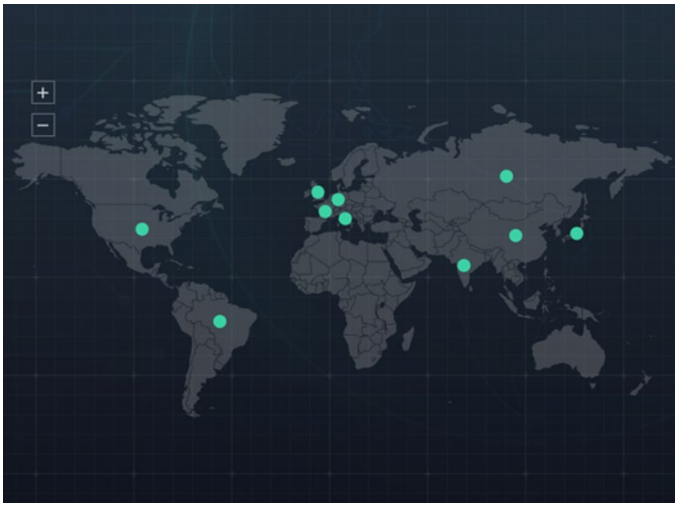
ARA SYSTEM

# CONTROL SOFTWARE (PAL-CS) DATASHEET



The PALAMYS system (Controlled/Customizable Strategic DDoS) is a purpose-built DDoS simulation and penetration-testing platform designed for special units and cyber-range operators who need the most realistic, operationally relevant attack emulation. Developed from real-world cyber-warfare observations and modern DDoS trends, PALAMYS combines powerful, field-proven attack techniques with an operator-friendly control surface so teams can design, schedule, execute and analyze realistic denial-of-service scenarios without excessive operational overhead.

PALAMYS replicates modern adversary behavior across volumetric, protocol and application layers while giving defenders the observability and repeatability required for high-value training and readiness exercises. The system was architected to reflect cyber threat evolution — from amplified reflection attacks and IoT/VM-based botnets to sophisticated HTTP/2 and browser-emulation application floods — and to let blue teams test detection, mitigation and incident-response playbooks under controlled but realistic pressure.

**Key capabilities:**

- High-impact volumetric & reflection attacks: generate amplified/reflective traffic against web apps, DNS, NTP, COAP, WSD and other vulnerable services to emulate real amplification campaigns.
- Autonomous discovery & augmentation: continuously scan the Internet to discover additional reflector/attack nodes and automatically incorporate them into campaigns.
- Botnet lifecycle management: add, remove and orchestrate attack nodes (bot/VM/reflector fleets) with fine-grained control over behavior, persistence and geographic distribution.
- Scheduled, automated campaigns: create reusable scenarios and run full attack playbooks on demand or on a calendar to support exercises and long-term readiness validation.
- Target reconnaissance & adaptive strategy: automated target profiling (application fingerprinting, API discovery, CDN/WAF detection, origin IP tracing) and automated selection of the most effective attack vectors.
- Visual attack path mapping: interactive visualizations of attack flows, vectors and impact metrics so operators can explain lessons learned to technical and non-technical stakeholders.

## Control Software (PAL-CS)

The Control Software is the central management console for the PALAMYS DDoS simulation system. It provides operators with a unified interface to monitor platform health, plan and execute attack campaigns, manage attack resources, and keep a complete, auditable record of all actions. Designed for use by specialised cyber-range teams and defensive units, the Controller balances powerful automation with precise operator control so exercises are repeatable, measurable and safe.

**Functional highlights**

- **System resource management**

System resource and status statistics, including the status of related system components such as CPU, RAM, storage, network throughput, and the software/software modules running on server services . All metrics are presented in dashboards.

- **Historical activity records**

Storage, statistics of historical logs of activities to executed network attack tasks, target information and identifiers, execution results. Historical data is searchable.

- **Command & Control (manual & automated modes)**

Functions for configuring targets, attack plans to build and launch campaigns in two modes:

  - *Manual mode:* specify attack technique/method, schedule (start time, duration, frequency/repeat), and traffic magnitude/throughput.
  - *Automated mode:* System automatically calculates and builds attack plans. For a given target, the system automatically selects an optimal attack vector and tuning parameters based on reconnaissance results.

- **Live attack visualization**

Interactive, real-time maps: Monitor real-time attack map showing the movement and routing of bots toward targets, including geographic/ASN coordinates and per-node contribution, enabling intuitive situational awareness during exercises.

- **Botnet Control, update and expansion**

Provide statistics on the number, types of compromised machines (botnet nodes), and visibility into the aggregate attack potential traffic/throughput that can be . Supports management of vulnerability/exploit artifacts (status, quantity, metadata) and the ability to add vulnerability/exploit information to the library.

Botnet expansion options include: ingesting threat-intel feeds to add/remove discovered bot addresses; automated scanning for additional vulnerable infrastructure (minimum support for commonly abused services such as DNS, NTP, SNMP and COAP misconfigurations, unsecured configurations);

Botnet expansion Horizontally scale attack-emulation hosts by adding server infrastructure to expand attack-emulation hosts to generate more threads (equivalent to a VM-based bot). Each added server can emulate up to **10,000** VM-based bots when provisioned to the specified server profile (8-core CPU, 16 GB RAM, 100 GB storage, 10 Gbps network).

- **Result tracking for expansions**

Manage the results of expanding and updating the botnet system: which hosts were added, their exploit status, and the updated aggregate capacity.

- **User and role management**

Native authentication with username/password and support for hardware-backed two-factor authentication via USB security tokens. Role-based permissions separate duties into distinct profiles: Technical Administrator; Activity Moderator/Auditor; Attack Operations Operator; Network Update Operations Operator.

- **Comprehensive logging & audit trail**

System Log Monitoring feature: Allows comprehensive monitoring of all system logs, including: authentication actions (logins/logouts), command execution activities, system configuration change activities, scanning and system-expansion activities. Logs are indexed for rapid search and long-term retention.