [10].

Divergence and critical perspective: The finding conflicts with assumptions in conventional media literacy paradigms and some traditional defenses of AI in education [9], according to which learners would immediately detect and reject machine errors because of their artificial character. Our findings reveal that, in recent language models, AI's rhetorical beauty not only fails to facilitate error detection but deliberately conceals errors.

For appeal to artificial authority, or presumed algorithmic omniscience, the data indicate a collapse of epistemic agency and analytical alienation among students. By attributing infallibility and statistical comprehensiveness to algorithms, learners abandon their position as self-aware subjects and become mere consumers of manufactured propositions. This epistemic submission prevents critical engagement with fabricated references and machine-generated data.

Convergence with previous research: This theme aligns with automation bias as discussed by Parasuraman and Manzey (2010), Zuboff's (2019) critique of the epistemic hegemony of computational systems, and Pinto et al.'s (2023) examination of elite submission to big data.

Divergence and critical perspective: This result directly challenges theories of human–machine collaborative learning and Siemens's (2005) connectivist ideas, which regard technology as facilitating an equitable redistribution of epistemic power [11]. The present findings indicate that hallucination-producing AI does not foster cognitive empowerment; instead, it creates debilitating dependence and an illegitimate concentration of authority within the algorithmic black box.

For false neural causation, or the immediate relief error, the findings show that immediate, definitive AI answers rapidly satisfy the learner's dopaminergic reward circuit. This instantly relieves the strain of not knowing or research anxiety. Learners conflate emotional relief and the calm of task completion with scientific adequacy and content accuracy, accepting the delivered hallucinations as certain.

Convergence with previous research: These results align with cognitive neuroscience findings concerning uncertainty reduction and the role of dopamine release in relieving doubt-related tension [4]. They also converge with Sparrow et al.'s (2011) research on Google's effects on cognitive laziness and false satisfaction through mental closure [12].

Divergence and critical perspective: These findings challenge technology-based inquiry learning approaches that assume faster access to answers frees time for deeper reflection. The qualitative evidence indicates that immediate access destroys the conditions for deep reflection in favor of premature pleasure in finishing the task.

For generalization from a fabricated part to the truth of the whole, the findings show that generative AI traps learners in the familiarity heuristic by embedding genuine keywords, book titles, or theorists' names within fabricated theories or data. After verifying a single reference or minor proposition, learners hastily validate the entire unreliable structure. This conclusion is consistent with Nisbett and Wilson's (1977) halo effect and models of anchoring bias in educational decision-making [13]. It also aligns with Ji et al.'s (2023) research on hallucination architecture in language models, indicating that hallucinations become more persuasive when mixed with factual information. This result contradicts the assumption of a discerning learner in self-regulated learning models [14], which presumes that postgraduate students can filter inconsistent and false information by checking part of the data. Our qualitative findings instead indicate that the correct fragment provides cover for extending and justifying subsequent fabrications.

For anthropomorphic analogy, the findings reveal that learners attribute subjective awareness, genuine understanding, and moral honesty to the system. Algorithmic apologies and empathetic feedback lead learners to interpret hallucination as an inadvertent, well-intentioned machine mistake rather than an inherent limitation of statistical next-token prediction. This finding aligns with Reeves and Nass's (1996) Computers Are Social Actors (CASA) theory and Turkle's (2021) critiques of artificial empathy [15]. Shanahan's (2024) studies of the illusion of understanding in language systems likewise support the identification of students' erroneous attribution of meaningful agency to processes without a lifeworld [16]. This insight conflicts with transhumanist and eliminative materialist perspectives that reduce the distinction between machine processing and human thought to computational capacity. Our results establish that conflating the two produces an emotional-epistemic trap rather than an epistemic leap, drawing learners into imagined emotional reciprocity.

For confirmatory conformity, or wishful thinking bias, the findings show that training based on human feedback and the tendency to please users (sycophancy) lead generative AI to align outputs with prompt assumptions. Learners are pleased by imaginary propositions that confirm their personal biases and enter a shared cycle of human-algorithm self-deception. This result aligns with Wason's (1960) classic work on confirmation bias and Perez et al.'s (2022) contemporary research on sycophantic behavior in AI models [17]. It indicates that systems tend to sacrifice truth to conformity with the user's viewpoint. The finding contradicts the traditional idea that technology enables Popperian falsification and escape from personal echo chambers. Hallucination-producing AI becomes a catalyst for sanctifying pre-existing biases instead of a tool for intellectual challenge.

7. Final Conclusion and Policy and Pedagogical Implications

Taken together, the findings from the six analytical tables indicate that hallucination in AI systems is not merely a glitch or transient technical defect. Within neural-cognitive interactions with learners, it becomes a syndrome of epistemic erosion. Reducing critical thinking to immediate synaptic gratification and

sacrificing propositional truth to the eloquence of statistical rhetoric empties the academic knowing subject of its identity.

Addressing this challenge requires a multifaceted redesign of higher education in the age of AI:

1. Transition to relational ethics and critical reflexivity: Pedagogy must move learners away from submissive consumption of fluent answers and restore their sensitivity to the gap between linguistic form and epistemic truth.
2. Teach falsification literacy and stop rewarding speed: University assessment should focus on the friction-filled research process, engagement with disconfirming evidence, and detection of fabrication, rather than the production of polished texts in the shortest possible time.
3. Remove the sanctification and anthropomorphism of machines: Curricula should teach the epistemological foundations of language-model operation so that students understand these systems as mechanical processes based on statistical fitting, inherently lacking experience, understanding, and commitment to truth, rather than as omniscient authorities or dialogue partners.

References

- [1] Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM FAccT Conference* (pp. 610–623). Association for Computing Machinery.
<https://doi.org/10.1145/3442188.3445922>
- [2] Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Yan, Y., Ishii, E., Bang, Y. J., Dai, W., Madotto, A., & Fung, P. (2023). Survey of hallucination in natural language generation. *ACM Computing Surveys*, 55(12), 1–38.
<https://doi.org/10.1145/3571730>
- [3] Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- [4] Schultz, W. (2016). Dopamine reward prediction-error signalling: A two-component response. *Nature Reviews Neuroscience*, 17(3), 183–195.
<https://doi.org/10.1038/nrn.2015.26>
- [5] Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors*, 52(3), 381–410
<https://doi.org/10.1177/0018720810376055>
- [6] Perez, E., Ringer, S., Lukošūtė, K., Nguyen, K., Chen, E., Heiner, S., Pettit, S., Esiobu, D., Durmus, E., & Bowman, S. R. (2022). Discovering language model behaviors with model-written evaluations. *arXiv preprint arXiv:2212.09251*.
- [7] Turkle, S. (2021). *The empathy diaries: A memoir*. Penguin Press.
- [8] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- [9] Luckin, R. (2018). *Machine learning and human intelligence: The future of education in the 21st century*. UCL Institute of Education Press.
- [10] Pennycook, G., & Rand, D. G. (2020). Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytical thinking. *Journal of Personality*, 88(2), 185–200.
<https://doi.org/10.1111/jopy.12476>
- [11] Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology and Distance Learning*, 2(1), 3–10.
- [12] Sparrow, B., Liu, J., & Wegner, D. M. (2011). Google effects on memory: Cognitive consequences of having information at our fingertips. *Science*, 333(6043), 776–778.
<https://doi.org/10.1126/science.1207745>

- [13] Nisbett, R. E., & Wilson, T. D. (1977). The halo effect: Evidence for unconscious alteration of judgments. *Journal of Personality and Social Psychology*, 35(4), 250–256.
<https://doi.org/10.1037/0022-3514.35.4.250>
- [14] Zimmerman, B. J. (2002). Becoming a self-regulated learner: An overview. *Theory Into Practice*, 41(2), 64–70.
https://doi.org/10.1207/s15430421tip4102_2
- [15] Reeves, B., & Nass, C. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. Cambridge University Press.
- [16] Shanahan, M. (2024). Role play with large language models. *Nature*, 626(7999), 493–498.
<https://doi.org/10.1038/s41586-023-06647-8>
- [17] Wason, P. C. (1960). On the failure to eliminate hypotheses in a conceptual task. *Quarterly Journal of Experimental Psychology*, 12(3), 129–140.
<https://doi.org/10.1080/17470216008416717>

A Rule-Based Framework for Assessing Industrial Applicability

Alikhan Rzaguliyev ✉ 

Department of Information Technologies, Western Caspian University, Baku, Azerbaijan

Received: 05.08.2026

Accepted: .03.09.2026

Published: 09.10.2026

<https://doi.org/10.54414/KQWH4828>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: Patent searches are conducted in multiple independent databases. In addition, it is necessary to mention that patent search identifies the novelty and inventive step criteria among the criteria of patentability. Hence, the model of patent search cannot define the industrial application criterion. As can be seen, the proposed structure clearly illustrates how the industrial applicability evaluation may be performed based on a series of predefined rules. In contrast to machine learning algorithms, which require large amounts of data, the offered approach may rely solely on legal and scientific criteria already used by patent offices in practice. The proposed framework enables different types of automation in conducting patent evaluations: Fully Automated systems; Semi-Automated systems; Partially automated systems. Using rule-based algorithms enables providing an explanation for each step made by the system.

Keywords: Patentability, industrial application, artificial intelligence, patentability evaluation, automation, system modeling

1.Introduction

The patent search in the Patent and Trademark Center of the Intellectual Property Agency of the Republic of Azerbaijan is carried out in several independent databases. These databases are the Azerbaijani Patent Database, FIPS, EAPATIS, PATENTSCOPE, Espacenet, USPTO, and Google Patents, among others [1], [2], [3], [4], [5], [6], [7]. Each database is to be accessed individually, and the search query has to be formulated and executed individually for each database. But it also needs to be noted that patent search only finds novelty and inventive step as criteria of patentability.

Analysis of patent applications usually presupposes checking compliance with three main requirements for the patentability of inventions: industrial applicability, novelty, and inventive step. In relation to the latter two requirements, much effort has been put into studying the potential for automating the search for relevant prior art using methods such as artificial intelligence, machine learning, natural language processing, and information retrieval systems. Nevertheless, there has not been so much attention paid to the problem of automation of industrial applicability analysis.

Industrial applicability is one of the basic patentability requirements in many countries, among which there is the Republic of Azerbaijan. Typically, before considering novelty and inventive step, patent examiners assess whether the claimed invention may be produced or applied in some area of industry. The task involves technical knowledge and reasoning about how the invention works. Existing patent search automation systems primarily focus on information retrieval and prior-art identification. Such systems assist examiners in finding relevant documents but generally do not evaluate whether an invention is capable of

industrial application. As a result, industrial applicability assessment remains largely dependent on human expertise.

In this paper, we present a rule-based approach to the evaluation of industrial applicability of inventions. The proposed rule-based approach is formulated as a decision support system that can be included in the automated/semi-automated systems of patent examination. Contrary to machine learning algorithms, our approach uses explicit rules based on patent legislation, scientific knowledge, and patent examination processes. The purpose of our rule-based system is to assist patent officers in determining the industrial applicability of inventions. The goal of the research is to construct the methodological basis for industrial applicability evaluation that can be used in the process of patentability examination under Azerbaijani patent legislation.

2. Literature review

Under the patent law of Azerbaijan, three types of patentable subject matter are recognized: inventions, utility models, and industrial designs. In the context of inventions, three fundamental patentability requirements are set. First, the requirement of novelty indicates that the subject matter of the invention should not be part of the prior art. Second, the invention should represent an inventive step, which indicates that the invention should not be obvious to a person skilled in the art. Third, the invention should be capable of industrial application, meaning that the invention can be produced or used in industry or in any other sector of the economy [8]. Utility models also have similar legislation. However, they can only be devices and require two criteria of patentability. These are industrial application and novelty [8].

A similar framework is in place in the Russian Federation. According to their Civil Code, patent protection is granted for inventions, utility models, and industrial designs [9]. The patentability criteria for an invention in the Russian Federation are similar to those in Azerbaijan, i.e., novelty, inventiveness, and industrial applicability. Similarly, in the Russian Federation, utility models can also only be devices and require two criteria of patentability: industrial application and novelty [8].

Under the current system of examination, the search for prior art documents is conducted based on combinations of IPC codes and keyword searches. Once the potentially relevant documents are identified, the impact of these documents on patentability is evaluated, and a conclusion is drawn. In most cases, the results of the evaluation are of three types: the documents do not influence patentability; the documents indicate a lack of inventive step; or the documents indicate a lack of novelty [10]

The methodology adopted in the present study is based on the above principles but aims at incorporating automation in the evaluation process. It is based on the patent databases currently in use and thus depends on the structure of these databases. The evaluation methodology is restricted to mechanical inventions, specifically device-related patents, in order to limit the scope of evaluation and make the results consistent. To make the evaluation methodology more formalized, three classes of documents are defined: A (generally relevant documents), Y (documents indicating lack of inventive step), and X (documents indicating lack of novelty) [10].

Moreover, the model includes a keyword similarity component based on synonyms. This can be achieved by a structured database in which terms are provided with similarity weights. In such a system, for instance, semantically related terms such as different technical terms can be connected in a table of similarity, thus facilitating a more flexible matching in the search procedure [10].

For a semantic-based retrieval system, the proposed system provides a patentability analysis using a three-stage process of query refinement. In the first stage, it identifies technical entities that are represented in noun-based keywords. In the second stage, it extends these keywords to include descriptive modifiers that identify attributes of an invention. In the third stage, it extends these keywords to include configuration-related expressions that identify relationships between various components of an invention, which are often logical in nature as found in patent claims [10].

The thresholds can be set based on expert opinion or by deriving them empirically. One such method of deriving thresholds could be by aggregating the opinions of patent experts and then normalizing the scale to obtain an average threshold based on the actual examination procedure [10]. The problem here is that the model finds novelty and inventive step. The model still lacks industrial application evaluation. Hence, using a framework for industrial application evaluation would be required.

Another paper discusses types of automation that could be deployed for patentability evaluation. The paper discusses the three main types of automation: fully automated, semi-automated, and partially automated systems. Where fully automated system doesn't need human examiner input, semi-automated system requires human examiner validation, and partially automated system automates the process based on examiner input [11]. Although the authors describe the algorithms for patentability evaluation and mention the model would check industrial application, the framework of evaluation of the said criterion is not mentioned [11].

3. Methodology

- General framework for evaluating industrial application:
- The proposed framework consists of four primary stages: Claim analysis; Technical domain identification; Rule-based industrial applicability assessment; Human examiner verification.
- The framework is intended to function as a component of an automated patentability examination system. Its purpose is not to replace patent examiners (depending on the type of automation) but to provide preliminary assessments that can support examination procedures.
- Stage 1: Claim Analysis: The system receives input from patent documentation, including: Claims; Description; Drawings; Abstract.
- Natural language processing techniques may be utilized to identify technical features, technical effects, structural components, and functional relationships described in the invention or utility model. For example, if an application describes a hydraulic turbine, the system would identify features such as blades, rotor, shaft, fluid flow, and power generation. Based on that, the system might also flag unrelated keywords based on IF-THEN rules and the type of automation.
- Stage 2: Technical Domain Identification: After extracting technical features, the system determines the relevant technological domain through IPC classification. The system would check if technical terms match the IPC codes. For example, an IPC code could be F16H 1/02 - Toothed gearing for conveying rotary motion, without gears having orbital motion [12]. However, the application could be in the field of chemistry. Therefore, the system would flag it and, based on the automated system deployed (described in [11]), would determine industrial application. The identified domain determines which scientific and technical rules will be applied during industrial applicability assessment.
- Stage 3: Rule-Based Assessment: The proposed system utilizes a knowledge base containing legal rules, technical rules, and scientific rules.

Examples of legal rules include:

Rule 1:

IF the application contains identifiable technical features
THEN continue examination.

Rule 2:

IF the application lacks sufficient technical disclosure

THEN request clarification from the applicant.

Examples of scientific rules include:

Rule 3:

IF the application violates established laws of physics

THEN industrial applicability = NO.

Rule 4:

IF the application requires perpetual motion without an external energy source

THEN industrial applicability = NO.

Rule 5:

IF the application cannot be reproduced using the disclosed information

THEN industrial applicability = NO.

Examples of technical rules include:

Rule 6:

IF the application contains identifiable components, operational mechanisms, and expected technical effects

THEN industrial applicability = YES.

Rule 7:

IF the application can be manufactured using existing or reasonably foreseeable technologies

THEN industrial applicability = YES.

Rule 8:

IF the application can be repeatedly utilized within an industrial environment

THEN industrial applicability = YES.

Knowledge Base Structure:

The knowledge base is made up of: Scientific databases; Technical standards; Patent databases; Engineering sources; Legal regulations; Rules generated by examiners.

The system may employ specialized knowledge depending on the IPC classification detected at Stage 2.

Stage 4: Verification by Humans. Please note that this stage will not be considered for an entirely automated system.

The final decision will always remain with the patent examiner. The system supplies: Activations of rules; Evidence; Rationale behind decisions.

4. Findings and Results

As one can see from the proposed framework, industrial applicability assessment can be expressed via a certain set of rules. In contrast to machine learning methods, which need to work on large amounts of data for learning purposes, the proposed solution can be developed based on the current set of requirements and laws applied by patent examiners.

There are different types of patent examinations that can be automated using the proposed framework: Fully automated systems; Semi-automated systems; Partially automated systems. One of the major advantages of

the proposed method is that the use of rules allows providing explanations for each decision made. It is very important because any legal decision has to be accompanied by an appropriate justification.

It is also possible to apply specialization based on the technical field of interest using the proposed framework. For example, linking industrial applicability rules to IPC classes will enable applying scientific knowledge specific to a certain domain.

The analysis of perpetual motion devices proves that the proposed framework can be really useful for patenting. Indeed, such devices break physical laws, and thus the lack of industrial applicability can be recognized without making a patent search.

5. Limitations

- Several considerations should be mentioned here. First, evaluation of applicability in industry is based on complex scientific and technical considerations, which are not necessarily represented by pre-defined rules and may necessitate constant growth of the knowledge base.
- Second, applicability assessment is dependent on the quality of patent documents; incomplete information can cause an error in assessment.
- Third, the scientific knowledge base changes over time. Thus, the rules need to be regularly updated according to new discoveries in science and technology.
- Fourth, there might be situations when a certain degree of subjectivity is needed. Thus, the proposed framework should not be taken as a substitute for a patent examiner, but rather as an advisory tool.
- And finally, at the moment, this study presents only a theoretical model, without extensive empirical validation using real data from patents. Future research could provide such validation.

Author Contributions

The sole author is responsible for conceptualizing, collecting, and analyzing data, and writing and editing the manuscript

Conflict of Interest

The authors declare no conflicts of interest

Funding

This study received no external funding

References

- [1] Azerbaijan Patent Database. (n.d.). *Azerbaijan Patent Database* [Closed-access database].
- [2] ФИПС (FIPS), Patent Database
<https://www.fips.ru/iiss/search.xhtml>
- [3] ЕАПАТИС (EAPATIS), Patent Database
<http://www.eapatis.com/>
- [4] PATENTSCOPE, Patent Database
<https://patentscope.wipo.int/search/en/search.jsf>
- [5] Espacenet, Patent Database
<https://worldwide.espacenet.com/patent/search>
- [6] USPTO, Patent Database
<https://ppubs.uspto.gov/pubwebapp/>
- [7] Google Patents, Patent Database
<https://patents.google.com>
- [8] Azərbaycan Respublikasının “Patent haqqında” Qanunu. (n.d.).
[https://patent.copat.gov.az/files//26290292722835030361312-IQ%20Patent%20haqq%C4%B1nda%20\(2\).pdf](https://patent.copat.gov.az/files//26290292722835030361312-IQ%20Patent%20haqq%C4%B1nda%20(2).pdf)

- [9] Civil Code of Russian Federation, Part four, Art. 1349 – 1352
- [10] Rzaguliyev, A. (2025, April 28). Automation of a patentability search using mathematical models based on weighted key terms [Conference presentation]. II Congreso Internacional Inteligencia Artificial, Innovación, Economía y Empresa.
<https://ciecem.org/ponencia/automation-of-a-patentability-search-using-mathematical-models-based-on-weighted-key-terms/>
- [11] Rzaguliyev, A., & Muradli, K. (2025, December 3). Automation of patentability for inventions [Conference presentation]. International Academic Symposium on New Research Methodologies and Modern Models of Industry-Academia Collaboration in Computer Science.
- [12] World Intellectual Property Organization. (2024). IPC publication.
<https://ipcpub.wipo.int/?notion=scheme&version=20250101&symbol=none&menulang=en&lang=en&viewmode=f&fipcpc=no&showdeleted=yes&indexes=no&heading>

Mathematical Integer Linear Programming Model for Optimal Placement of Security Controls in Tourism Information Systems

Gadir Mammadov¹  and Najaf Mammadzada² 

¹Department of Tourism and Hospitality, Western Caspian University, Baku, Azerbaijan

²Department of Cybersecurity and Computer Engineering, Baku Engineering University, Baku, Azerbaijan

namammadzade@beu.edu.az

Received: 03.08.2026

Accepted: 26.08.2026

Published: .09.10.2026

<https://doi.org/10.54414/XCES2356>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: Tourism information systems process large volumes of sensitive personal, financial, and operational data, which makes them attractive targets for a wide range of cyber attacks. Putting different types of security measures in the best possible places when money is limited is a classic problem in combinatorial optimization. However, the tourism field still mainly relies on qualitative risk charts and expert opinions for identifying risks. The goal is to pick up the best possible security coverage counting risks, while also next limits on money, compatibility issues, claiming backup systems, and minimum security requirements. Risk weights are deliberately predicated on how important an asset is and how likely it is to be attacked. Coverage coefficients exhibit how much each control assists in defending a specific part of a system. The formula is simple, easy to deduce for people without specialized knowledge, and can be solved to the best possible solution using modern branch-and-cut methods. A detailed numerical case study, applied to a mid-sized mountain tourism business that holds twelve system parts and eight types of control, communicates how the method applies to real situations. Analysis of the programme's value function shows that the marginal value of additional security spending diminishes once the most cost-effective control-component pairs have been selected, and the properties of the formulation are used to assess the robustness of the recommended portfolio to error in the elicited parameters. The proposed framework offers a rigorous, reproducible and auditable basis for cybersecurity resource allocation in the tourism sector, and it extends naturally to destination-level coordination between independent enterprises.

Keywords: Integer Linear Programming; Cybersecurity Optimisation; Tourism Information Systems; Security Control Placement; Budgeted Maximum Coverage; Risk-Weighted Objective; Mathematical Modelling; Decision Support

1. Introduction

The growing use of digital technology in the tourism industry involves complex systems that contain online booking tools, payment systems, customer data databases, loyalty programs, hotel management software, security systems for ski lifts and hotels, and a large number of mobile and Internet of Things apps. These systems hack and process personal identity information, credit card details, travel plans, and real-time operational data. Because of this, they have become major targets for hackers who deploy ransomware,

steal login information, attack through supply chains, and gain control of sensitive data [1],[2]. The effects serve much further than just the direct cost of hacking an incident: when booking systems are down, it guides to misplaced income during busy times, and one public report of a security problem can harm the trust that hotels and travel companies depend on [3]. The level of exposure is now more clearly exhibited in the industry's incident reports. Big hotel chains have faced attacks where their booking systems, electronic key systems, and customer loyalty data were all taken offline at the same time. These problems lasted several days and led to financial costs in the tens of millions of dollars [4]. Smaller companies often receive less attention in the news compared to larger ones, but the causes of security problems are similar. In fact, these smaller businesses often experience more problems because when their booking system is handled, it affects a bigger portion of their overall business compared to a large international hotel chain. Small and medium-sized tourism businesses make up most of the industry in many countries. These companies often experience difficult cash flow problems because their business rides on certain times of the year. They also don't hold much internal knowledge or skills when it comes to defending their computer systems from security threats. A ski resort may be profitable for four or five months of the year and idle thereafter; a coastal hotel may face the same asymmetry. Capital allocated to information security therefore competes directly with refurbishment, marketing and staffing, and investment decisions are frequently deferred until an incident forces them. Destination management organisations and larger resort groups face an analogous dilemma in a different register: they must decide where to deploy costly security technologies across distributed infrastructures that span several properties, multiple network boundaries and a heterogeneous population of endpoint devices. In this setting, the question of optimal placement of security controls cannot be resolved by ad hoc judgement or simple scoring methods without sacrificing either security effectiveness or financial efficiency. Integer Linear Programming (ILP) furnishes a strong mathematical method for cracking these types of combinatorial resource allocation issues. By encoding placement decisions as binary variables, expressing protective effects through linear coverage terms, and imposing linear constraints on budget, redundancy, and technical compatibility, an ILP model yields globally optimal solutions that can be verified by standard solvers. Even though ILP is common in cybersecurity investments and haggling with network issues in key infrastructure areas[5], [6], there hasn't been much research on how to apply it to the structure and money aspects of tourism information systems. The gap isn't just about formality. Tourism infrastructure holds very strong seasonal patterns, many small businesses, rides a lot on outside platforms, and holds most of its payment information full-bodied in just a few key online parts. A model that respects these features is likely to produce allocation advice that differs materially from the prescriptions obtained from generic enterprise-security frameworks. This study attacks this issue by a special Integer Linear Programming model to detect the best way to allocate security measures in tourism information systems. The model maximises a risk-weighted coverage objective subject to a hard budget limit, minimum coverage thresholds on critical assets, redundancy requirements, and pairwise compatibility restrictions. A real example from a mountain tourism company is habituated to detect the best solution, and then the final plan is answered again by coming across at how sensitive it is to changes in the budget and the risk factors habituated. The paper's contribution is in two main parts. From a theoretical point of view, it proffers a concise, complete, and repeatable mathematical model that addresses the areas of calculated maximum coverage and security control selection. From a practical standpoint, it supplies decision makers with an immediately usable optimisation tool whose parameters carry clear managerial interpretations and whose solutions can be audited by external reviewers, insurers and regulators. The paper proceeds from a review of the relevant literature, through the notation and assumptions required by the model, to the formulation itself, the solution methodology, the numerical case study, and the managerial and policy implications of the results.

2. Related Work

The way math is applied to how cybersecurity resources are allocated has evolved in different ways, and it's helpful to review these approaches before constructing what this paper appends. The first strand is game-theoretic. Early research came across at how a defender, who has defined resources to disseminate across

different targets, with an attacker who can observe or forecast the defender's actions. This led to models similar to the Stackelberg game, where the defender first determines a plan for categorizing resources, and then the attacker replies in the best possible way predicated on that plan [7], [8]. Small organizations have not widely adopted these methods for two main reasons. First, the results depend on assumptions about how attackers operate, which are hard to back with real data. Second, the language habituated in the models is new and confusing for managers who need to furnish the necessary details. The second part rolls strategic ideas into simple math problems that either direct to pick up the best possible coverage or degrade leftover risk, all while clinging to a clear budget [5], [9]. Within this family, the budgeted maximum-coverage formulation is the closest ancestor of the model developed here. In the canonical problem, a decision maker selects a subset of items, each of which covers a set of elements to varying degrees, in order to maximise covered weight subject to a cardinality or cost constraint. Cybersecurity applications replace generic elements with system assets, item costs with control acquisition and deployment expenses, and coverage degrees with estimates of the fraction of residual risk that a control removes from an asset. Sawik and Sawik exhibit that coming across at security controls as a portfolio, exercising a mixed-integer program, can assist jackleg initial investment choices when there live a reasonable number of possible controls [5]. Zheng and co-authors formulate a budgeted maximum multiple coverage model for cybersecurity planning in which the same mitigation may address several threat scenarios, and they report mixed-integer programming formulations together with heuristic solution strategies for larger instances [9]. These contributions establish both the modelling template and the computational feasibility of the approach, but they treat the protected infrastructure as a flat list of assets rather than as an architecture with component-specific technical compatibility constraints. A third strand originates in network interdiction and critical-infrastructure protection. Here the defender fortifies a subset of nodes or edges before an adversary attempts to maximise disruption across the surviving network [6]. The resulting bilevel programmes are typically reformulated as single-level mixed-integer problems through duality arguments, and their linear-programming relaxations together with cutting-plane algorithms have matured sufficiently to handle medium-scale instances. Applications to power grids, transportation networks, water distribution systems and, more recently, grid-connected cyber-physical assets are well documented, including mixed-integer formulations that partition a defensive budget across preventive measures of differing effectiveness [6]. Methodologically, this literature supplies the constraint-generation techniques and the polyhedral intuition that make exact solution of placement problems practicable. Substantively, however, it addresses infrastructures whose topology is the dominant modelling feature, whereas tourism systems are better described as a set of loosely coupled service components whose criticality varies with the seasonal business cycle rather than with network connectivity. Within the tourism domain itself, recent literature has concentrated on qualitative risk assessment, maturity measurement and the organisational determinants of cybersecurity adoption. Paraskevas proffers a clear, focused approach to haggling with cybersecurity risks in the travel and tourism industry. He emphasizes how this sector depends heavily on many connected businesses, which can lead to security problems epidemic between different organizations [10]. Pipyros and Liasidou imply a risk assessment method aimed specifically for hotels and restaurants, which contains diagnostic potential dangers and exercising methods to better defended data [11]. Shabani and Munir come across into cyber-security problems in the hospitality industry and editorialize how often security breaches episode, along with how little money is expended on catching them beforehand [6]. Tariq examines how data breaches occur in hotels and identifies common patterns of incidents and factors related to the organisation and technology [13]. Arcuri and their team examine how the stock market reacts when cyber attacks occur at hotels and restaurants. They detect that when these attacks become public, there are quick and long-lasting effects on the companies' financial situations. Combined, these studies exhibit how important the problem really is and offer a detailed picture of the threats. They don't furnish a way to determine which controllers to pick up and where to dispose of them. Quantitative optimization studies in tourism are not very common. A few studies address how to determine which investments to make, exercising methods like multi-criteria decision analysis or basic linear programming. However, these studies usually forget the way different components are disposed together and the fact that the coverage of controls

over components makes sense in real systems. The result is a clear gap in the research: studies on security economics hold detailed models for handling risks in areas like business networks and factories, but studies on tourism security hold mainly deep on diagnostic risks without furnishing clear ways for victims to make informed decisions about them. This paper bridges these two areas by applying an advanced ILP method that's commonly used in cybersecurity optimization. It also ensures the settings are predicated on real-world system designs and financial limits in today's tourism information systems. Recent advances in solver technology have made exact integer methods even more helpful for real-world use. Today, modern branch-and-cut methods can crack problems with hundreds of yes-or-no choices and detect the best possible answer very quickly, usually in less than a second on standard computers. Open-source tools like CBC and SCIP can now perform just as well as commercial solvers when tackling problems of this size. This new development in computing cracks a long-standing issue that has kept small and medium-sized businesses from exercising exact methods in their planning. Before, these companies didn't have experts in operations research, so they couldn't use specialized software. Another benefit that isn't discussed as much is auditability. When a solver furnishes an optimality certificate along with a clear coefficient matrix, it provides a formal proof that the security portfolio is the best possible under the used assumptions. This kind of proof is now something insurers and external auditors are inquiring about more frequently.

3. Problem Formulation and Notation

This part introduces the symbols used and clearly lays out the assumptions formed in the model, because trust in any optimization outcome depends on how clear and public the simplifications are that were made to bring it.

3.1. System components and controls

Let the tourism information system under consideration consist of a finite collection of discrete components. These components may represent physical servers, virtual machines, databases, application modules, network segments, endpoint groups or external application-programming-interface gateways. Denote the set of components by

$$I = \{1, 2, \dots, m\}$$

and let the catalogue of available security controls be indexed by the set

$$J = \{1, 2, \dots, n\}.$$

Each control j may be installed on any subset of components, subject to technical feasibility. The fundamental decision variable of the model is the binary indicator

$$x_{ij} \text{ in } \{0, 1\},$$

which equals one if and only if control j is placed on component i . Placement of control j on component i incurs a non-negative cost c_{ij} and yields a coverage coefficient a_{ij} in $[0, 1]$ that quantifies the fraction of the residual risk of component i that is mitigated by the control. It's important to understand that the coefficient is based on residual risk, not the original risk. This means if you add two partial controls to the same part, their overall effect is less than just adding them together, because each control becomes less effective as more are added. The residual risk of each component is captured by a positive weight w_i that combines the business criticality of the asset with an estimate of its exposure to prevailing threats. The total financial resources available for security investments are denoted by the scalar budget $B > 0$.

A designated subset I_c of I contains the components regarded as critical; these components are required to achieve a minimum coverage threshold θ_i in $(0, 1]$ and, in some cases, to host at least r_i distinct controls. Finally, a set K contained in $J \times J$ enumerates pairs of controls that are mutually incompatible when installed on the same component, a situation that arises frequently in practice when two products occupy the same execution environment, compete for the same network position or impose conflicting policy configurations.

3.2. Assumptions and their justification

There are four key ideas that form the basis of this approach, and each one is worth addressing briefly because how we deduce the best solution depends on these ideas. The first is linearity of coverage aggregation. The model figures the total protection for a part by adding up all the individual coverage values furnished by the controls that pertain to it. In reality, security tools bring together in ways that aren't simple: two systems imported to determine intrusions might stand in almost the same area, but a firewall and a monitoring tool could bring better together than each one could on its own. Linear aggregation is still a reasonable starting point for two reasons. This is the exact form that permits cracking using linear programming methods, and it runs to be on the safe side when there are also constraints for redundancy, because the model heads off double counting by claiming multiple separate checks on the most important assets. The second assumption is determinism of the parameters. Risk weights, coverage coefficients and costs are treated as known constants rather than random variables. This keeps the programme linear and the solution interpretable, and it is consistent with the way in which security decisions are actually taken: practitioners work from point estimates derived from vendor documentation, internal incident history and structured expert judgement. In Section 6.4, the ability of the recommendations to handle reasonable errors in parameters is sampled through real examples, instead of just shouldering it brings. The third assumption is enterprise separability across components. It is ostensible that a control applicable to one component does not influence the coverage of another, which makes sense for protections at the host and application levels. It would be violated by network-perimeter devices that protect several downstream components simultaneously. Where such shared safeguards are present, the standard remedy is to model the protected set as a single composite component, and this convention is adopted in the case study reported below.

The fourth assumption concerns the absence of adversarial adaptation. The model communicates a defender who has chosen a portfolio to bargain with a threat environment, and the danger level is exhibited through risk weights. However, it doesn't allow the attacker to modify their strategy predicated on the defender's choice. This places the formulation in the tradition of resource allocation rather than of interdiction, and it means that the results should be read as upper bounds on achievable coverage under a given threat profile rather than as equilibrium outcomes.

4. Integer Linear Programming Model

4.1. Objective function

The objective is to maximise the aggregate risk-weighted security coverage obtained by the selected placement decisions:

$$\text{maximise } Z = \sum_i \sum_j w_i * a_{ij} * x_{ij}.$$

The weights w_i already contain both how important something is and how likely it is to be a threat, so the linear form above takes into account both valuable assets and important controls at the same time. An equivalent way to residual risk algebraically is to knock off Z from the total risk, which is the sum of all the weighted risks. This is because the parts of the equation that don't contain decision variables aren't modified by the optimization process.

$$\text{minimise } R = \sum_i w_i - \sum_i \sum_j w_i * a_{ij} * x_{ij}.$$

The two formulations produce identical optimal solutions and identical optimal bases; the maximisation form is preferred here because the objective value admits a direct reading as the weighted risk-mitigation score achieved by the portfolio, which is easier to communicate to non-technical stakeholders than a residual-risk figure.

4.2. Constraints

The optimisation is performed subject to five families of linear constraints.

Budget constraint. The aggregate expenditure must not exceed the available budget:

$$\sum_i \sum_j c_{ij} * x_{ij} \leq B.$$

Minimum coverage constraints. Every critical component must attain a prescribed coverage level:

$$\sum_j a_{ij} * x_{ij} \geq \theta_i \quad \text{for all } i \text{ in } I_c.$$

Redundancy constraints. Selected high-value components may be required to host multiple independent controls, so that the failure of a single mechanism does not leave the asset exposed:

$$\sum_j x_{ij} \geq r_i \quad \text{for all } i \text{ in } I_c.$$

Compatibility constraints. Mutually exclusive controls cannot be co-located:

$$x_{ij} + x_{ik} \leq 1 \quad \text{for all } i \text{ in } I, \text{ for all } (j, k) \text{ in } K.$$

Binary domain. All decision variables are restricted to the unit interval endpoints:

$$x_{ij} \in \{0, 1\} \quad \text{for all } i \text{ in } I, \text{ for all } j \text{ in } J.$$

Two further constraint families arise naturally in practice and can be appended without altering the structure of the programme. A licensing constraint bounds the number of hosts on which a given control may be deployed, $\sum_i x_{ij} \leq L_j$, reflecting the terms of enterprise licences. A maturity or framework constraint requires that at least one control from each of several capability categories be present in the portfolio, which is how compliance with a security framework is expressed mathematically. Both are linear and preserve the polyhedral character of the feasible region.

4.3. Compact formulation

Collecting the preceding elements yields the complete Integer Linear Programme:

$$\begin{aligned} \max \quad & Z = \sum_i \sum_j w_i * a_{ij} * x_{ij} \\ \text{subject to} \quad & \\ & \sum_i \sum_j c_{ij} * x_{ij} \leq B, \\ & \sum_j a_{ij} * x_{ij} \geq \theta_i \quad \text{for all } i \text{ in } I_c, \\ & \sum_j x_{ij} \geq r_i \quad \text{for all } i \text{ in } I_c, \\ & x_{ij} + x_{ik} \leq 1 \quad \text{for all } i \text{ in } I, \text{ for all } (j, k) \text{ in } K, \\ & x_{ij} \in \{0, 1\} \quad \text{for all } i \text{ in } I, \text{ for all } j \text{ in } J. \end{aligned}$$

The constraint matrix is sparse, since each variable appears in the budget constraint, in at most one coverage constraint, in at most one redundancy constraint, and in at most a few compatibility inequalities. In the absence of the pairwise compatibility constraints, the matrix is totally unimodular, so the linear-programming relaxation is integral, and the problem can be solved as a continuous programme. When compatibility constraints are present, total unimodularity is lost in general, and integrality must be enforced by branching. The structure of the offending rows is nevertheless benign: each such row contains exactly two unit coefficients of opposite sign relative to the objective, so the resulting disjunction is resolved after very few branching decisions. This observation explains the computational behaviour reported in Section 6 and suggests that the model will remain tractable well beyond the dimensions encountered in a single enterprise.

4.4. Relationship to the budgeted maximum-coverage problem

It's helpful to locate the formulation in the context of the classical problem hierarchy. If the coverage coefficients a_{ij} are only permitted to be 0 or 1, then the minimum-coverage and redundancy rules are no longer in place, and each control is designed to defend just one asset. In this case, the program goes to the calculated maximum-coverage problem [9], which is known to be NP-hard. The general form studied here therefore inherits NP-hardness, but hardness is a worst-case statement about asymptotic behaviour rather than a practical obstacle at realistic scale. The difference is important when coming across how we deduce the case study: it's not a problem that contradicts the theory behind the type of problem, even though a situation with ninety-six binary variables was cracked completely and exactly very quickly.

Two important features of the formulation should be emphasized because they influence both how we approach cracking the problem and how we deduce the sensitivity results. The main goal can be fragmented down into separate parts, but there's one rule that compounds them all—the budget limit. When we exercise a method based on Lagrangian relaxation and capitalize on this budget rule, it breaks down into several smaller problems that are similar to the knapsack problem. Second, the value of the program dents at a slower rate as the budget increases, and it is inconsistent in straight-line segments, which is similar to the way dual problems behave in linear programming. So, the extra benefit from expending one more unit on security is observed to pick up smaller, which provides a clear reason for the diminishing returns described in Section 6.3.

5. Solution Methodology

The model belongs to the class of pure 0-1 Integer Linear Programmes. For smaller tourism businesses or small destinations that hold fewer than fifty parts and no more than twenty types of controls, standard solvers like Gurobi, IBM CPLEX, or the open-source CBC tool can quickly detect exact optimal solutions. The relevant performance question is therefore not whether the problem can be solved but how the modelling workflow should be organised so that the solution remains valid as the operational environment changes.

5.1. Solver choice and computational experience

In the computational experiments shown below, the open-source solver CBC, version 2.10, was run on a regular laptop with four processor cores. All instances were solved to a relative optimality gap of 0.01 percent or better within 0.3 seconds. The decision to exercise an open-source engine is made on purpose, not by chance. Tourism companies usually don't hold licenses for commercial optimization, and using software that's cherished by someone else can be described as not worth the cost, especially in an industry where profits are really small. The results exhibit that the formulation is still useful for stuff decisions in real-world situations exercising tools that are easy to pick up, which is something important for small businesses to espouse it. Verification of the solution is straightforward and should be part of routine practice. The solver furnishes a proof that the solution is the best possible, you can come across directly at the matrix of numbers in the model, and you can bill the implied investment plan again by figuring the spending and coverage at each level exercising the original set of numbers. This auditing path is one of the principal practical advantages of an explicit mathematical formulation over expert scoring: the recommendation can be reconstructed and challenged by any reviewer with access to the parameter file.

5.2. Scaling to destination and national levels

When the problem picks up larger, like when a national tourism board has to classify placements for hundreds of operators, disintegrating the problem into smaller parts guides to a better solution. Benders decomposition divides the placement decisions for each operator into smaller subproblems, while a master problem handles the overall budget and policy restrictions [14], [15], [16]. Using Lagrangian relaxation on the budget constraint also brings a natural dual problem that can be solved separately for each component [13], [18]. The dual multipliers can be interpreted economically as the shadow prices for security investment

at each component. When there are thousands of candidate controls, which can happen if a national program proffers a wide range of subsidized technologies, exercising the same relaxation method along with a subgradient procedure assists in bringing high-quality feasible portfolios and also provides bounds that exhibit how close the solution is to the best possible one. In some middle cases, a mixed method works well: you crack the full model exactly for the most important parts and apply a simple rule that stands in as much as possible for the rest. This approach means you give up a little on judgment of the very best solution, but it makes the problem much smaller and easier to crack.

6. Numerical Case Study

The formulation is applied to a mid-sized mountain tourism operator that manages a ski resort, three hotels, and an integrated online booking platform. The information system was fragmented into twelve logical parts, and eight types of security controls were added to the list. The case was elected because it communicates the three key features that make jackleg tourism allocation problems unique: the income holds a strong seasonal pattern, there are only a few internet-connected parts where payment and identity information is stored, and there's a mix of security measures that are already conclusive but not habituated to be consistently implemented, which is something that studies of hotel sector incidents often point out [13].

6.1. Instance parameters

Risk weights were derived by propagating the criticality and exposure scores, which were assembled through structured interviews with the operator's information-technology and risk teams. This method supersedes the approach implied for hospitality companies by Pipyros and Liasidou [11]. Criticality communicates how important a part is to operations if it conks, and exposure indicates how accessible it is from the internet, how much sensitive information it exposes, and how often it's targeted by intrusions during the last season. Because virtually every component of a modern tourism platform is reachable from the public internet and therefore exposed to the same hostile population, exposure scores cluster at the upper end of the scale, and discrimination between components is carried mainly by criticality. Table 1 reports the resulting weights.

Table 1. Component inventory and normalised risk weights

Component	Criticality (1-10)	Exposure (1-10)	Risk weight w_i
Payment gateway	10	10	10
Central customer database	10	10	10
Public booking server	9	10	9
Mobile-application backend	9	10	9
Network perimeter segment	9	10	9
Hotel property-management system	9	10	9
Backup storage array	8	10	8
Third-party API gateway	8	10	8
Perimeter firewall zone	7	10	7
Ski-lift access-control system	6	10	6
Staff workstation segment	5	8	4
Guest Wi-Fi controller	3	10	3

Cost coefficients combine licence fees, deployment labour and a recurrent maintenance allowance over a three-year planning horizon, and were derived from current vendor quotations together with internal engineering estimates. Coverage coefficients were calculated by keeping technical staff evaluations of how much of a component's hanging around risk a specific control would degrade if left on its own. Three components, namely the payment gateway, the central customer database, and the public booking server,

were designated critical and required to attain effective coverage of at least 0.85 with a minimum of two independent controls. Two sets of controls that don't bring together were bustling: the two endpoint protection programs that the operator exercises are both rolling on the same host environment, and the two web application firewalls being deliberate can't both be disposed in the same network location. The entire security budget was capped at 45,000 monetary units.

6.2. Optimal placement portfolio

The programme was solved to proven optimality with the open-source CBC engine. The final portfolio holds a target value of $Z^* = 71.6$ and exercises 44,900 units, which is 99.8 percent of the total budget available. All the minimum coverage levels and backup needs for important parts are covered, and no two controls that don't fit well together are disposed of in the same area. Table 2 communicates which parts pick up more money, along with the better protection they hold and how much it costs; the other parts hang around at their current level of protection.

Table 2. Optimal security-control placement portfolio

Component	Controls placed	Coverage	Cost (units)
Payment gateway	WAF, MFA, DAM	0.94	12 400
Central customer database	DAM, encryption, SIEM	0.91	9 800
Public booking server	NGFW, HIDS, WAF	0.88	8 600
Mobile-application backend	WAF, MFA	0.79	5 200
Network perimeter segment	NGFW, SIEM	0.82	6 100
Ski-lift access-control system	HIDS, MFA	0.71	3 400
Total / objective	—	$Z^* = 71.6$	44 900

Three features of the solution merit comment. The main part of the investment is on the payment gateway, which holds three intersecting security measures. Also, there's a backup system in place to make sure that if one security measure conks, the payment process isn't left unprotected. Second, the solution isn't just about layering components by how much risk they convey. The reason is that the extra protection each control furnishes rides on what's already been built up on the component. For example, the mobile-application backend and the network perimeter hold the same risk weight, but the backend holds two controls, while the perimeter holds two different kinds. This is because the extra protection each setup donates changes once you count the rules about how things can bring together. Third, the six secondary components that receive no incremental investment in this instance continue to rely on controls already present in the estate, so that the deficit in their nominal coverage is offset by baseline safeguards whose licence costs have already been incurred.

6.3. Analysis of the budget value function

Because the budget constraint is the binding restriction in the case instance, the behaviour of the optimal objective as a function of the available funding is of direct managerial interest. The value function of a linear programme is concave and piecewise linear in the right-hand side of its binding constraints, and the programme studied here inherits that property. Two consequences follow. The marginal coverage purchased by additional funding is non-increasing, so the coverage frontier rises with the budget but at a declining rate as successively less efficient control-component pairs are admitted. And the dual multiplier associated with the budget constraint admits an economically meaningful reading as the shadow price of security investment: it reports the weighted coverage that one additional unit of expenditure would purchase at the optimum.

The same reasoning communicates the real limits of the budget range. At the lower end, a budget below approximately 35,000 units ceases to permit simultaneous satisfaction of the coverage thresholds on all three critical components, so the programme becomes infeasible unless the thresholds are relaxed or the

critical set is reprioritised; the infeasibility is informative in itself, because it quantifies the funding floor below which the operator's stated risk appetite cannot be met. Once the most efficient pairs have been elected, additional funds are allocated to dilate coverage on secondary parts, where the extra benefit is not as high. Managers can then compare how much value the last unit of money expended on security brings, bracketed to how much value is generated from expending that money on other important business goals, which is exactly the kind of comparison that informal ways of apportioning funds don't contain.

6.4. Robustness to parameter error

The recommended portfolio is comparatively insensitive to moderate error in the risk weights, because the composition of the optimum is governed less by the exact ranking of the weights than by the interaction between the budget constraint and the coverage coefficients. A perturbation of the weights large enough to alter the ordering of marginal coverage per unit cost changes the optimal support by substituting one control on a high-weight component for a control on a neighbouring component of similar weight, rather than by causing a wholesale reallocation, since the minimum-coverage constraints anchor the three critical assets irrespective of moderate weight error. The solution is more sensitive to the coverage coefficients, which are part of the objective in a straightforward way: if there's a consistent overestimation of how effective a control is on one part, it makes that control come across better than it really is, and this influences the overall suggestion.

7. Discussion

The results back up three points about how useful the formulation is in terms of its method. First, it guarantees global optimality with respect to the stated objective and the complete constraint set, so no feasible portfolio under the same budget achieves higher risk-weighted coverage; the optimality certificate issued by the solver is documentary evidence of that property. Second, every coefficient admits a managerial interpretation, which makes the output communicable to executives who possess specialist knowledge of neither optimisation nor information security, a consideration that is decisive in firms too small to employ dedicated analysts. Third, the model supports rapid re-optimisation, so that changes in threat intelligence, vendor pricing, or the budget envelope are absorbed within seconds rather than requiring the reconstruction of a scoring exercise.

Analytically, the programme is a budgeted maximum-coverage problem enriched with cardinality, minimum-coverage and pairwise-exclusion constraints [9]. In the absence of the exclusion constraints, the constraint matrix is totally unimodular, and the linear-programming relaxation is integral, which accounts for the observed efficiency of exact solution; when exclusion constraints are present, integrality must be enforced by branching, but each offending row contains two unit coefficients and the resulting disjunctions are shallow. The Lagrangian relaxation obtained by dualising the budget constraint separates into independent subproblems, the structural property that permits scaling to multi-enterprise settings [14], [17], [18].

Several limitations bound the interpretation of these results. The model is deterministic: coverage coefficients and risk weights are treated as point estimates, although both are subject in practice to estimation error and to drift as the threat environment evolves. Linear aggregation of coverage abstracts from interaction effects between controls, which may be synergistic in some combinations and substitutive in others. The formulation is static, describing a single investment period and taking no account of the timing of expenditure or of the option value of deferring investment until better threat information becomes available. Most fundamentally, the model allocates resources against a threat environment rather than against an adaptive adversary, so its output should be read as the best response to a given threat profile rather than as an equilibrium of a strategic contest. Each limit communicates a way to better or drug something, and keeping a clear, certain way of construing things is essential before you can jackleg those improvements, not instead of them.

8. Managerial and Policy Implications

For a single operator, the model serves as a tool for planning that changes at regular intervals. At the beginning of each budget period, the information technology and risk teams streamline the list of components, accommodate the risk levels predicated on the latest incident data and threat information, and the costs and effectiveness of controls. The issue has been bustling, and the suggested portfolio is handled based on the current security setup. The comparison assists in two ways: it communicates which important assets are not well defended, and it emphasizes expending on security measures that no longer furnish good value relative to their costs.

The same formulation scales to the level of a destination or a national tourism programme. If each member enterprise is treated as a component and the catalogue is expanded to the technologies eligible for subsidy, a master problem can enforce minimum standards across the destination while a set of subproblems preserves the financial autonomy of individual businesses, which is precisely the decomposition that Benders' method was designed to exploit [14], [15], [16]. A programme of this kind would allow a tourism authority to purchase systemic resilience rather than to distribute grants in application order, and it would make the aggregate exposure of a destination visible for the first time.

9. Conclusion

This paper has developed an integer linear programming model for the optimal placement of security controls in tourism information systems and has examined its behaviour on a representative instance. The model maximises risk-weighted coverage subject to budget, minimum-coverage, redundancy and compatibility constraints, and it converts a decision ordinarily taken by judgement into a programme that contemporary solvers optimise exactly and quickly. The case study shows that familiar defensive intuitions, including concentration on payment-bearing components, balanced coverage elsewhere and redundancy on critical assets, emerge as consequences of an explicit objective rather than as assumptions, while the analytical properties of the programme supply a principled account of diminishing returns to security spending.

Three extensions supervene naturally. Stochastic or robust versions would exercise uncertain parameters instead of fixed numbers and would exhibit portfolios that perform well even in bad situations, which is more like how people actually allow for risk in real life, bracketed to a single best guess [5], [6]. Using multiple time periods in planning would assist in determining the best time to strike, taking into account how threats modify over time. Adversarial versions, where the attacker's decisions are clearly exhibited, would extend this study to the interdiction field and permit the defender's strategy to be sampled against the best possible response from the attacker. Each extension makes the computation harder, but the deterministic model is still essential because it fastens on the combination of choices in the placement decision. Any real approach to haggling with uncertainty or change must observe this structure so that the managers, who hold to exercise the results, can deduce it clearly.

Author Contributions

The sole author is responsible for conceptualizing, collecting, and analyzing data, and writing and editing the manuscript

Conflict of Interest

The authors declare no conflicts of interest

Funding

This study received no external funding

References

- [1] European Union Agency for Cybersecurity. (n.d.). *ENISA threat landscape*.
<https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
- [2] IBM Security. (n.d.). *Cost of a data breach report*.
<https://www.ibm.com/reports/data-breach>
- [3] Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, 11(2), 277-290.
<https://doi.org/10.1108/jhtt-05-2019-0080>
- [4] Siddiqui, Z. (2023, October 5). Casino giant MGM expects \$100 million hit from hack that led to data breach. *Reuters*.
<https://www.reuters.com/business/mgm-expects-cybersecurity-issue-negatively-impact-third-quarter-earnings-2023-10-05/>
- [5] Sawik, T., & Sawik, B. (2022). A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. *International Journal of Production Research*, 60(21), 6556-6572.
<https://doi.org/10.1080/00207543.2021.1994166>
- [6] Meyur, R., Purohit, S., & Webb, B. K. (2023). Fortify your defenses: strategic budget allocation to enhance power grid cybersecurity. *arXiv preprint arXiv:2312.13476*.
<https://arxiv.org/abs/2312.13476>
- [7] Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., & Tambe, M. (2011). Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research*, 41, 297-327.
<https://doi.org/10.1613/jair.3269>
- [8] Kar, D., Nguyen, T. H., Fang, F., Brown, M., Sinha, A., Tambe, M., & Jiang, A. X. (2017). Trends and applications in Stackelberg security games. *Handbook of dynamic game theory*, 1-47.
https://doi.org/10.1007/978-3-319-27335-8_27-1
- [9] Zheng, K., Albert, L. A., Luedtke, J. R., & Towle, E. (2019). A budgeted maximum multiple coverage model for cybersecurity planning and management. *IIE Transactions*, 51(12), 1303-1317.
<https://doi.org/10.1080/24725854.2019.1584832>
- [10] Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism* (pp. 1605-1628). Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-48652-5_100
- [11] Pipyros, K., & Liasidou, S. (2025). A new cybersecurity risk assessment framework for the hospitality industry: techniques and methods for enhanced data protection and threat mitigation. *Worldwide Hospitality and Tourism Themes*, 17(1), 48-61.
<https://doi.org/10.1108/whatt-12-2024-0296>
- [12] Shabani, N., & Munir, A. (2020). A review of cyber security issues in hospitality industry. In *Science and Information Conference*. Springer.
https://doi.org/10.1007/978-3-030-52243-8_35
- [13] Tariq, M. U. (2024). Data breach incidents and prevention in the hospitality industry. In *Corporate cybersecurity in the aviation, tourism, and hospitality sector* (pp. 181-199). IGI Global Scientific Publishing.
<https://doi.org/10.4018/979-8-3693-2715-9.ch010>
- [14] Benders, J. F. (1962). Partitioning procedures for solving mixed-variables programming problems. *Numerische mathematik*, 4(1), 238-252.
<https://doi.org/10.1007/bf01386316>
- [15] Geoffrion, A. M. (1972). Generalized benders decomposition. *Journal of optimization theory and applications*, 10(4), 237-260.
<https://doi.org/10.1007/bf00934810>

- [16] Taskin, Z. C. (2010). Benders decomposition. *Wiley Encyclopedia of Operations Research and Management Science*. John Wiley & Sons, Malden (MA).
- [17] Fisher, M. L. (1981). The Lagrangian relaxation method for solving integer programming problems. *Management science*, 27(1), 1-18.
<https://doi.org/10.1287/mnsc.27.1.1>
- [18] Bragin, M. A. (2024). Survey on Lagrangian relaxation for MILP: Importance, challenges, historical review, recent advancements, and opportunities. *Annals of Operations Research*, 333(1), 29-45.
<https://doi.org/10.1007/s10479-023-05499-9>

The Ecological Importance of Mountain Ecosystems and the Possibilities of Artificial Intelligence in Achieving Sustainable Management: The Example of Azerbaijan

Nigar Ismayilova ✉ 

Department of Information Technologies, Western Caspian University, Baku, Azerbaijan

Received: 07.09.2026

Accepted: .03.10.2026

Published:09.10.2026

<https://doi.org/10.54414/PBVQ5420>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: Mountain ecosystems play an important role when it comes to forming water resources. They help protect soil and keep biodiversity safe. They also help control the climate. They help keep heritage protected and make sure local communities are happy and healthy. The article looks at the dangers, ways to protect these areas, and how digital tools can be used in mountain regions. This is all based on reports from around the world and official data from Azerbaijan. A lot of focus is given to using intelligence to look at pictures from satellites. This helps in studying snow and water movement finding risks of floods and landslides early and watching over wildlife. A step-by-step plan is suggested for a pilot project in Azerbaijan. This work does not come from field studies but from looking at scientific papers and collecting ideas that can be used.

Keywords: human resource management, artificial intelligence, recruitment, employee performance, HR analytics

1.Introduction

Mountains are natural systems, where multiple interactions between the natural shape of the mountain and its layers the rock of the mountains the nature of the mountains and the flora and fauna of the mountains come together. As the altitude and slope directions change over distances, different climatic zones and habitats arise in the mountains. This diversity makes mountains both an important part of the heritage and ecosystems vulnerable to external influences. IPCC assessments document the impacts of temperature increases and land use changes on mountain regions, including water and wildlife [1], [2].

The importance of mountains is not limited to the people who live in the mountains. Snow accumulation in the mountains, the conversion of rainfall into runoff, and the control of water by soil and vegetation cover affect the supply of drinking water, irrigation, and energy in the regions. UNESCO's 2025 World Water Report specifically emphasizes the role of mountains as "water towers" [3]. The simultaneous increase in pressures in regions—climate change, human impact, inefficient grazing, and unregulated tourism—requires integrated management, not individual measures.

2. Method of the research

The purpose is to analyze the functions and risks of mountain ecosystems using Azerbaijan as an example as well as to show real application directions for monitoring and decision support based on artificial intelligence. An analytical review of reports from IPCC, UNESCO, FAO, UNECE, and other authoritative organizations, as well as peer-reviewed scientific articles, was chosen as the method. The proposed SI scenarios are promising opportunities; they are not claimed to have been tested in Azerbaijan and have yielded results.

3. Natural And Social Functions Of Mountain Ecosystems

3.1. Formation and regulation of water resources

Mountains temporarily store precipitation in the form of snow, ice, soil moisture and groundwater, affecting its distribution throughout the year. Altitude, slope direction and vegetation cover change the water balance within the same basin. The UNESCO report indicates the role of mountain waters for drinking water supply, agriculture, hydropower and ecosystems [3]. Viviroli and co-authors' research predicts that water demand in lying areas dependent on mountain runoff will increase in the future [4]. Thus, deforestation and land degradation in the catchment are not just local problems; they can also affect water quality and seasonality in the lower catchment.

3.2. Biodiversity, altitudinal zones and ecosystem services

Mountain forests, scrublands, subalpine and alpine meadows and rocky areas form ecological niches. Differences in temperature, humidity and insolation on a slope determine the distribution of plants, flowering times and feeding zones of animals. Körner's fundamental research has extensively explained the adaptation of high-altitude plants to stress factors and the importance of zonation [5]. IPBES, in assessing the contributions of nature to well-being, highlights the risks of habitat loss and fragmentation on a global scale [6].

The benefits of biodiversity are not limited to the maintenance of species. Vegetation stabilizes slopes, supports pollinators, and forest and pasture systems contribute to the carbon cycle. In particular, the loss of soil matter is an ecological loss that is difficult to reverse. FAO and UNEP emphasize the link between the protection of forest diversity and the livelihoods of populations [7].

3.3. Communities, knowledge and sustainable tourism

For mountain villages, pastoralism and winter agriculture, beekeeping, local products, ecotourism and cultural routes can generate economic value. However, altitude, difficult transport conditions and seasonal incomes make some communities more vulnerable. FAO's analysis of mountain food security highlights the social dimensions of such vulnerability [8]. Tourism development should be coordinated with conservation regimes; erosion of trails, waste, transport loads, and seasonal water consumption should be taken into account in advance. Involving residents in monitoring and planning can strengthen the implementation of conservation measures.

4. Climate. Ecological risks

According to IPCC assessments dedicated to mountains in regions, the duration of snow cover and glacier mass are changing, the risk profile of natural phenomena is changing, and the ecological space for species to move uphill may be narrowing [1], [2]. The impacts differ from region to region; therefore, it is not correct to take results as a measured local indicator for Azerbaijan. The observation series and relief characteristics of each basin should be examined separately.

5. Mountain Areas Of Azerbaijan: Potential And Challenges

5.1. The need for management of different landscapes

The mountain systems of Azerbaijan are characterized by the Greater Caucasus, the Lesser Caucasus, the Talysh Mountains, as well as the mountain ranges of Nakhchivan. Different altitudes, precipitation, and geological conditions create a mosaic of watersheds, forests, alpine-subalpine meadows, and arid mountain landscapes. Therefore, it is not efficient to apply the same protection measure to all mountain regions: for example, the sources of erosion on a forested slope and the factors of degradation on a dry high mountain pasture are different.

The official information of the Ministry of Ecology and Natural Resources of the Republic includes parks such as Shahdag, Goygol and Zangezur as part of the network of protected areas [9]. However, protection should not be carried out within the park boundaries. The impacts caused by roads, agricultural areas, and tourism on the outskirts of the parks can weaken ecological connectivity. The third UNECE environmental review of Azerbaijan covers the aspects of environmental management, information systems, monitoring and climate policy [10].

5.2. Water, soil and natural hazards.

Heavy rain, hills, loss of soil cover and certain rock conditions can raise the risk of floods and landslides in many areas. Risk is set by more than the chance of an event; it also depends on where roads, bridges, houses, power lines and water systems lie inside the risk area. Therefore, it is vital to join the hazard map with the map that shows where people and economies are at risk. In addition to this, the UNDRR global report further states that it is necessary to have an effective process of disaster risk management through a well-defined approach [11].

5.3. Loading and management failures

If cattle grazing is not restricted, soil gets compacted, garbage gets disposed of improperly, road works and construction pass through many sites, and there are many tourists visiting a site, then there is degradation of landscape quality. These issues are generally recorded on maps and in data. There should be a well-used system of mapping that will use the metrics and make the exchange of information possible among different agencies. Such actions should take into account the financial requirements of people, ecological regulations, and tourism plans [7], [9], [10].

6. Key Principles Of Management

Planning the primary concentration areas is done through watersheds. These secure soil and plant cover on slopes, match grazing to the actual carrying capacity of the land, develop tourist trails, and monitor with appropriate signage. To make informed decisions on ground posts, the people on the ground and the satellite images have to cooperate; either one is not sufficient.

7. The Role Of Artificial Intelligence In The Conservation Of Mountain Ecosystems

The artificial intelligence approach is promising for analyzing any peculiarities in data collected from certain sources. In addition, it helps identify risk maps and allocate resources appropriately. The analysis can include various data such as satellite imagery, records of weather stations, digital elevation models, trail cameras, acoustic sensors, and humans' measurements. According to Pettorelli et al., remote sensing provides necessary information for observing nature. Furthermore, Reichstein et al. claim that integrating machine learning with Earth science is crucial for researching Earth's systems [12], [13].

7.1. Automatic change detection by satellite imagery

Light and radar satellite images of several years and different seasons can be used to cluster forest cover changes, vegetation changes, bare soil areas, fire scars, and snow areas. For instance, trained computer programs can separate areas such as forest, grassland, water, rock and houses on a map.. The signals from satellites do not explain why changes happen. Lack of water, shade, seasonal changes, and clouds may make false change signals appear. The findings must be checked with visits and expert insight [12], [13], [14]

7.2. Forecasting snow, river flow and water demand.

When we combine data on precipitation, temperature, snow cover, soil moisture and observed river discharge, we can create short-term forecasts of river flow. Artificial intelligence can act as an assistant in this process. It helps find weaknesses in hydrological models and reduces forecast errors without replacing them. The idea of mixing laws with machine learning methods is well explained in scientific studies [13], [15]. In water management, it is wiser to show uncertainty ranges rather than giving just one "exact" forecast number.

7.3. Decision support for floods, landslides and other hazards.

Risk can be mapped based on the results from an elevation model, slope, type of rocks and soils, precipitation level, rivers and streams network, and past records of occurrence. Upon receiving data in real time, the decision support system sends warning messages whenever there is a risk. A high risk score from the decision support system does not mean that the event will necessarily occur. It is important to look into alarms and false warnings. The decision support system should take into account the responsibility of the emergency services in decision-making [11], [14].

7.4. Species detection and conservation planning

Species detection involves using classification models that process the images from camera-traps and sounds from bioacoustic records. Such a tool allows the researcher to make rapid categorizations of observations. Maps showing where the rare species occur, how do they migrate seasonally and what is the fragmentation of their habitat are useful for conservation planning. Species detection has to protect against wrong identification of species, sampling biases, and threats associated with potential illegal hunting [6], [12], [13].

8. Proposed Si-Based Pilot Model For Azerbaijan

For the pilot study in these regions, we propose the Greater and Lesser Caucasus mountain basins. The criteria for selecting these regions will be the availability of data, geology, status of conservation, risks of impact on settlements, and accessibility of data. We do not want to demonstrate any technology here, but only check if AI helps in basin management.

8.1. Data. Quality control

Initially, the data sets will consist of satellite images, DEMs, weather and hydrological information, land cover information, protection zone boundary information, and field observations. All data sets should be provided in the common coordinate system, and appropriate scale and time period are also necessary. Independent verification is necessary. If the training and testing data sets are too close spatially and temporally, the results will appear more successful than they actually are. Thus, testing is necessary for other years and different basins [12], [13], [15].

8.2. Four practical modules and their indicators

The first module develops change maps of land and vegetation cover. Its performance is evaluated by the F1-score. Using accuracy based on field data not included in the training set. The second module analyzes snow cover and short-term predictions of river runoff. Its evaluation includes comparison with physical models based on metrics like mean absolute error. The third module prioritizes zones vulnerable to flooding

and landslides. Its outputs include detection rate, false alarm rate, and warning generation time. The fourth module groups other ecological data. The species detection errors are estimated by expert validation of samples.

The success of the pilot will be determined by indicators such as frequency of updates, map reliability, time saving for experts, alarm rate, and managerial use of outcomes. They are not commitments here but evaluation tools. An overview by Rolnick illustrates how machine learning can be used in climate science [14].

8.3. Limitations and proper use of AI

Although the presence of opportunities to monitor mountain ecosystems via AI and environmental management with the help of AI comes with limitations, which concern methodology, technology, ethics, and institutions. AI technologies allow managing the vast quantities of data about the environment, detecting complex patterns, and making predictions about the future. The effectiveness of AI depends greatly on the quality of data, algorithms used and places where the technology is applied. Therefore, AI needs to be considered as an additional instrument of support for science and environmental management [13], [14].

One significant issue is data itself. Mountainous areas are difficult to examine due to numerous slopes, substantial variations in elevation, rapidly changing weather conditions, and significant discrepancies between microclimates. All these factors make it rather difficult to get consistent and representative data. Weather stations are unevenly distributed across highlands. Satellites also have trouble seeing through clouds, atmospheric disturbances, shadows of mountains, and snow cover. Thus, the models trained on the data might provide faulty and misleading outcomes in other mountain areas. This is especially evident in the case of Azerbaijan, with three mountain systems (the Greater Caucasus, Lesser Caucasus, and Talysh Mountains) having their distinct climates, geology, and ecology [1], [2].

In my opinion, algorithm bias and adaptability of machine learning algorithms in specific locations is another problem. The model developed with the use of data collected in a certain region would not necessarily perform well in another location due to differences in vegetation, precipitation, soil, and anthropogenic activity. Climate change adds an additional level of uncertainty as the historical patterns might not be suitable for predicting conditions. Due to the above-mentioned factors, AI models should be validated, adjusted, and verified with local data [13], [15]

Moreover, it seems essential that decision makers have an understanding of the meaning of AI predictions. Some AI models have high accuracy, but they are complicated. In such cases, explanations of why the model made a particular prediction are required. It is even more crucial when AI predicts environmental problems such as landslides, flood risks, ecological system impairment, or water management. Otherwise, the wrong prediction can cause wrong actions, financial expenditures, and missed threats. Therefore, environmental systems should be built on AI technology, modeling techniques, and measurement of uncertainty [14 15].

AI-based predictions should be viewed as less than 100% certain. It is well known that natural hazards have a probabilistic character. They depend on many interacting factors that cause the problem. Landslides, for instance, are caused by several factors like rains, wet soils, steep slopes, no vegetation, human impact. The most advanced algorithms can miss relationships between all those factors. Hence, it is necessary that the prediction be accompanied by the confidence level and uncertainties. The risk assessment categories should be clear. Environmental agencies should consider the results of AI, together with the empirical observations, scientific approach, and experts' opinion.

9. Conclusions And Recommendations

The protection of the mountains is vital for the region's water security, biodiversity, soil conservation, and sustainable development. Some of the major initiatives needed by Azerbaijan are the improvement of long-term ecological monitoring and watershed management in a unified system.

Author Contributions

The sole author is responsible for conceptualizing, collecting, and analyzing data, and writing and editing the manuscript

Conflict of Interest

The authors declare no conflicts of interest

Funding

This study received no external funding

References

- [1] Adler, C., Wester, P., Bhatt, I. və b. (2022). Cross-Chapter Paper 5: Mountains. In: Climate Change 2022: Impacts, Adaptation and Vulnerability (IPCC AR6, WGII). <https://www.ipcc.ch/report/ar6/wg2/chapter/ccp5/>
- [2] Hock, R., Rasul, G., Adler, C., Cáceres, B., Gruber, S., Hirabayashi, Y., ... & Zhang, Y. (2019). High mountain areas. In *IPCC special report on the ocean and cryosphere in a changing climate* (pp. 131-202). H.-O. Pörtner, DC Roberts, V. Masson-Delmotte, P. Zhai, M. Tignor, E. Poloczanska, K. Mintenbeck, A. Alegria, M. Nicolai, A. Okem, J. Petzold, B. Rama, NM Weyer (eds.). <https://www.ipcc.ch/srocc/chapter/chapter-2/>
- [3] United Nations. (2025). *The United Nations World Water Development Report 2025: Mountains and glaciers: Water towers*. UNESCO <https://www.unesco.org/reports/wwdr/en/2025>
- [4] Viviroli, D., Kumm, M., Meybeck, M., Kallio, M., & Wada, Y. (2020). Increasing dependence of lowland populations on mountain water resources. *Nature Sustainability*, 3(11), 917-928. <https://doi.org/10.1038/s41893-020-0559-9>
- [5] Körner, C. (2003). *Alpine plant life: Functional plant ecology of high mountain ecosystems* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-642-18970-8>
- [6] Brondizio, E. S., Settele, J., Diaz, S., & Ngo, H. T. (2019). *Global assessment report of the intergovernmental science-policy platform on biodiversity and ecosystem services*. IPBES. <https://doi.org/10.5281/zenodo.3831673>
- [7] Food and Agriculture Organization of the United Nations, & United Nations Environment Programme. (2020). *The state of the world's forests 2020: Forests, biodiversity and people*. <https://doi.org/10.4060/ca8642en>
- [8] Romeo, R., Vita, A., Testolin, R., & Hofer, T. (2015). Mapping the vulnerability of mountain peoples to food insecurity. <https://openknowledge.fao.org/handle/20.500.14283/i5175e>
- [9] Azərbaycan Respublikası Ekologiya və Təbii Sərvətlər Nazirliyi. *Milli parklar: Xüsusi mühafizə olunan təbiət əraziləri*. <https://eco.gov.az/az/tebii-servetlerimiz/milli-parklar>
- [10] United Nations Economic Commission for Europe. (2024). *Third environmental performance review of Azerbaijan*

- <https://unece.org/info/publications/pub/386688>
- [11] United Nations Office for Disaster Risk Reduction. (2022). *Global assessment report on disaster risk reduction 2022: Our world at risk: Transforming governance for a resilient future*.
<https://www.undrr.org/gar/gar2022-our-world-risk-gar>
- [12] Pettorelli, N., Laurance, W. F., O'Brien, T. G., Wegmann, M., Nagendra, H., & Turner, W. (2014). Satellite remote sensing for applied ecologists: opportunities and challenges. *Journal of applied ecology*, 51(4), 839-848.
<https://doi.org/10.1111/1365-2664.12261>
- [13] Reichstein, M., Camps-Valls, G., Stevens, B., Jung, M., Denzler, J., Carvalhais, N., & Prabhat, F. (2019). Deep learning and process understanding for data-driven Earth system science. *Nature*, 566(7743), 195-204.
<https://doi.org/10.1038/s41586-019-0912-1>
- [14] Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling climate change with machine learning. *ACM computing surveys (CSUR)*, 55(2), 1-96.
<https://doi.org/10.1145/3485128>
- [15] Karpatne, A., Atluri, G., Faghmous, J. H., Steinbach, M., Banerjee, A., Ganguly, A., ... & Kumar, V. (2017). Theory-guided data science: A new paradigm for scientific discovery from data. *IEEE Transactions on knowledge and data engineering*, 29(10), 2318-2331.
<https://doi.org/10.1109/TKDE.2017.2720168>

Digital Sovereignty for National Cybersecurity

Razil Mirzeyev¹ , Tofiq Mirzeyev¹ , Faig Musayev²  and Shakir Aliyev¹ 

¹Department of Design and Industrial Technologies, Azerbaijan Technological University, Ganja, Azerbaijan

²Department of Information Technology and Security, Azerbaijan Technological University, Ganja, Azerbaijan

Received: 04.09.2026

Accepted: 29.09.2026

Published: 09.10.2026

<https://doi.org/10.54414/RGMW6792>

Copyright: © 2026 by the authors.
Licensee: Journal of Smart Technologies and Computational Systems, Western Caspian University, Baku, Azerbaijan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract: In modern times, the rapid development of information technologies has led to the formation of new directions in the security policies of states. The digitalization process affects all sectors of the economy, public administration, and society. Alongside this process, cybersecurity issues are also becoming increasingly relevant. State information systems, strategic infrastructures, and personal data databases are exposed to various cyber threats. In this regard, the concept of digital sovereignty has become a crucial component of national security. Digital sovereignty refers to a state's ability to independently manage and protect its own information space, data, and digital infrastructure. This concept ensures the protection of the state's technological resources, databases, and communication systems against external influences. The article examines the essence of digital sovereignty, its role in the national cybersecurity system, and the strategies implemented by states in this area. Furthermore, issues regarding the development of local technologies, the protection of national databases, and the formulation of cybersecurity policy in ensuring information security were analyzed. The results of the study show that strengthening digital sovereignty enhances states' resilience against cyber threats and serves to protect national interests.

Keywords: digital sovereignty, cybersecurity, information security, national security, information technologies, cyber threats, digital infrastructure

1. Introduction

Cybersecurity emerged with the development of information technologies and has become an increasingly important field over time. Cybersecurity is a set of measures and technologies that ensure the protection of computer systems, networks, and data against unauthorized access, attacks, and malicious software. The emergence of this field is closely linked to the development of computers and the Internet. The history of cybersecurity begins with the advent of computers in the mid-20th century. The first electronic computers, created in the 1950s, were primarily used for military and scientific purposes. At that time, computers were not interconnected, and data security was ensured primarily through physical protection. In other words, the computers were kept in special rooms, and only certain individuals were permitted to use them. The creation of computer networks in the 1960s gave impetus to the development of the cybersecurity field. During this period, ARPANET, one of the first major computer networks, was created in the United States. This network facilitated the exchange of information among various universities and research centers. With the interconnection of computers, the issue of data protection and secure transmission became increasingly important [1].

The first computer viruses and malicious programs began to appear in the 1970s. In 1971, the Creeper Virus, considered one of the first computer viruses in history, was created. This virus spread across the

network and displayed a message on the computer screen. Subsequently, a program named Reaper was developed to remove this virus. This program is considered the first antivirus program in history. With the spread of personal computers in the 1980s, the number of viruses also increased. Many new malicious programs emerged during this period. One of them was Brain Virus, created in 1986. This virus is considered one of the first widely spread computer viruses in the world and primarily spread via disks.

The widespread adoption of the Internet in the 1990s further exacerbated cybersecurity issues. With the increase in the number of internet users, hacker attacks, data theft, spam, and other cybercrimes have also begun to rise. During this period, antivirus programs, firewall systems, and other security technologies were developed [2].

Since the 2000s, cybersecurity has become an increasingly strategic field. Banking systems, government agencies, companies, and individual users began to be targeted by cyberattacks. In the modern era, cybersecurity encompasses the protection not only of computers but also of mobile devices, cloud systems, and all technologies that operate via the internet. Artificial intelligence, encryption technologies, and modern defense systems are considered key tools in this field. Cybersecurity emerged alongside the development of computer technologies and has today become one of the most important areas of security in the world. In the modern information society, data protection is of great importance for states, organizations, and individual users alike. As a result of the rapid development of information technologies in the 21st century, the global economy and public administration have been integrated into the digital environment. The widespread adoption of the Internet, along with the use of cloud technologies, artificial intelligence, and big data, plays a significant role in the operations of states. At the same time, the digital environment also gives rise to new security risks.

Cybersecurity issues are among the most significant challenges facing states in the modern era. Attacks on the information systems of government agencies, data theft, and interference with the operation of critical infrastructure pose a serious threat to society. For this reason, states implement various strategies to protect their information space and ensure their independence in the digital environment. It is precisely in this context that the concept of digital sovereignty has emerged. This concept entails states exercising control over their digital resources and ensuring their security. Digital sovereignty encompasses not only technical issues but also legal, political, and economic aspects. In modern times, many states pay special attention to the issue of digital sovereignty in their national cybersecurity strategies. The development of local technologies, the protection of national databases, and the training of cybersecurity specialists are among the key measures being implemented in this field.

2. Relevance of the topic

The acceleration of the digitalization process and the widespread adoption of internet technologies have made the issue of cybersecurity even more pressing. Cyber threats pose a serious risk because government institutions, banking systems, energy infrastructure, and other strategic sectors rely on digital systems. For this reason, the issue of digital sovereignty occupies a significant place in the security policies of states. Protecting information resources and ensuring independence in the digital environment is one of the key priorities for states in the modern era.

3. The aim of the study

The main objective of this study is to examine the role of digital sovereignty in the national cybersecurity system and to analyze the existing challenges in this field. The objectives of the study are as follows:

- to define the essence of the concept of digital sovereignty;
- to examine its role in the national cybersecurity system;
- to analyze the strategies implemented by states in this area;

4. Object of the study

The object of the study is the role of digital sovereignty in ensuring national cybersecurity and its impact on the state's information security. In the study, the digital infrastructure, information systems, databases, and cybersecurity strategies of states were taken as the primary objects of research. In this context, cyber threats emerging in the digital environment, data protection mechanisms, and measures implemented by states to ensure digital sovereignty have been examined. Issues regarding the protection of national information resources and the enhancement of technological independence are also included in the main scope of the research.

5. Novelty of the research

The scientific novelty of the research lies in the comprehensive analysis of the concept of digital sovereignty within the context of national cybersecurity. The study systematically examines the impact of digital sovereignty on state security, its formation mechanisms, and the challenges arising in the modern era. Furthermore, a comparative analysis of the cybersecurity strategies of various countries was conducted, and modern approaches implemented to ensure digital sovereignty were identified. This approach has enabled a broader and more up-to-date exploration of the topic.

6. Practical significance of the research

The results of the research are of practical importance for the development of the national cybersecurity system and the strengthening of digital sovereignty. The research findings may be useful for government agencies, organizations operating in the information technology sector, and cybersecurity specialists. Furthermore, the research findings can be used in the educational process within the fields of information security and cybersecurity. These materials can help students in higher education institutions acquire broader and more systematic knowledge of the subject.

7. Materials and discussions.

Digital sovereignty is considered one of the key principles in ensuring national cybersecurity. This concept entails state control over digital infrastructure, databases, and communication systems. Many countries are paying special attention to the development of domestic software and hardware to reduce dependence on foreign technologies. This both increases economic independence and reduces cybersecurity risks. Excessive reliance on foreign platforms and technologies can negatively affect the information security of states. The following areas are of great importance for ensuring digital sovereignty. Furthermore, the recommendations put forward in the article can support the development of practical measures aimed at enhancing security in the digital environment and protecting national information resources.

Development of national information infrastructure- States ensure that data is stored within the country by developing their own data centers and server systems. Formulation of a cybersecurity strategy. National cybersecurity strategies aim to ensure the information security of government agencies and the private sector. Data protection and privacy assurance. Specific legislative and technical mechanisms are implemented to protect personal data. Training cybersecurity specialists. Training information security specialists in educational institutions plays a crucial role in strengthening digital sovereignty. Discussions indicate that digital sovereignty is not merely a technological issue but also a crucial aspect of state policy. The measures implemented by states in this area enhance their resilience against cyber threats [3].

8. Research method

Various scientific methods were used during the research process. Methods of comparative analysis, analysis of scientific literature, and an analytical approach were primarily employed. To investigate the topic, reports from international organizations, scientific articles, and studies on information security were

examined. Furthermore, the cybersecurity strategies of various states were compared, and the measures taken to ensure digital sovereignty were analyzed. Through an analytical method, the role of digital sovereignty within the national security system has been determined, and existing problems in this area have been examined [4], [5].

9.Result

Research shows that digital sovereignty is one of the key elements of national cybersecurity in the modern era. Protecting the information resources of states and ensuring the security of their digital infrastructures play a crucial role in safeguarding national interests. The development of local technologies, the formulation of cybersecurity strategies, and the training of specialists are of great importance for strengthening digital sovereignty. These measures enhance the resilience of states against cyber threats and ensure their independence in the digital environment. In conclusion, it can be said that digital sovereignty is not merely a technological issue but also one of the strategic aspects of state security.

Author Contributions

The sole author is responsible for conceptualizing, collecting, and analyzing data, and writing and editing the manuscript

Conflict of Interest

The authors declare no conflicts of interest

Funding

This study received no external funding

References

- [1] Anisimov, A. A. (2009). *Menedzhment v sfere informatsionnoy bezopasnosti* Internet-Universitet Informatsionnykh Tekhnologiy; BINOM. Лаборатория знаний.
- [2] Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know®*. Oxford University Press.
<https://doi.org/10.1093/wentk/9780199918096.001.0001>
- [3] Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.
- [4] Yusupov, R. M., & Shishkin, V. M. (2013). Informatsionnaya bezopasnost i kiberbezopasnost: Semanticheskiy konflikt ili sosushchestvovanie. *Informatizatsiya i svyaz*, (6), 22–27.
- [5] Shishkin, V. M. (2011). Pokazateli nadyozhnosti i bezopasnosti: Vozmozhnosti nelineynogo perekhoda. *Trudy Mezhdunarodnogo simpoziuma "Nadezhnost i kachestvo"*, 1, 101–103.

WESTERN CASPIAN UNIVERSITY

Journal of Smart Technologies and Computational Systems

Volume 1, Number 3, October 2026, 54 p

Editorial Office Address: 17A, Ahmad Rajabli Street, III Parallel, Baku, Azerbaijan

E-mail: smarttechjournal@wcu.edu.az

<https://smarttechjournal.wcu.edu.az/>

Tel: +994 12 565 39 77

The editorial office is not responsible for the author's position.

When using materials, reference to the journal is required.

Submitted for collection: 09.10.2026

Print signed: 13.10.2026