ARI®
SIMULATION
A SUBSIDIARY OF ZEN TECHNOLOGIES

ZEN TECHNOLOGIES
being there...

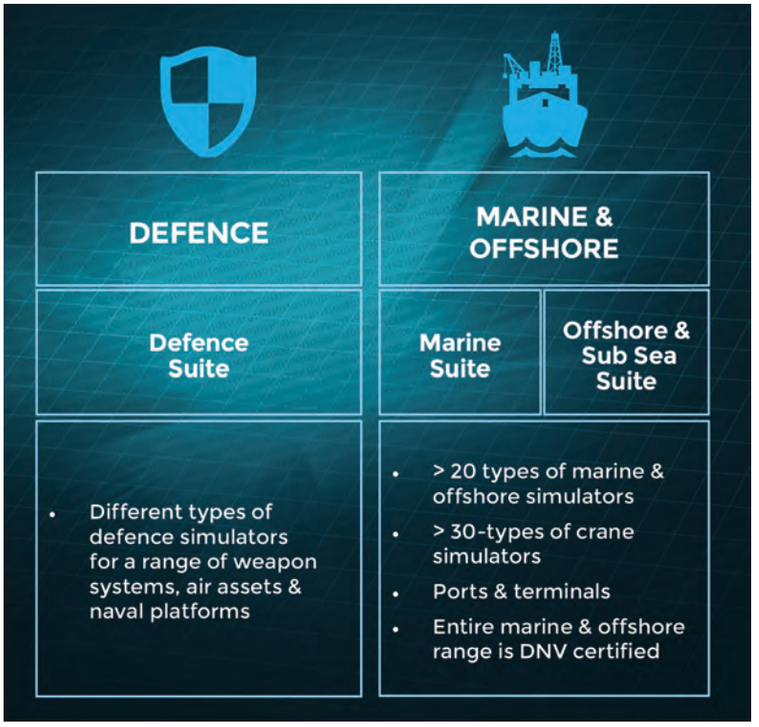
CYBER SECURITY SUITE

INTEGRATED 6-LAYER DEFENCE ECOSYSTEM

www.arisimulation.com

OVERVIEW

Applied Research International (ARI), the naval and marine simulation arm of Zen Technologies Limited, is a global leader in the production of sophisticated simulation and virtual reality training solutions for the defence, marine & offshore industries.



At the forefront of innovation, our simulators stand as the pinnacle of excellence, meticulously crafted to adhere to the highest international standards set by respected industry authorities like the International Maritime Organization (IMO), Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) 2010, The Nautical Institute, Offshore Petroleum Industry Training Organisation (OPITO), Association of Marine Electronic and Radio Colleges (AMERC), International Marine Contractors Association (IMCA), and more. Our marine, offshore, and crane simulation solutions have achieved the prestigious Class A Standard certification from Det Norske Veritas (DNV), exemplifying our commitment to excellence.

Built on the proven and certified simulation technology, ARI's products are built to military grade standards and add a considerable set of unique defence related features. Our technologies are used by multiple armed forces all over the world.

From operations to tactical and strategic evaluation; from electronic warfare to troop movement planning, our simulators can be deployed in a variety of roles. Participants can visualise tactical inputs, analyse multiple courses of action and evaluate a range of decision response scenarios in a combat or mobilisation environment.

CYBER SECURITY SUITE

INTEGRATED 6-LAYER DEFENCE ECOSYSTEM

The Challenge

Defence networks face threats at every level – from social engineering at the perimeter to advanced persistent threats moving laterally inside. No single product addresses the full attack surface. Organisations deploy fragmented tools from multiple foreign vendors, each with its own licensing, cloud dependencies, and data sovereignty risks. The result: gaps between layers, blind spots between tools, and critical reliance on foreign infrastructure for national security.

Our Answer

ARI's Cybersecurity Solutions is an integrated 6-layer defence ecosystem – 8 indigenous products that cover the entire security lifecycle from awareness to deception. Every product is designed, developed, and deployed in India. No foreign cloud. No foreign AI services. No foreign encryption dependencies. One vendor. One sovereign stack.

LAYER 1 — AWARENESS & TRAINING

- Phishing & Vishing Simulator

LAYER 2 — MONITORING & INTELLIGENCE

- OSINT Intelligence Platform

LAYER 3 — PROTECTION & PREVENTION

- AegisNex Insider Threat Control System
- VAPT & STIG Platform

LAYER 4 — ENCRYPTION & DATA SOVEREIGNTY

- Suraksha Encryption SDK
- Suraksha-Net

LAYER 5 — THREAT DECEPTION

- Cyber Deception Framework (Honeypot)

LAYER 6 — INVESTIGATION & RESPONSE

- Forensic Disk Imager

POST-QUANTUM READY • CRYPTO-AGILE • ZERO FOREIGN DEPENDENCIES • ON-PREMISES • ATMANIRBHAR BHARAT

PHISHING AND VISHING SIMULATIONS

THE PROBLEM

91% of cyber attacks start with a phishing email. Defence personnel are targeted by nation-state actors using sophisticated social engineering. One click on a crafted email can compromise an entire classified network. Traditional awareness training is passive and forgettable — personnel need to experience real attack simulations to build instinct.

KEY CAPABILITIES

- **Simulated campaigns:** Craft realistic phishing emails, SMS, and voice (vishing) attacks targeting your own personnel
- **50+ attack templates:** Credential harvesting, malware attachment, URL redirect, QR code, spear-phishing
- **Real-time dashboard:** Who opened, who clicked, who submitted credentials, who reported
- **Vulnerability scoring:** Per user, team, and unit – with department-wise risk heat maps
- **Progressive difficulty:** Campaigns get harder as personnel improve
- **Instant feedback:** User clicks phishing link - gets immediate educational intervention explaining what they missed
- **Recurring campaigns:** Monthly, quarterly, or event-triggered – continuous security posture assessment
- **Compliance reporting:** CERT-In and ISO 27001 awareness requirements

Your People Are Your Weakest Link — Until You Train Them Under Fire.

OSINT INTELLIGENCE PLATFORM

THE PROBLEM

Adversaries communicate, recruit, plan, and signal intent on open sources — social media, forums, dark web, news, paste sites. Manually monitoring these sources is impossible at scale. Defence needs AI-powered, continuous, multilingual monitoring that converts raw open-source noise into verified, geotagged, actionable intelligence.

KEY CAPABILITIES

- **Multi-platform connectors:** YouTube, X/Twitter, Reddit, Meta, Telegram, Paste Sites, news aggregators, forums, and more
- **3-layer web coverage:** Surface web, deep web, and dark web (Tor) from a single platform
- **AI/NLP engine:** Sentiment, entity extraction, topic clustering, narrative tracking across 55 languages
- **Person-of-interest tracking:** Persistent profiles with cross-platform activity correlation
- **Hybrid deepfake detection:** Frequency-domain artefact analysis + ML classifiers for image/video authenticity
- **Query intelligence:** Natural-language question source-cited answer powered by local LLM (RAG)
- **GIS intelligence:** Every data point geotagged – heat maps, temporal overlays, interactive maps
- **Alert engine:** Priority scoring: source credibility × content risk × entity relevance × temporal urgency
- **Reports:** PDF, Word, PowerPoint with embedded GIS maps – analyst-ready in minutes
- **On-premises deployment:** No foreign AI services or cloud APIs. All AI models deployed locally within Indian infrastructure.

The internet talks. We listen, verify, and deliver actionable intelligence.

LAYER 3

PROTECTION & PREVENTION

AEGISNEX INSIDER THREAT CONTROL SYSTEM

THE PROBLEM

Sensitive data leaves organisations through USB drives, email attachments, cloud uploads, print jobs, and screen captures — often undetected until the damage is done. Insider threats are the hardest to detect because the attacker has legitimate access. Defence organisations need real-time visibility into every data movement with policy-enforced control.

KEY CAPABILITIES

- **Network traffic analysis:** Monitors all data in motion across the network in real-time
- **File tracking:** Knows where every sensitive file is, who accessed, copied, or moved it
- **USB/removable media:** Block, allow, or audit all USB device activity per policy
- **Sensitive data detection:** Fingerprints classified documents, PII, credentials, and custom patterns
- **Policy engine:** Configurable rules per classification level, department, user role – block, alert, or log
- **Email insider threat control system:** Scans outbound email for sensitive content before it leaves the network
- **Screen + clipboard:** Prevents screen capture and clipboard exfiltration of classified content
- **Endpoint agent:** Lightweight, tamper-resistant, works offline
- **Risk scoring:** Per-user risk score based on behaviour patterns and policy violations
- **Compliance:** DPDP Act and IT Act compliance reporting

If sensitive data moves, we see it. If it shouldn't move, we stop it.

VAPT & STIG COMPLIANCE PLATFORM

THE PROBLEM

Defence networks run hundreds of services, servers, and endpoints — each a potential entry point. Without continuous vulnerability assessment, security teams don't know what's exposed until an attacker finds it first. Manual penetration testing is expensive, slow, and point-in-time. Compliance with STIG hardening benchmarks requires systematic, repeatable checking — not spreadsheets.

KEY CAPABILITIES

- **Network vulnerability scanning:** Automated host discovery, service detection, and vulnerability identification across the entire network
- **Web application scanning:** OWASP-aligned security testing for web applications – injection, XSS, misconfiguration, authentication flaws
- **Credentialed scanning:** Authenticated scans across 15+ service families – SSH, SMB, RDP, databases, LDAP – for deeper vulnerability discovery
- **Scan profiles:** Fast, standard, and deep scan modes – balance speed vs thoroughness based on operational need
- **Severity scoring:** CVSS-based risk scoring with OWASP mapping – prioritise remediation by actual risk, not volume
- **STIG compliance:** Automated Security Technical Implementation Guide checks against hardening benchmarks – systematic, repeatable, auditable
- **Scheduled + manual:** Recurring scans on schedule or on-demand manual testing with service/check filtering
- **Reporting:** Standard and audit-oriented PDF reports – management-ready with findings, severity, and remediation guidance
- **Centralised dashboard:** Real-time scan progress, completed scan history, severity trends, and compliance status at a glance
- **Scalable:** Distributed execution via background workers – scales from single-site to enterprise-wide deployments

Know your vulnerabilities before the attacker does. Prove your compliance before the auditor asks

LAYER 4

ENCRYPTION & DATA SOVEREIGNTY

SURAKSHA ENCRYPTION SDK

THE PROBLEM

India's classified communications and sensitive data need post-quantum cryptographic protection today — not when quantum computers arrive. Foreign encryption libraries create dependency and potential backdoor risk. Defence needs an indigenous, NIST-compliant, hardware-enhanced encryption engine that can be embedded into any application, device, or platform.

KEY CAPABILITIES

- **Crypto agility:** Algorithm-agnostic architecture. Swap encryption primitives as standards evolve without changing applications. Future-proof by design.
- **Post-quantum ready:** Protects classified data against future quantum computing threats. Compliant with latest NIST post-quantum standards.
- **Hybrid approach:** Classical + post-quantum algorithms running together. Security equals the stronger of both. If either holds, your data is safe.
- **Forward secrecy:** Compromise of one session exposes nothing else – past and future sessions secure
- **Hardware-enhanced keys:** Leverages hardware security where available, with secure fallback on any platform
- **Full key lifecycle:** Automatic generation, rotation, retirement, and revocation. Zero key reuse.
- **Classification-aware:** Enforces clearance levels at the encryption layer itself – operations denied, never silently degraded
- **Cross-platform:** Desktop, mobile, embedded, and server – single lightweight library
- **Production-tested:** Verified across desktop and embedded hardware platforms
- **Indigenous:** Zero foreign cryptographic dependencies. Full source code ownership. Atmanirbhar compliant.

Sovereign encryption. Crypto-agile. Post-quantum ready. Zero foreign dependencies.

SURAKSHA-NET

Secure Communication Platform

THE PROBLEM

Military units exchange classified information over public internet and across air-gapped networks. Current methods — email, messaging apps, USB drives — are insecure, unauditable, and vulnerable to interception. Foreign communication platforms cannot be trusted for classified defence communications. India needs an indigenous, end-to-end encrypted, post-quantum-secure communication platform.

KEY CAPABILITIES

- **E2E encrypted:** Messaging, file transfer, and real-time streaming (voice, video, telemetry)
- **Post-quantum:** Hybrid classical + quantum-resistant key exchange per session – future-proof
- **Forward secrecy:** Every conversation uses fresh keys – compromise of one exposes nothing else
- **Identity-based:** User-to-user and group channels by identity (name, role, unit) – not IP
- **Server-zero-knowledge:** Server relays ciphertext only – cannot access plaintext under any condition
- **Cross-platform:** Desktop (primary) + mobile (supported) + embedded endpoint client
- **Remote lock + wipe:** Lost device → keys destroyed, data irrecoverable
- **Classification-aware:** Fail-closed policy engine prevents unauthorised exchange across clearance levels
- **Double encryption:** Two independent encryption layers – attacker must break both to access any data
- **Streaming encryption:** Evolving keys for real-time tactical communication

HOW IT WORKS

Sender encrypts → Encrypted tunnel → Server relays ciphertext (cannot decrypt – has no keys) → Encrypted tunnel → Receiver decrypts

Your messages. Your keys. No server, no adversary, no one else can read them.

CYBER DECEPTION FRAMEWORK

Honeypot System

THE PROBLEM

Traditional defences (firewall, AV, EDR) try to keep attackers OUT. But once inside — through phishing, zero-day, or insider — the attacker moves freely. There is nothing inside the network that detects lateral movement, credential theft, or data targeting. Defence networks need an active trap layer: realistic fake assets that only an attacker would touch.

6 DECOY CATEGORIES

DECOY TYPE		WHAT IT CATCHES
Service decoys	:	Fake SSH, RDP, SMB, DNS — catches reconnaissance and unauthorised access
Server decoys	:	Fake AD, database, mail server — catches lateral movement and data targeting
File decoys (honey files)	:	Sensitive-named files on real endpoints — any access = instant alert
User decoys (honey tokens)	:	Fake credentials in AD — catches credential theft and pass-the-hash
Endpoint decoys	:	Ghost workstations on network — catches network scanning and lateral movement
Application decoys	:	Fake admin panels, VPN pages — catches web attacks and credential harvesting

HOW IT WORKS

Attacker enters network → Touches decoy → AI detects + classifies (MITRE ATT&CK) → Full session recorded → SOC alerted + auto-response

Record & replay: Complete forensic recording of every attacker session – commands, files, credentials, timeline

AI/ML: Behavioural anomaly detection, TTP classification, attacker session clustering

SIEM integration: Syslog, CEF, STIX/TAXII – fits any existing SOC workflow

The attacker doesn't know what's real. We know exactly what they touched.

INVESTIGATION & RESPONSE

FORENSIC DISK IMAGER

THE PROBLEM

When a cyber incident occurs — breach, insider theft, malware infection — investigators need an exact, unaltered copy of the compromised device's storage. If evidence is tampered with (even accidentally), it's inadmissible. Defence and law enforcement need forensic-grade imaging that is legally defensible, tamper-evident, and chain-of-custody proven.

KEY CAPABILITIES

- **Bit-for-bit imaging:** Exact, verifiable copy of any storage device – HDD, SSD, USB, NVMe, SD card
- **Write-blocking:** Source device never modified during imaging – hardware-enforced read-only
- **Hash verification:** SHA-256 and MD5 computed during imaging – any tampering detectable
- **Chain-of-custody:** Every action timestamped, operator-identified, cryptographically tamper-evident
- **Multiple formats:** Industry-standard forensic output formats
- **Compression + encryption:** Images compressed for storage, Encrypted for secure transport
- **Parallel imaging:** Image multiple devices simultaneously
- **Evidence packaging:** Complete evidence bundle – imaging log, hash report, chain-of-custody certificate
- **Portable:** Runs on standard laptops or dedicated workstations – no internet required
- **Court-admissible:** Meets forensic standards for legal proceedings

Capture the truth. Preserve it. Prove it in court.

ARI®
SIMULATION
A SUBSIDIARY OF ZEN TECHNOLOGIES

Applied Research International Pvt. Ltd.

SALES & CUSTOMER SERVICES

ARI WORLDWIDE

With operations, partners and representatives around the world, an ARI representative is only a mouse click away.
Drop us a mail at info@arisimulation.com and an ARI representative will get back to you promptly.

India
E-44/14, Okhla Industrial Area, Phase II,
New Delhi - 110020, India.
Tel +91-11-41326882
email: info@arisimulation.com

USA
Bishop Ranch 3, 2603 Camino Ramon, Suite
200, San Ramon, California, 94583, USA.
Tel: +1 408 338 6093
email: ariusa@arisimulation.com

Singapore
14 Robinson Road, #08-01A, Far East
Finance Building, Singapore 048545
email: arisingapore@arisimulation.com

www.arisimulation.com

ZEN TECHNOLOGIES
being there...