



International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Operating Publisher
SciFormat Publishing Inc.
ISNI: 0000 0005 1449 8214

2734 17 Avenue SW,
Calgary, Alberta, T3E0A7,
Canada
+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	CYBERSECURITY OF IoT DEVICES IN THE INTERNAL NETWORKS OF MILITARY UNITS AND ORGANIZATIONS
----------------------	---

DOI	https://doi.org/10.31435/ijitss.3(51).2026.6692
------------	---

RECEIVED	23 July 2026
-----------------	--------------

ACCEPTED	11 September 2026
-----------------	-------------------

PUBLISHED	25 September 2026
------------------	-------------------

LICENSE	 The article is licensed under a Creative Commons Attribution 4.0 International License .
----------------	--

© The author(s) 2026.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

CYBERSECURITY OF IoT DEVICES IN THE INTERNAL NETWORKS OF MILITARY UNITS AND ORGANIZATIONS

Unenbat Erdenesuvd

PhD candidate in Defence and Security Studies, National Defense University of Mongolia; Head of the Department of Information Technology, Ider University, Ulaanbaatar, Mongolia
ORCID ID: 0009-0002-5135-3001

Nergui Bayartogtokh

Colonel, Ph.D., Associate Professor, Chief of Policy Analysis Center, Defense Research Institute of Mongolia
ORCID ID: 0009-0009-0276-2125

Batbayar Densmaa

Associate Professor, Ph.D., Department of Cybersecurity, Mongolian University of Science and Technology, Ulaanbaatar, Mongolia
ORCID ID: 0000-0002-1016-9622

ABSTRACT

The digital transformation of the defense sector has expanded the use of Internet of Things devices in the internal networks of military units and organizations. These devices include IP cameras, access-control systems, biometric equipment, smart displays, multifunction printers, conferencing systems, building-management systems, environmental sensors, and smart meters. They improve operational efficiency, monitoring, and automation, but they also enlarge the cyberattack surface because of weak credentials, outdated software, vendor-managed cloud services, automatic device-discovery protocols, limited logging, and long service lifecycles. In a military organization, the consequences extend beyond the loss of information confidentiality. A compromised device may disclose the location and layout of facilities, security routines, personnel movements, and logistics patterns; provide a foothold for lateral movement within the internal network; and ultimately disrupt mission continuity.

This study identifies the principal attack surfaces, threats, and vulnerabilities associated with IoT devices in military internal networks and develops a mission-oriented risk-assessment method and a security model based on zero-trust principles. The research comparatively examines Mongolian cybersecurity legislation and authoritative sources, including NIST CSF 2.0, NISTIR 8259A, NIST SP 800-213, NIST SP 800-207, NIST SP 800-82 Rev. 3, ETSI EN 303 645, and MITRE ATT&CK. The findings show that military IoT risk is not confined to technical vulnerabilities at the device level. It also arises from incomplete asset inventories, flat network architectures, uncontrolled vendor remote access, cloud dependency, and weak lifecycle governance. The study proposes a five-zone network architecture, evidence-based risk assessment, and integrated security measures covering the entire lifecycle from procurement to disposal.

KEYWORDS

Internet of Things, IoT Device, Military Internal Network, Cybersecurity, Attack Surface, Zero Trust, Microsegmentation, Residual Risk

CITATION

Erdenesuvd, U., Bayartogtokh, N., & Densmaa, B. (2026). Cybersecurity of IoT devices in the internal networks of military units and organizations. *International Journal of Innovative Technologies in Social Science*, 3(51). [https://doi.org/10.31435/ijitss.3\(51\).2026.6692](https://doi.org/10.31435/ijitss.3(51).2026.6692)

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

1 Introduction

The Internet of Things, or IoT, is an integrated system of network-connected physical devices, sensors, software, and supporting services that can collect, process, and transmit data and perform defined actions automatically. Military units and organizations use IoT technologies in many areas, including surveillance cameras, biometric access-control systems, fire and motion sensors, warehouse monitoring, energy management, vehicle tracking, building automation, and conferencing equipment.

IoT devices differ from conventional computers in several important respects. They often have limited computing resources, purpose-built software, a high degree of vendor dependency, long service lives, no practical means of installing endpoint security software, and limited logging and monitoring capabilities. The security of some devices also depends on several external components, including mobile applications, vendor servers, cloud platforms, third-party libraries, and update-distribution infrastructure.

Research on the Mirai botnet demonstrated with empirical data that large-scale attacks can be conducted through IoT devices protected by weak or factory-default passwords; at its peak, the botnet infected approximately 600,000 devices (Antonakakis et al., 2017). This case showed that cameras, routers, and embedded systems cannot safely be treated as simple peripheral devices.

The compromise of an IoT device in a military internal network may produce the following serious consequences.

- creation of an indirect path to command-and-control information
- disclosure of locations, facility layouts, and security procedures
- loss of video, audio, biometric, and personnel information
- creation of an initial foothold for lateral movement within the internal network
- disruption of access control, surveillance, fire-alarm, and power systems
- external dependency through a vendor cloud platform
- limited digital evidence for detecting and proving an attack

IoT cybersecurity therefore cannot be reduced to changing passwords or installing antivirus software. It requires integrated governance of procurement, the supply chain, network architecture, identification and authentication, software updates, monitoring, incident response, and secure disposal.

1.1 Research Aim

This study aims to identify the cybersecurity risks of IoT devices used in the internal networks of military units and organizations, develop a mission-oriented assessment method, and propose a security architecture and policy recommendations consistent with zero-trust principles.

1.2 Research Objectives

The study pursues the following objectives.

1. Classify the types, data flows, and attack surfaces of IoT devices used in military organizations.
2. Identify threats and vulnerabilities associated with devices, networks, vendor services, and human factors.
3. Compare international standards with the legal requirements of Mongolia.
4. Develop a risk-assessment model that accounts for effects on mission performance.
5. Propose an integrated model for network zoning, microsegmentation, device identification, monitoring, and incident response.
6. Define implementation phases and performance indicators.

1.3 Research Questions

The study addresses the following research questions.

- Which types of IoT devices and protocols create the largest attack surfaces in the internal networks of military units and organizations?
- How should IoT risk be assessed in relation to mission performance, confidentiality, integrity, availability, and physical safety?
- Which zero-trust architecture is suitable for a military internal network?
- What security requirements should apply at each stage of the IoT device lifecycle?

1.4 Research Contribution

Rather than assessing technical vulnerabilities in isolation, this study proposes a mission-oriented model that integrates device risk, information confidentiality, effects on the physical environment, mission continuity, vendor and supply-chain dependencies, and the demonstrated effectiveness of security controls. It also proposes a five-zone network classification comprising classified, mission, facility, administrative, and guest environments.

2 Theoretical and Methodological Foundations

2.1 Characteristics of IoT Cybersecurity

IoT security extends beyond information confidentiality, integrity, and availability. It also encompasses device authenticity, software integrity, physical safety, resilience, and mission assurance.

NISTIR 8259A groups the core cybersecurity capabilities of IoT devices into the following six categories (Fagan et al., 2020).

- Uniquely identify the device.
- Securely manage device configuration.
- Protect data that the device stores, processes, and transmits.
- Restrict access to logical interfaces.
- Securely update software.
- Report the device's cybersecurity state.

NIST SP 800-213 recommends aligning these capabilities with organizational system risk and procurement requirements (Fagan et al., 2021). ETSI EN 303 645:2024 establishes baseline requirements such as eliminating universal default passwords, maintaining a vulnerability-disclosure mechanism, updating software in a timely manner, protecting sensitive data, and minimizing the attack surface (ETSI, 2024).

2.2 Zero Trust Principles

Zero trust does not treat a device or user as trustworthy merely because it is located inside the organization's network. Every access request is evaluated against device identity, user privileges, device posture, the requested resource, environmental conditions, and risk. NIST SP 800-207 defines zero-trust architecture as a shift from implicit trust based on network location to controls centered on users, devices, and resources (Rose et al., 2020).

The U.S. Department of Defense Zero Trust Strategy organizes implementation around mutually reinforcing pillars for users, devices, applications, data, networks, automation, and visibility. This provides a relevant model for military environments (DoD CIO, 2022).

Direct implementation is difficult for legacy IoT devices with limited resources or no certificate support. Such devices require compensating controls through security gateways, network access control, dedicated security zones, proxy servers, and microsegmentation.

2.3 Legal and Regulatory Environment of Mongolia

Mongolia's 2021 Law on Cybersecurity establishes the institutional, legal, and operational foundations for protecting the confidentiality, integrity, and availability of information in cyberspace. State-owned legal entities must adopt internal procedures, implement recommendations issued by competent authorities, report cyberattacks and incidents, allocate the necessary budget, and retain system activity logs (State Great Khural of Mongolia, 2021a).

The National Cybersecurity Strategy, approved by Government Resolution No. 493 of 2022, sets objectives for protecting critical information infrastructure, developing human resources, strengthening cooperation, and improving cyber-incident response capability. The period 2026-2027 constitutes the second phase of the strategy (Government of Mongolia, 2022).

The General Procedure for Ensuring Cybersecurity, approved as an annex to Government Resolution No. 224 of 2023, requires each organization to adopt internal procedures appropriate to the nature and scale of its activities and to update them annually and after every material change to its systems or networks (Government of Mongolia, 2023). Joint Orders Nos. A/30 and A/148 of 2024 approved the national procedure and methodology for cybersecurity risk assessment (Minister of Digital Development, Innovation and Communications & Director General of the General Intelligence Agency, 2024).

Cameras, biometric devices, and access-control systems can process images, audio, location data, and biometric identifiers and are therefore also subject to the Law on the Protection of Personal Information (State Great Khural of Mongolia, 2021b). Devices that process state or official secrets must comply with the Law on State and Official Secrets and the procedures adopted under that law (State Great Khural of Mongolia, 2016).

Consumer-grade IoT devices that require persistent connections to vendor cloud servers should therefore not be connected directly to networks that process state or official secrets. Where a specialized device is operationally necessary, its use should be based on approval by the competent authority, a documented risk assessment, and a purpose-built security architecture.

3 Research Methodology

3.1 Research Design

The study combines qualitative document analysis, comparative analysis, threat modeling, a risk matrix, and security-architecture design. It does not rely on unauthorized scanning or vulnerability exploitation in operational military networks. Instead, it is an applied model-based study grounded in open and primary sources.

The analytical sequence links assets, data flows, threats, vulnerabilities, security controls, residual risk, and management decisions.

3.2 Scope of the Study

The study covers the following devices connected through internal IP networks, wireless networks, or IoT gateways.

- IP cameras, video recorders, and video-analytics equipment
- biometric and card-based access-control systems
- smart televisions, displays, and conferencing equipment
- network printers, copiers, and scanners
- building-management, ventilation, heating, and power equipment
- fire, smoke, water-leak, temperature, and motion sensors
- RFID, asset-tracking, and warehouse-monitoring equipment
- smart meters, uninterruptible power supplies, and power-monitoring systems
- dedicated IoT gateways and companion mobile applications
- wearable sensors that measure health status or location

Detailed architectures of weapon systems, combat-management networks, and specialized cryptographic equipment fall outside the scope of this open study.

3.3 Data Collection Methods

An operational organizational assessment should use the following evidence.

- Fixed-asset and technical inventories.
- DHCP, DNS, NAC, and network-switch MAC-address records.
- Firewall, NetFlow, proxy, DNS, and SIEM logs.
- Devices and protocols identified through passive network monitoring.
- Vendor technical documentation, software versions, and support periods.
- Procurement contracts, licenses, and cloud-service terms.
- Physical inspection of networks, server rooms, and devices.
- Interviews with responsible engineers, information-security personnel, and user units.

Active scanning and load testing can disrupt IoT and operational-technology devices, so the initial assessment should rely on passive discovery. Active vulnerability testing should be conducted only within a formally authorized scope, in a test environment, or during a scheduled maintenance window. NIST SP 800-82 Rev. 3 emphasizes that safety and reliability must take priority in OT assessments (Stouffer et al., 2023).

3.4 Proposed Risk Assessment Model

IoT device risk is assessed as the product of likelihood and impact. Each factor is scored on a scale from 1 to 5.

Likelihood is calculated as follows.

$$L = 0.30E + 0.30V + 0.25T + 0.15D$$

In this equation, E represents the device's network exposure and reachability from external or other security zones; V represents vulnerabilities, configuration weaknesses, and ease of exploitation; T represents the relevance and capability of threats likely to target the device; and D represents weaknesses in detection controls or the degree to which activity is not visible.

Impact is calculated as follows.

$$H = 0.30M + 0.20C + 0.20G + 0.15A + 0.15S$$

In this equation, M represents the effect on military mission performance; C represents the effect on information confidentiality; G represents the effect on the integrity of information, commands, and measurements; A represents the effect on system availability and continuity; and S represents the effect on the safety of personnel, equipment, and facilities.

Inherent risk is determined as follows.

$$R_0 = L \times H$$

Residual risk after implementing security controls is calculated as follows.

$$R_r = R_0(1 - K)$$

K represents the demonstrated effectiveness of security controls.

Table 1. Assessment of security control effectiveness

K value	Control status
0.0	No control
0.2	Documented but not fully implemented
0.4	Partially implemented with limited evidence
0.6	Fully implemented and tested
0.8	Automated, continuously measured, and independently validated

Table 2. Risk levels and decision guidance

Score	Risk level	Primary decision guidance
1.0-4.0	Low	May be operated under routine controls
4.1-9.0	Moderate	Additional controls and a time-bound mitigation plan
9.1-16.0	High	Management decision and priority action
16.1-25.0	Very high	Disconnect, isolate, or eliminate the risk

This model is intended to compare and prioritize IoT assets. Where a mandatory national methodology uses different thresholds or criteria, the official methodology takes precedence.

3.5 Worked Example

Consider an IP camera with outdated firmware that connects directly to the vendor's P2P cloud service. Its likelihood score is 4.30 and its impact score is 3.90, producing an inherent risk score of 16.77, which is very high. If the organization disables the P2P connection, moves the camera to a dedicated VLAN, applies unique credentials and certificates, updates the firmware, permits only authorized traffic to the recording server, and implements SIEM monitoring, the control-effectiveness value can reach $K=0.6$. The residual risk then falls to 6.71, which is moderate.

If the device is located in a classified or command zone, only the authorized risk owner may decide whether a moderate residual risk is acceptable.

4 Research Findings

4.1 IoT Asset Categories and Potential Mission Effects

Table 3. IoT asset categories and potential effects on mission performance

Device group	Data processed	Primary risk	Potential mission effect
IP cameras, NVRs, video analytics	Images, movement, location, time patterns	Loss of recordings, falsified images, disabled cameras	Disclosure of security routines and personnel movements
Biometric and access control	Face, fingerprints, cards, access logs	Loss of personal data or unauthorized privilege changes	Unauthorized entry into restricted areas
Smart displays and conferencing systems	Audio, video, displayed content, calendars	Covert recording or transfer of data to cloud services	Disclosure of meetings, plans, and command information
Printers, copiers, scanners	Documents, email, address books	Extraction of internal storage or printing of falsified documents	Loss of official or classified information
Building management, HVAC, UPS	Temperature, power, control commands	Service disruption or altered measurements	Disruption of server rooms and work areas
Fire, smoke, and water sensors	Environmental status and alarms	False alarms or suppression of genuine alarms	Physical harm to personnel, materiel, or facilities
RFID and warehouse monitoring	Assets, location, movement	Loss of logistics data or alteration of records	Disruption of supplies, reserves, and movements
Wearable sensors	Location, health status, movement	Tracking personnel or loss of personal data	Exposure of personnel locations and activity patterns
Consumer shadow IoT	Audio, video, device identifiers	Unregistered connections and dependence on vendor clouds	Creation of an uncontrolled communication channel

The analysis shows that a single device can create several overlapping risks. An IP camera, for example, may expose video data while also functioning as a continuously connected computer inside the internal network and providing a foothold for access to other systems. A smart display has multiple attack surfaces, including audio and video sensors, wireless interfaces, mobile-device control, and cloud registration.

4.2 Principal Categories of Threats and Vulnerabilities

The study groups military IoT risk into the following eight categories.

First device identity and access-control weaknesses

Factory-default passwords, reused passwords across devices of the same model, shared administrator accounts, and remote administration without multifactor authentication are major causes of unauthorized access. A joint CISA and NSA assessment identified default credentials and weak network segmentation among the most common security misconfigurations (CISA & NSA, 2023).

Second software and update risks

Devices remain vulnerable for extended periods when vendor support has ended, updates are no longer issued, or update files are not verified with digital signatures. The operational life of an IoT device commonly exceeds the vendor's period of security support.

Third unnecessary interfaces and services

The attack surface increases when unused interfaces and services remain enabled, including Telnet, FTP, legacy HTTP, UPnP, test APIs, vendor maintenance accounts, USB, Bluetooth, and Wi-Fi Direct.

Fourth flat network architecture

Placing IoT devices in the same VLAN as user workstations, servers, printers, and management systems increases the potential for lateral movement after a single device is compromised. MITRE ATT&CK identifies the use of valid accounts, remote services, network-service discovery, and adversary-in-the-middle techniques as methods used in real attacks (MITRE, 2026).

Fifth vendor cloud services and the supply chain

Some devices maintain persistent connections to vendor servers and transmit telemetry, images, and diagnostic data. An organization loses effective control when it cannot determine the country in which data are stored, the subcontractors that process them, or the conditions under which vendor engineers can obtain remote access.

Sixth insufficient logging and visibility

If a device cannot export system logs, lacks time synchronization, or does not report failed logins and configuration changes, the organization has less ability to detect attacks promptly and reconstruct events.

Seventh physical attack

Cameras, sensors, and door readers are often installed in public or weakly protected locations. Attackers may access reset buttons, memory cards, USB ports, or service ports to retrieve configurations, modify devices, or replace them with fraudulent equipment.

Eighth weak lifecycle governance

Devices with no identified owner, no inventory record, expired support, or incomplete data erasure at disposal create shadow IoT. Asset inventory is therefore a fundamental security control, not merely an administrative task.

4.3 Risks in Device Discovery and Communication Protocols

Automatic discovery protocols are not inherently vulnerable. Risk arises when they cross trust boundaries, remain enabled without an operational need, or are combined with unauthenticated management.

Table 4. IoT protocols and security controls

Protocol or service	Primary purpose	Risk condition	Control for a military network
UPnP/SSDP UDP 1900	Automatic discovery of devices and services	Exposure of device and service information; creation of unnecessary connections	Block by default on the organizational network; permit only within isolated zones
mDNS/DNS-SD UDP 5353	Discovery of local network names and services	Disclosure of printer, display, service, and model information	Do not forward multicast across zones; allow only approved gateways
WS-Discovery/ONVIF UDP 3702	Discovery of cameras and access-control devices	Disclosure of camera locations, models, and management addresses	Confine to the camera VLAN; permit access only from management servers

Protocol or service	Primary purpose	Risk condition	Control for a military network
RTSP typically 554	Video and audio streaming	Unencrypted streams and weak authentication	Do not expose externally; use a protected gateway and approved encryption
SNMP UDP 161/162	Device status and management	Disclosure of SNMPv1/v2c community strings and configuration	Use SNMPv3 authPriv and restrict access to management addresses
MQTT 1883/8883	Sensor publish/subscribe messaging	Anonymous connections and missing topic-level authorization	Use mTLS, topic-based ACLs, an internal broker, and prohibit anonymous access
CoAP 5683/5684	Communication for constrained devices	Multicast discovery and unencrypted commands	Use DTLS or OSCORE where supported; restrict to approved gateways and zones
Vendor P2P and cloud services	Remote viewing, management, and updates	Uncontrolled outbound traffic and third-party access	Deny by default; permit only after risk assessment, contractual controls, and allow-listing

mDNS uses UDP port 5353 to discover services on a local network (RFC 6762). CoAP is designed for resource-constrained devices and defines separate standard ports for unsecured and DTLS-secured communications (RFC 7252). MQTT is a lightweight publish/subscribe protocol widely used for IoT and machine-to-machine communications, but its practical security depends on TLS, broker configuration, and client and topic permissions (OASIS, 2019). ONVIF devices are discovered through WS-Discovery, so multicast traffic from a camera zone need not be forwarded into other trust zones (ONVIF, 2020).

4.4 Potential Attack Chain

A common attack chain involving an IoT device can be modeled as follows.

- An unregistered or weakly protected device connects to the internal network.
- The device is identified through automatic discovery protocols, logs, or network traffic.
- The attacker gains access through weak credentials, outdated firmware, or a vendor remote service.
- The attacker collects the device's network location, DNS and gateway settings, server addresses, and user information.
- The attacker moves laterally to other systems in the same VLAN.
- Video, audio, documents, access records, or logistics data are exfiltrated.
- The device is disrupted, false data are injected, or evidence of the attack is erased.

The most effective way to break this chain at the earliest stage is to prevent unauthorized devices from connecting, place approved devices in dedicated zones, and restrict network traffic under a default-deny policy.

5 Proposed Security Architecture for Military Organizations

5.1 Five Zone Network Model

Table 5. Zoning model for a military IoT network

Zone	Systems included	Connectivity principle
Zone I Classified and command environment	State and official secrets, command, and management systems	Prohibit consumer IoT; use only specially approved devices through a separate architecture
Zone II Mission security IoT	Surveillance cameras, access control, and security alarms	Dedicated VLAN or VRF; no direct Internet access; connect only to recording, management, time, and logging servers
Zone III Facility IoT and OT	HVAC, UPS, power, fire, and environmental systems	IT-OT security boundary; preserve local operation; allow remote maintenance only through authenticated, time-limited channels
Zone IV Administrative IoT	Printers, displays, and conferencing equipment	Separate from user devices; restrict outbound traffic through allow-lists
Zone V Guest, BYOD, and consumer devices	Personal phones, guest devices, and approved consumer IoT	Internet only; no route to internal organizational resources

Traffic between zones should be authorized precisely by business purpose, source, destination, port, protocol, and time condition. Any-to-any rules, uncontrolled inter-zone multicast, and arbitrary device access to internal servers other than approved DNS and NTP services should be prohibited.

5.2 Device Identity and Access Control

Each device should be registered with the following information.

- a unique asset identifier
- MAC address and certificate
- manufacturer, model, and serial number
- firmware version
- location, owning unit, and responsible officer
- classification of the data processed
- authorized network flows
- update and support expiration dates

Devices that support certificates should use IEEE 802.1X and EAP-TLS. Devices without certificate support should enter an isolated NAC registration zone and receive limited access based on device characteristics, switch port, location, and observed behavior. MAC Authentication Bypass is not reliable identity assurance on its own and must be combined with compensating controls.

5.3 Network Microsegmentation

Placing devices of the same type in a dedicated VLAN is necessary but insufficient. Where a camera has no operational need to communicate directly with another camera, or a printer with another printer, east-west traffic between devices should be blocked. Cameras should communicate only with the NVR, time server, DNS server, and log server; sensors should communicate only with the IoT broker or management gateway.

Users should not access device management interfaces directly from ordinary workstations. Administration should occur through a dedicated management server or jump host protected by multifactor authentication and comprehensive activity logging.

5.4 Data and Cryptographic Protection

Video, audio, biometric data, and access logs should be protected in transit and at rest through cryptographic mechanisms approved by the organization. Certificate validity, key rotation, revocation, and secure key deletion when a device is replaced should be centrally managed.

Legacy devices that do not support encryption should not process classified or high-value information. Where operational necessity requires their continued use, compensating controls should include a security gateway, physical isolation, or unidirectional data flow.

5.5 Patch and Vulnerability Management

Firmware updates should not be installed directly in the production environment. They should first be tested on an identical device model for functionality, compatibility, configuration retention, and rollback capability and then deployed in stages. The vendor's digital signature and the file hash should be verified before installation.

Vulnerabilities should be prioritized by correlating the CISA Known Exploited Vulnerabilities catalog, vendor advisories, CVE records, and internal assessments. Priority should not depend on CVSS alone; it should also account for device location, external connectivity, data classification, and mission effect.

5.6 Logging and Continuous Monitoring

To the extent supported, the following IoT events should be centralized in the SIEM system.

- successful and failed logins
- changes to administrator privileges or passwords
- firmware and configuration changes
- device reboots and factory resets
- attempts to connect to new network addresses or domains
- camera obstruction and abnormal sensor states
- use of USB, memory cards, or other physical interfaces
- loss of time synchronization
- interruption of log forwarding

A baseline of normal behavior should be established for each model, location, and operating schedule. Alerts should be generated for changes such as connections to previously unused external domains, sudden increases in DNS queries, unusual traffic volumes, or management connections outside working hours.

6 Security Measures Aligned with NIST CSF 2.0

NIST CSF 2.0 organizes cybersecurity risk management into six functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024).

Table 6. NIST CSF 2.0 functions and military IoT security measures

Function	Measures for a military IoT environment
Govern	IoT policy, designated risk owners, a device-approval board, supplier criteria, budgeting, accountability, and internal audit
Identify	Passive asset discovery, inventory, data-flow mapping, data classification, support periods, and mission dependencies
Protect	Segmentation, NAC, unique credentials, certificates, encryption, secure boot, updates, least privilege, and physical security
Detect	SIEM, network-behavior monitoring, detection of unauthorized devices, configuration changes, traffic anomalies, and interrupted logging
Respond	NAC quarantine, certificate revocation, traffic blocking, evidence preservation, and notification of the competent center
Recover	Approved firmware, golden configurations, backups, re-enrollment, operational validation, and policy updates based on lessons learned

7 Procurement and Supply Chain Requirements

IoT security begins during procurement. Technical specifications and contracts should include the following mandatory requirements.

- Each device must be free of universal factory-default passwords and must generate unique credentials at first startup.
- The device must support secure boot, digitally signed firmware, and integrity verification.
- The vendor must maintain a formal channel for receiving and disclosing vulnerability information.
- The contract must specify security-update timeframes, the end-of-support date, and service levels for remediating critical vulnerabilities.
- The vendor should be able to provide a software bill of materials, or SBOM.
- The device must retain its essential local functionality without the vendor's cloud service.
- Unnecessary protocols, services, and wireless interfaces must be capable of being disabled.
- The device must export security logs through Syslog or another standard format.
- The device must interoperate with the organization's DNS, NTP, PKI, and certificate infrastructure.
- The device must use TLS and cryptographic mechanisms approved by the organization.
- Data, certificates, and keys must be securely erased when the device is retired.
- Vendor remote access must be disabled by default.
- The vendor must disclose the content of telemetry, the country of storage, and any third-party processing.
- The organization must retain access to device functions and data if the vendor changes ownership, becomes insolvent, or discontinues the service.
- Acceptance testing must verify ports, services, firmware, updates, logging, cloud connections, and factory-reset behavior.

A certification mark for a standard such as ONVIF confirms interoperability but does not independently establish the overall cybersecurity of a product. Standards compliance should therefore be assessed together with vulnerability history, the vendor's update policy, and the device's actual configuration.

8 Cyber Incident Response

An incident involving an IoT device should be handled in the following sequence.

8.1 Detection and Initial Classification

The organization should determine whether the incident affected only the device's operation or also affected video, biometric data, classified information, physical safety, or mission performance. It should record the device model, serial number, IP and MAC addresses, location, firmware, network zone, and most recent changes.

8.2 Containment

The device should be moved to a quarantine zone through NAC, the network switch, or the firewall. Surveillance, access-control, and fire-alarm systems should not be shut down automatically because doing so may create physical safety risks. Containment should be coordinated with operational and security units.

8.3 Preservation of Evidence

Before restoring factory settings or formatting the device, investigators should preserve device logs, network traffic, configuration, firmware version and hash, contacted domains and IP addresses, administrator activity, and time-synchronization status. Evidence associated with state or official secrets must be protected under the applicable special procedures.

8.4 Scoping

All devices that use the same vendor, model, or firmware should be examined. Investigators should determine whether the compromised device's password, certificate, or vendor account has been reused on other devices.

8.5 Eradication and Recovery

The organization should install approved firmware, restore the golden configuration, rotate all passwords and certificates, disable unnecessary services, and review network rules. After recovery, normal traffic, logging, and mission functionality should be validated.

8.6 Reporting and Lessons Learned

Where required by the Law on Cybersecurity and internal procedures, the organization should notify the relevant cyberattack and incident response center and other competent authorities. It should document the cause of the incident, control failures, response time, and measures adopted to prevent recurrence.

9 Implementation Phases

9.1 Immediate Phase 0 to 90 Days

- Issue a management directive prohibiting unauthorized IoT devices on classified and command networks.
- Create a consolidated IoT asset inventory through passive network discovery and physical inspection.
- Replace factory-default and reused passwords.
- Disable unnecessary Telnet, FTP, UPnP, P2P, and vendor remote-access services.
- Isolate unsupported, unregistered, and ownerless devices.
- Block direct Internet access from IoT devices and apply allow-lists.
- Conduct accelerated assessments of high-risk camera, conferencing, and biometric systems.

9.2 Foundational Capability Phase 3 to 12 Months

- Implement five-zone segmentation.
- Deploy NAC, a centralized asset inventory, SIEM, and passive IoT and OT monitoring.
- Adopt standard cybersecurity requirements for procurement.
- Assign a device owner, technical custodian, and risk owner.
- Develop and exercise a dedicated IoT incident-response plan.
- Establish a test environment for firmware updates.
- Make vendor remote access time-limited and subject to multifactor authentication.

9.3 Advanced Phase 12 to 24 Months

- Fully deploy device certificates and the organizational PKI.
- Implement policy-based microsegmentation and automated quarantine.
- Institutionalize SBOM and supply-chain risk requirements in contracts.
- Deploy behavioral baselines and anomaly analytics for IoT devices.
- Conduct authorized red-team and blue-team exercises in a laboratory environment.
- Assess residual risk quarterly and report it to management.
- Progressively deepen zero-trust implementation at the device, network, data, and user levels.

10 Performance Indicators

Implementation should be evaluated through measurable outcomes rather than only by the number of security products installed.

Table 7. IoT cybersecurity performance indicators

Indicator	Target direction
Percentage of IoT devices included in the inventory	100 percent
Percentage of devices with identified owner, location, and firmware	100 percent
Percentage of devices with unique credentials	Continuous increase
Percentage of devices located in segmented IoT zones	100 percent
Number of devices permitted direct Internet access	Minimum operationally necessary level
Percentage of devices forwarding logs centrally	Continuous increase
Average time to install critical updates	Continuous reduction

Indicator	Target direction
Number of unsupported devices	Reduction toward zero
Mean time to detect an unauthorized device	Minutes
Time required to isolate a suspicious device	Continuous reduction
Number of high and very high residual risks	Reduction in every reporting period
Coverage of IoT incident exercises and training	Full annual implementation

11 Discussion

The findings indicate that the central IoT cybersecurity problem in a military organization is not a single device vulnerability. It is the context in which the device operates: the network to which it is connected, the privileges it holds, the data it processes, and the vendor services on which it depends. Even a well-secured camera remains high risk if it shares a flat network with user workstations, has uncontrolled Internet access, and permits permanent vendor remote administration.

First, a complete asset inventory is the foundation of security. An organization that does not know which devices are present on its network cannot manage updates, segmentation, monitoring, or incident response effectively.

Second, network isolation is among the highest-impact measures available in the short term. Even when a legacy device cannot be replaced, a dedicated security zone, restrictive firewall rules, and blocked Internet access can reduce risk substantially.

Third, zero trust should be understood as a governance principle rather than a product. Many IoT devices do not support certificates or endpoint agents, so their limitations must be offset through network controls, gateways, proxies, microsegmentation, and physical protection.

Fourth, confidentiality and physical safety must be assessed together. Loss of camera footage is an information incident, whereas alteration of an access-control command or suppression of a fire alarm may endanger personnel and facilities. The CIA triad alone is therefore insufficient; mission and safety effects must also be assessed.

Fifth, procurement is a cybersecurity decision. After delivery, it is difficult to change the vendor's update policy, cloud dependency, logging capability, or support period. Security requirements should therefore be embedded in technical specifications, contracts, and acceptance testing before purchase.

11.1 Limitations of the Study

This article is a model-based study grounded in open sources, standards, and legal instruments; it does not contain empirical measurements from operational Mongolian military networks. The proposed weights, thresholds, and zoning model must therefore be validated through testing and adjusted to the organization's mission, network architecture, secrecy classification, and device types.

Future research could conduct 30 to 60 days of passive monitoring in an unclassified test environment at a selected military unit or organization. Such research could compare the actual number of devices, protocols, outbound flows, update status, inherent risk, and residual risk before and after controls are implemented.

12 Conclusions

IoT devices used in the internal networks of military units and organizations increase operational efficiency, security monitoring, and automation while also changing the boundaries of conventional cyber defense. Cameras, biometric equipment, smart displays, printers, and environmental sensors are not simple data-collection tools. They are complete computing devices with operating systems, network interfaces, remote services, and vendor dependencies.

The study identifies the most common causes of IoT risk as incomplete asset inventories; factory-default and reused passwords; outdated or unsupported firmware; flat networks and excessive access privileges; uncontrolled vendor P2P and cloud services; inadequate logging and monitoring; and weak lifecycle governance.

A baseline policy for military organizations should rest on three principles: unregistered devices do not connect to the network; unapproved devices do not operate on classified or mission networks; and every device communicates only with the resources required for its assigned function.

The principal security measures are to exclude consumer IoT from classified and command networks; place approved devices in dedicated zones; implement NAC, certificates, microsegmentation, allow-listed traffic, centralized logging, and secure updates; and govern vendor dependency through contracts and technical requirements.

These measures can transform IoT devices from invisible weak points into inventoried and monitored assets with measurable and governable risk. In addition to protecting confidentiality, integrity, and availability, this approach supports mission continuity, physical safety, and cyber resilience in military units and organizations.

REFERENCES

1. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the mirai botnet. *26th USENIX Security Symposium, 1093-1110*. <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf>.
2. Cybersecurity and Infrastructure Security Agency, & National Security Agency. (2023). NSA and CISA red and blue teams share top ten cybersecurity misconfigurations. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>
3. Department of Defense Chief Information Officer. (2022). Department of Defense zero trust strategy. <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
4. European Telecommunications Standards Institute. (2024). ETSI EN 303 645 V3.1.3: Cyber security for consumer Internet of Things: Baseline requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
5. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259A>
6. Fagan, M., Marron, J., Brady, K. G., Jr., Cuthill, B. B., Megas, K. N., & Herold, R. (2021). IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (NIST SP 800-213). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-213>
7. Internet Engineering Task Force. (2013). Multicast DNS (RFC 6762). RFC Editor. <https://doi.org/10.17487/RFC6762>
8. Internet Engineering Task Force. (2014). The constrained application protocol CoAP (RFC 7252). RFC Editor. <https://doi.org/10.17487/RFC7252>
9. MITRE. (2026). MITRE ATT&CK knowledge base. <https://attack.mitre.org/>
10. State Great Khural of Mongolia. (2016). Law on State and Official Secrets [In Mongolian]. <https://legalinfo.mn/mn/detail/12408>
11. State Great Khural of Mongolia. (2021a). Law on Cybersecurity [In Mongolian]. <https://legalinfo.mn/mn/detail?lawId=16390365491061>
12. State Great Khural of Mongolia. (2021b). Law on the Protection of Personal Information [In Mongolian]. <https://legalinfo.mn/mn/detail?lawId=16390288615991>
13. Government of Mongolia. (2022). National Cybersecurity Strategy, Government Resolution No. 493 [In Mongolian]. <https://legalinfo.mn/mn/detail?lawId=16532522791411>
14. Government of Mongolia. (2023). General Procedure for Ensuring Cybersecurity, Government Resolution No. 224 [In Mongolian]. <https://legalinfo.mn/mn/detail?lawId=16759862495731>
15. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. <https://doi.org/10.6028/NIST.CSWP.29>
16. OASIS Open. (2019). MQTT version 5.0. <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>
17. ONVIF. (2020). ONVIF core specification. <https://www.onvif.org/specs/core/ONVIF-Core-Specification-v2006.pdf>
18. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
19. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to operational technology security (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
20. Minister of Digital Development, Innovation and Communications, & Director General of the General Intelligence Agency. (2024). Procedure and methodology for cybersecurity risk assessment, Joint Orders Nos. A/30 and A/148 [In Mongolian]. <https://legalinfo.mn/mn/detail?lawId=17141973551921>