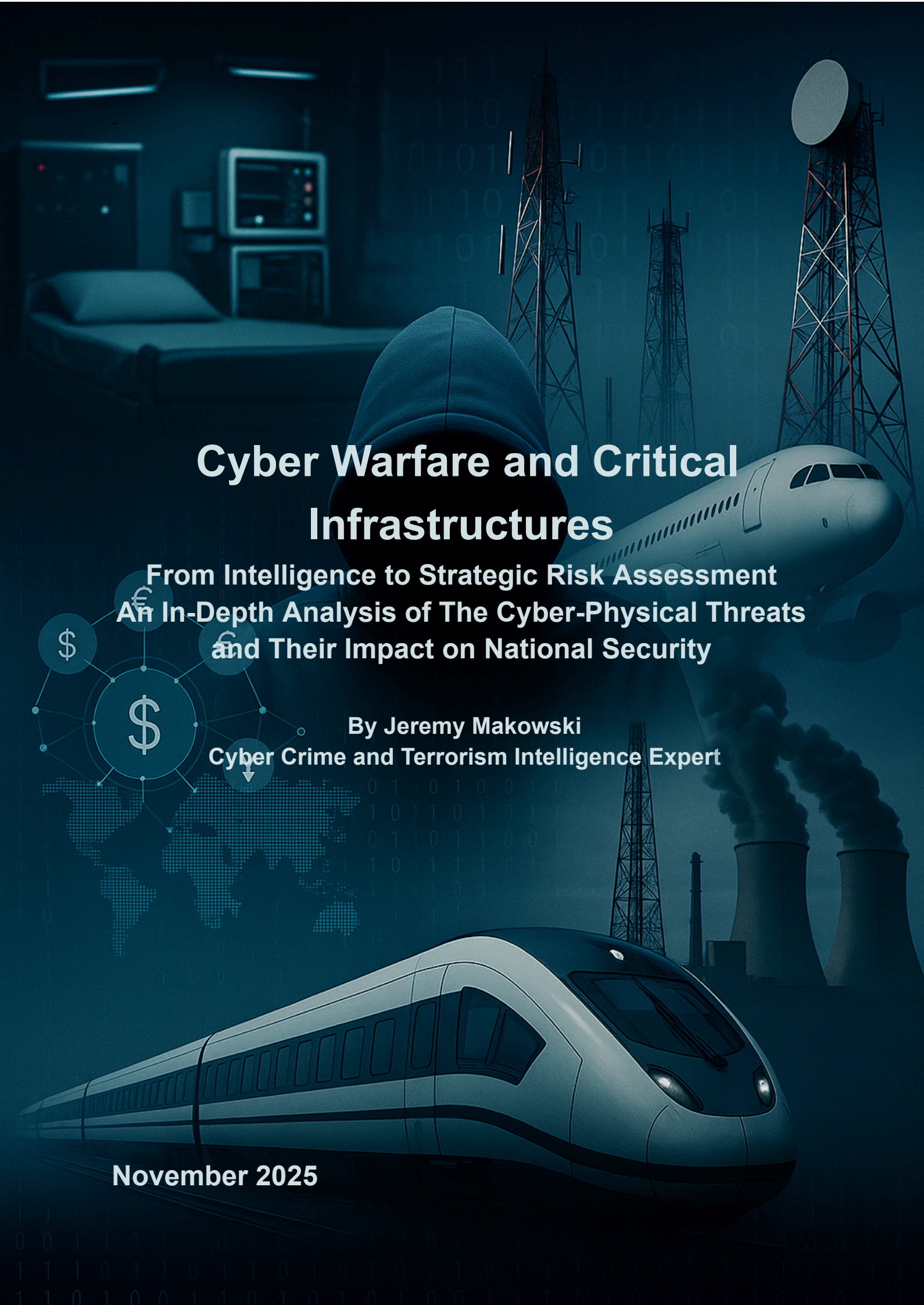


Cyber Warfare and Critical Infrastructures

From Intelligence to Strategic Risk Assessment
An In-Depth Analysis of The Cyber-Physical Threats and Their Impact on National Security

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

November 2025

Disclaimer

This document is made freely available for informational purposes and to support a deeper understanding of the evolving dynamics of power in the cyber age.

Reproduction of any part of this document whether in whole or in part must include proper attribution to the author and a clear reference to the original source.

Any commercial use of the content, in full or in part, is strictly prohibited without the express written consent of the author.

Table of Contents

Disclaimer **2**
Executive Summary **5**
1. Introduction & Methodology **6**
1.1 Defining Cyber-Physical Warfare **6**
1.2 Assessment Methodology **6**
1.3 Critical Infrastructure in National Strategy **7**
1.3.1 Cascading Effects and Strategic Vulnerabilities 7
1.3.2 Single-Technology Dependence and Lack of Redundancy 7
1.3.3 Elements Defining the Infrastructure–Security Nexus 8
1.3.4 National Resilience as a Cross-Sector Capability 9
1.4 Producing Decision-Grade Intelligence 9
2. The Cyber-Physical Threat Environment **9**
2.1 Hybrid Warfare: The Cyber-Physical Nexus **9**
2.2 Cyber Coercion and Strategic Leverage **10**
2.3 Threat Actor Profiles **11**
2.3.1 Military and Intelligence Services 11
2.3.2 State-Sponsored Proxies and Contractor Ecosystems 12
2.3.3 Cybercriminal Organizations 12
2.3.4 Hacktivists and Ideologically Motivated Groups 13
2.4 Main nations engaged in cyberattacks on critical infrastructures. **14**
2.4.1 Russia **14**
2.4.1.1 Russia’s Cyber Power: Key Institutions and Structures 15
2.4.1.2 Operational Objectives and Tactics 17
2.4.1.3 Target Profile and Geographical Focus 18
2.4.2 China **19**
2.4.2.1 China's Cyber Power: Key Institutions and Structure 19
2.4.2.2 Operational Objectives and Tactics 22
2.4.2.3 Target Profile and Geographical Focus 23
2.4.3 Iran **23**
2.4.3.1 Iran’s Cyber Power: Key Institutions and Structures 24
2.4.3.2 Operational Objectives and Tactics 26
2.4.3.3 Target Profile and Geographical Focus 27
2.4.4 North Korea **28**
2.4.4.1 North Korea’s Cyber Power: Key Institutions and Structures 28
2.4.4.2 Operational Objectives and Tactics 30
2.4.4.3 Target Profile and Geographical Focus 31
2.5 Attack Vectors and Campaign Patterns **32**
2.6 Global Trends and Strategic Implications **35**

3. Sectoral Cyber-Physical Risk Assessment **36**
3.1 Energy **36**
3.1.1 Power Generation Facilities 36
3.2 Healthcare **40**
3.2.1 Public Health Infrastructure 44
3.3 Financial **48**
3.3.1 Banking Infrastructure 48
3.3.3 Payment & Settlement Networks 55
3.4 Transportation **58**
3.4.1 Air Transport: Airports and Aircraft Systems 58
3.4.2 Railways **62**
3.4.2.1 Rail and Subway Networks 62
3.4.3 Roads **65**
3.4.3.1 Road Traffic Systems 65
3.4.4 Maritime Transport **69**
3.4.4.1 Seaports & Terminals 69
3.4.4.2 Ships and Maritime Navigation 72
3.5 Telecommunications **74**
3.5.1 ISPs and Telecom Operators 74
3.5.2 Satellite Communications 78
3.5.3 Data Centers and Cloud Infrastructure 81
3.6 Government and Public Administration **83**
3.6.1 Government IT & Cyber Infrastructure 83
3.6.2 Public Services and Regulatory Oversight 87
3.6.3 Elections and Civic Systems 89
3.7 Defense and Military **92**
3.7.1 Military Infrastructure 92
3.7.2 Intelligence and Security Agencies 95
4. Conclusion **98**
5. About the Author **99**
6. References **100**

Executive Summary

Critical infrastructures, such as energy, transportation, finance, healthcare, communications, government, and defense, form the backbone of national stability, economic continuity, and military readiness. Their increasing digital interdependence has created a strategic environment where disruption in one sector can rapidly cascade across many others, turning technical failures into national crises. As states and non-state actors refine the ability to manipulate these systems for coercive, political, or military advantage, cyber-physical warfare has emerged as a defining feature of modern conflict.

This assessment provides senior leaders with an integrated picture of that evolving threat landscape. It examines how adversaries combine cyber intrusion, pre-positioning, supply-chain compromise, and information operations with the potential for physical disruption, and it maps the diverse ecosystem of actors, military services, intelligence agencies, proxy groups, criminal networks, and ideologically motivated movements that now operate across the cyber-physical domain. Detailed national profiles of Russia, China, Iran, and North Korea illustrate how each organizes its cyber power, selects targets, and conducts operations against critical infrastructure worldwide.

Beyond actor intent, the report examines the structural vulnerabilities that render national infrastructures susceptible to cascading effects, including legacy technologies and single-technology dependencies, opaque supply chains, and limited cross-sector coordination. A sector-by-sector risk assessment highlights where exposure is most acute and how adversaries exploit operational blind spots in energy grids, hospitals, financial markets, transport systems, telecom networks, public administration, and defense capabilities. Together, these insights offer decision-makers a strategic framework for understanding how cyber-physical threats translate into national-level risk and for prioritizing resilience, redundancy, and intelligence-driven defense. The report emphasizes that nations capable of securing and integrating their critical infrastructures will be significantly better positioned to deter coercion, manage escalation, and maintain operational continuity in an increasingly contested world.

1. Introduction & Methodology

1.1 Defining Cyber-Physical Warfare

Cyber-physical warfare refers to the deliberate use of digital means to cause, enable, or amplify physical outcomes. These may be destructive (e.g., turning off a turbine), disruptive (blocking rail switches), or coercive (triggering a public health scare by corrupting sensor data). What distinguishes cyber-physical warfare from ordinary cyber intrusion is not merely the target but the intent to alter real-world conditions, behaviors, or safety. Three conceptual categories help anchor analysis. First, kinetic-trigger cyber operations utilize cyber access to support or conceal physical actions. For example, turning off security camera feeds to facilitate a covert ground operation. Second, direct-effect operations use digital manipulation to produce immediate physical results, such as opening circuit breakers to cause localized power outages. Third, enabling and cognitive operations seek to shape perception or operational tempo. An adversary might manipulate chemical plant telemetry so that local operators believe a reaction is unstable, prompting an emergency shutdown that achieves strategic disruption without overt sabotage. These examples demonstrate the diversity of tools that fall under the cyber-physical umbrella and highlight the analytical challenge: effects may emerge from subtle chains of cause and perception rather than apparent sabotage.

1.2 Assessment Methodology

The assessment approach combines systems mapping, actor analysis, scenario modeling, and indicators-based monitoring. Systems mapping begins with identifying critical assets, their dependencies, and the failure modes associated with them. For instance, a regional water utility may depend not only on pumps and filtration systems but also on a telecommunications backbone that, if disrupted, prevents remote command and oversight. Recognizing these interdependencies helps analysts avoid siloed assessments. Actor-capability mapping analyzes adversaries' historical behavior, technical maturity, and political objectives. A state actor with a track record of coercive energy disruptions in neighboring countries will be evaluated differently from a criminal group whose primary motive is financial gain. Scenario modeling then tests plausible attack paths. For example, analysts might examine how a compromise in a railway scheduling system could escalate from minor delays to a broader transportation standstill if timed with labor unrest or severe weather. This method makes latent risks more concrete, allowing planners to identify interventions that break the causal chain. Finally, indicators-and-warnings frameworks provide a structured approach to monitoring. Examples include unusual polling of OT devices, unexplained shifts in access privileges, or simultaneous probing of multiple infrastructure operators. These help decision-makers distinguish between background noise and signals of strategic intent.

1.3 Critical Infrastructure in National Strategy

Critical infrastructure is inseparable from national security because it constitutes the operational substrate on which state stability, economic continuity, and public safety depend. These sectors, energy, transportation, water, telecommunications, finance, and healthcare, do not function as isolated assets but as a tightly coupled architecture. Their technical, operational, and cyber dependencies create what national security doctrine recognizes as a system-of-systems environment, where a disruption in one domain can generate cross-sector effects that compromise national capacity to deter, respond to, or recover from threats.

1.3.1 Cascading Effects and Strategic Vulnerabilities

The security implications of interdependence become clear in cascading-failure scenarios. A targeted intrusion on an electric grid control center may cause the shutdown of substations supplying power to cellular towers. This degradation of mobile networks can then impede emergency services' ability to coordinate ambulance routing or disseminate evacuation instructions. The national-security significance arises not from the isolated loss of electricity or communications, but from the compound effect: diminished situational awareness, delayed state response, and reduced public trust in governmental protective functions.

Other sectors illustrate how tactical disruptions can create strategic vulnerabilities. A railway signaling failure does not merely halt logistics operations; it can obstruct the movement of military equipment to ports of embarkation. A compromised financial clearinghouse can affect the liquidity of defense contractors, slowing procurement cycles. Natural gas pipeline networks exhibit similar complexity: even if compressor stations are well-protected, an adversary exploiting unsecured telemetry units can manipulate flow rates, jeopardizing heating, electricity generation, and broader societal resilience. These examples illustrate how technical disruptions can escalate into national-scale security concerns.

1.3.2 Single-Technology Dependence and Lack of Redundancy

A core, and increasingly visible, national-security concern is the dependence of critical infrastructure on a narrow set of digital platforms and service providers, often without meaningful redundancy. This concentration risk is not limited to intentional adversarial actions; it also includes accidental failures, software errors, and operational misconfigurations that can lead to national-level disruption, simply because a single point of failure is embedded across multiple sectors. Recent incidents illustrate the scale of this systemic fragility. A CrowdStrike software update error propagated globally within minutes, grounding airlines, disrupting airport operations, and affecting hospitals, police systems, and government networks.

The outage was not the result of a targeted attack but of a single-vendor fault amplified by the ubiquity of the affected endpoint security product. Similarly, Microsoft cloud service disruptions have periodically halted email, identity management, and collaboration tools, directly impacting government agencies and critical industries that rely on cloud authentication to operate even their internal systems. The impact of these events demonstrates how technology providers, once considered peripheral suppliers, now function as de facto national-infrastructure operators.

The danger becomes more pronounced when critical infrastructure sectors converge around the same vendor ecosystem. European airports in Brussels, London Heathrow, and Berlin experienced operational paralysis when a cyberattack affected a single check-in software provider. Although the attack targeted one commercial platform, its effects spread instantly across national borders and airline networks. In such contexts, national-security exposure arises less from the sophistication of adversaries and more from structural homogeneity: the same codebases, cloud tenants, authentication systems, and operational workflows embedded everywhere. When a sector relies on a single software provider for essential functions such as identity verification, baggage routing, or industrial control, it creates a monoculture that magnifies both accidental and intentional disruptions.

The strategic risk lies in the alignment between commercial optimization and national security. Market incentives favor consolidation, efficiency, and standardized platforms, while national-security requirements demand distributed architectures, diversified supply chains, and controllable fallback modes. When critical infrastructure operators depend on a monoculture of digital services without independent failover paths, resilience becomes contingent on the operational stability of private entities whose internal failures can ripple into national crises. This structural concentration transforms software publishers and cloud platforms into single points of national failure, with consequences ranging from travel disruption and stalled emergency response to large-scale economic paralysis.

1.3.3 Elements Defining the Infrastructure–Security Nexus

Several key elements further solidify the deep connection between infrastructure and national security. Critical nodes, such as major substations, undersea cables, water treatment facilities, and air-traffic control centers, serve as strategic chokepoints whose continuity is fundamental to state functionality. The adversary landscape includes actors capable of conducting reconnaissance, infiltrating industrial control systems, or exploiting software supply chains to create effects traditionally associated with kinetic operations. Moreover, private ownership of most critical infrastructure produces a structural asymmetry: commercial entities manage operational and financial risk, while the state carries the strategic burden of national-level failure.

1.3.4 National Resilience as a Cross-Sector Capability

The ability to maintain national resilience, therefore, depends on more than asset hardening. It encompasses sustained cross-sector information exchange, interoperable response frameworks, and the capability to operate under degraded conditions. Manual fallback procedures such as local control of water treatment valves or analog air-traffic sequencing illustrate the continuing value of physical redundancy. Coordinated public communication strategies also mitigate adversaries' ability to amplify disruptions with disinformation. In this framing, critical infrastructure is not merely a collection of assets but a national-security ecosystem whose integrity determines a nation's capacity to withstand shocks, absorb failures, and project stability under contested conditions.

1.4 Producing Decision-Grade Intelligence

Decision-grade intelligence is actionable, concise, and tightly linked to the decisions it informs. Instead of long technical descriptions, it highlights what happened, what it means, who is most likely responsible, and what options are available. For instance, if analysts detect coordinated scanning of industrial control systems across multiple ports in a single maritime region, a decision-grade brief would not simply list the IPs and timestamps. It would explain whether this represents routine background noise, a pre-operational survey by a known actor, or a signal of potential coercive leverage tied to ongoing diplomatic tensions. It would propose immediate protective steps, such as increasing isolation of port crane controllers or restricting remote vendor access during crisis periods. This framing allows leadership to act quickly without wading through technical detail and reduces the risk of overreaction or paralysis due to uncertainty.

2. The Cyber-Physical Threat Environment

2.1 Hybrid Warfare: The Cyber-Physical Nexus

Hybrid warfare blends conventional, irregular, informational, and cyber tools into coordinated campaigns. The cyber-physical domain adds a layer of subtlety and strategic ambiguity. For example, an adversary might not need to shut down a power plant; a brief but well-timed outage during a national referendum could be enough to sow doubt about the state's competence or legitimacy. Such a disruption, although limited, amplifies political narratives and forces leadership into defensive communication. Operationally, hybrid campaigns often combine multiple instruments for a cumulative effect.

One illustrative scenario involves an adversary conducting low-level OT intrusions at energy distribution centers while simultaneously launching an online narrative that claims the outages reveal corruption or mismanagement. Even if the physical disruption is modest, the psychological effect may be substantial, especially if political or economic tensions already heighten public awareness. Countering hybrid operations requires integrated planning. Technical teams must coordinate with public affairs, legal authorities, and intelligence services to ensure seamless integration and alignment. Exercises that simulate concurrent physical disruptions and information attacks help identify security gaps. For example, a drill that combines a localized water treatment anomaly with a fabricated online rumor about contamination can test whether authorities can maintain public trust while diagnosing the technical issue.

2.2 Cyber Coercion and Strategic Leverage

Cyber coercion leverages the threat or demonstration of disruptive capacity to shape another state's behavior. It rarely aims for catastrophic damage. Instead, the goal is to impose manageable but politically salient pressure. An illustrative example is an adversary intermittently disrupting logistics management systems at major freight hubs during sensitive trade negotiations. The disruptions need not halt operations completely; creating delays or forcing manual workarounds may be enough to remind political leaders of the attacker’s access and willingness to escalate. This “dial-a-disruption” approach enables calibrated coercion while maintaining deniability.

Another example is the manipulation of environmental sensors or floodgate controls during the monsoon season. Even if the attacker does not trigger flooding, demonstrating the ability to interfere with these systems can compel local authorities to divert resources, adopt a more conciliatory posture in negotiations, or hesitate in deploying law enforcement. Defensive posture must therefore integrate deterrence, denial, and political resilience. Deterrence can involve clear policy statements that specific categories of cyber-physical interference will be treated as strategic aggression. Denial entails building redundancies, for example, ensuring that transport hubs can revert to manual scheduling within minutes if the primary system is compromised. Political resilience involves preparing leadership and the public to accurately interpret disruptions, thereby reducing the adversary’s psychological leverage.

2.3 Threat Actor Profiles

Threat actors targeting critical infrastructures constitute a dynamic, overlapping, and increasingly interdependent ecosystem. Although their campaigns may share tools, infrastructure, or access vectors, their motivations, risk thresholds, and strategic logic differ sharply. Understanding these distinctions is critical: contemporary intrusions into critical infrastructure often blend espionage, monetization, and strategic coercion. In many cases, states leverage criminal syndicates, proxy operators, or commercial contractors, creating hybrid campaigns designed to maintain deniability while expanding operational reach. The following typology integrates strategic intent, operational behavior, and observed targeting patterns across major actor classes, followed by deeper country-specific analyses in subsequent sections.

2.3.1 Military and Intelligence Services

- **Strategic Intent:** State actors represent the most capable and strategically consequential threat class. Their operations align directly with national objectives: reshaping geopolitical competition, establishing coercive leverage, influencing adversary decision-making, and preparing options for crisis or armed conflict. They pursue long-term strategic positioning rather than immediate disruption.

- **Operational Logic: State operations typically involve sustained, covert campaigns that emphasize** deep reconnaissance, access cultivation, and sophisticated intrusion across both IT and OT environments. Their activities are often synchronized with diplomatic messaging, economic pressure, military force posture adjustments, and information operations. Effects are calibrated, timed, reversible, and plausibly deniable, allowing for the management of escalation while preserving optionality.

- **Infrastructure Targeting Tendencies:** States target high-leverage systems whose compromise offers strategic influence or crisis leverage:
    - Power generation and transmission networks
      Telecommunications backbones and undersea cables
      Transportation and logistics hubs
    - Satellite communications and PNT systems
    - Financial clearing and settlement infrastructure
    - Government digital service platforms

2.3.2 State-Sponsored Proxies and Contractor Ecosystems

- **Strategic Intent:** State-linked proxies provide scalability, plausible deniability, and operational flexibility. Governments leverage these entities to distribute workload, outsource specialized components, or pursue activities unsuitable for official intelligence or military units.
- **Operational Logic:** These operators function within hybrid command structures, which are a combination of government-directed and commercially motivated elements. They often reuse widely available tools, exploit criminal marketplaces, and maintain modular operations:
    - Reconnaissance stages can later support espionage or sabotage.
    - Access initially gained for intelligence purposes may be repurposed for disruption.
    - Campaigns evolve in response to geopolitical events.

- **Infrastructure Targeting Tendencies**
    - Third-party vendors and managed service providers
    - Regional utilities and municipal service networks
    - Politically symbolic institutions
    - Supply-chain ecosystems and cloud service environments

2.3.3 Cybercriminal Organizations

- **Strategic Intent:** Criminal groups pursue profit above all else. Their operations monetize access through ransomware, extortion, data theft, or the sale of footholds into critical infrastructure.
- **Operational Logic:** Criminal ecosystems are decentralized but highly efficient, typically composed of:
    - Initial access brokers
    - Ransomware developers
    - Affiliate operators
    - Money launderers

Their campaigns are opportunistic, fast-moving, and designed to maximize revenue. While not political, they routinely trigger strategic-level effects, disrupting hospitals, utilities, transportation hubs, and manufacturing plants. Many operate from jurisdictions that tacitly tolerate or shield their activities.

- **Infrastructure Targeting Tendencies:** Sectors with low outage tolerance and high incident-resolution pressure are prime targets:
    - Healthcare systems
    - Energy distributors and pipeline operations
    - Water and wastewater utilities
    - Transportation scheduling and routing platforms

    - Municipal governments and public services

2.3.4 Hacktivists and Ideologically Motivated Groups

- **Strategic Intent:** Hacktivist actors seek visibility, ideological expression, political messaging, and symbolic disruption, not strategic advantage.
- **Operational Logic:** Their campaigns prioritize public impact. Tooling ranges from basic DDoS and web defacement to opportunistic exploitation of vulnerable systems. Many groups publicly claim attacks to amplify message reach. During geopolitical crises, hacktivist collectives may align voluntarily or implicitly with state narratives, contributing to attribution ambiguity and information disorder. Although generally less capable of causing deep OT compromise, they can still inflict reputational and societal damage.
- **Infrastructure Targeting Tendencies:** Typical targets include:
    - Government portals and emergency services
    - Media outlets and political institutions
    - Public-facing payment or service portals
    - Municipal platforms with high public visibility

Insiders and Supply-Chain Enablers

- **Strategic Intent:** Insider threats originate from a spectrum of motivations, including personal grievance, financial incentive, coercion, ideological alignment, or unintentional human error. Supply-chain enablers, such as compromised vendors, contractors, or trusted service providers, extend the insider threat across organizational boundaries.
- **Operational Logic:** Insiders possess privileged access, operational knowledge, and the ability to bypass security controls. Their actions may be deliberate or inadvertent:
    - Malicious insiders exfiltrate data, turn off safeguards, or facilitate external access.
    - Negligent insiders expose credentials, misconfigure systems, or fall prey to social engineering.
    - Supply-chain enablers unintentionally propagate compromise through software updates, managed services, or hardware dependencies.

These actors often serve as force multipliers for state or criminal groups, enabling stealthy lateral movement or rapid operational escalation.

- **Infrastructure Targeting Tendencies:** High-trust roles and interconnected vendor ecosystems create risk across:
    - Energy and utility operators
    - Industrial control system integrators
    - Managed service and cloud providers
    - Healthcare and emergency response networks
    - Transportation and logistics management systems

2.4 Main nations engaged in cyberattacks on critical infrastructures.

Critical infrastructure (energy, water, transportation, telecommunications, healthcare, finance) is attractive to state cyber actors because it provides leverage short of and sometimes instead of kinetic conflict: espionage for planning and policy, disruption to coerce or punish, revenue/finance theft to fund state goals, and pre-positioning to enable contingency sabotage during crises. States differ in their doctrine, risk tolerance, and tooling: some prioritize disruption and coercion, while others focus on long-term espionage and breaching access to resilience. Below, I analyze six state actor groups/countries, highlighting each country's objectives, preferred techniques, operational patterns, and specific incidents that illustrate their approach.

2.4.1 Russia



Russia's cyber strategy, rooted in the doctrine of *information confrontation* (informatsionnoye protivoborstvo), treats cyberspace as a decisive arena for shaping adversary behavior and undermining state resilience. This concept integrates cyber operations, information manipulation, and electronic warfare into a unified system designed not only to influence public perception but also to degrade or disrupt critical national infrastructure (CNI) in rival states.

Following the 2015 military doctrine, Russia institutionalized specialized information and cyber units within its armed forces, prioritizing capabilities that enable infiltration of energy systems, transportation networks, military command structures, and governmental digital infrastructure. These units conduct persistent engagement campaigns aimed at maintaining silent, long-lasting access to vital systems, enabling reconnaissance, pre-positioning for potential sabotage, and shaping adversary decision-making. Russia's conflict with Ukraine has demonstrated the centrality of critical infrastructure targeting in its operational approach.

Cyberattacks on energy grids, satellite communications, and logistics networks have been synchronized with kinetic military operations, illustrating Russia's view of CNI disruption as a force multiplier in hybrid warfare.

2.4.1.1 Russia's Cyber Power: Key Institutions and Structures

Russia has expanded and structured its cyber institutions to support sustained operations against foreign critical infrastructure. This evolution reflects a strategic recognition that disrupting power grids, fuel pipelines, telecommunication nodes, and government systems can yield strategic advantages without open confrontation. Cyber institutions work closely with military, intelligence, and security agencies to design and coordinate operations aimed at destabilizing or coercing adversaries through CNI vulnerabilities.

The major institutions involved include:

The Main Directorate of the General Staff (GRU), Russia's military intelligence service, is the principal driver of offensive cyber operations against foreign critical infrastructure.

- **Unit 26165 (APT28/Fancy Bear):** Focuses on cyber espionage targeting defense, government, and industrial sectors. While historically known for its political intrusions, it is increasingly collecting intelligence on critical infrastructure ecosystems, including supply chains and operational technology (OT) networks.
- **Unit 74455 (Sandworm Team):** The primary Russian entity associated with destructive cyber operations against CNI. Sandworm has historically targeted electric grids, industrial control systems (ICS), and public utilities. Its operations against Ukraine's power grid and the NotPetya campaign exemplify the unit's capacity to conduct widespread disruption.
- **Unit 29155:** Although traditionally linked to covert physical operations, this unit increasingly participates in hybrid missions that combine digital and physical sabotage, aimed at undermining the resilience of infrastructure abroad.

Federal Security Service (FSB) The FSB oversees domestic cyber control and plays a significant role in foreign cyber operations targeting CNI. Its cyber units engage in attacks on government systems, telecommunications, energy infrastructure, and financial networks. Domestically, the FSB enforces surveillance regimes like SORM, controls data localization compliance, and secures CNI against foreign intrusion. Internationally, it conducts espionage and disruption campaigns, including operations aimed at undermining electoral systems, energy companies, and industrial enterprises.

Key units include:

Centre 16 (Main Offensive Cyber Unit)

- Conducts foreign hacking, espionage, and long-term intrusions.
- Linked to advanced malware and attacks on critical infrastructure.

18th Centre Information Security Centre

- Focuses on domestic cyber control, censorship, and counterintelligence.
- Works with telecoms to monitor internet traffic inside Russia.

Operational-Technical Directorate (OTU)

- Handles technical surveillance and communications interception.
  Supports hacking operations with SIGINT capabilities

Scientific-Technical Service

- Develops cyber tools, exploits, and technical equipment.
  Serves as the FSB's R&D lab for cyber operations.

Regional FSB Cyber Departments

- Local teams supporting surveillance and cyber operations in each region.
- Provide access to local infrastructure and assist national units.

The Foreign Intelligence Service (SVR) conducts long-term cyber espionage operations targeting foreign governmental and industrial systems, particularly those managing sensitive infrastructure, such as nuclear facilities, aerospace sectors, and energy production facilities.

Key units include:

- **Unit 26165/26166 (APT29/Cozy Bear):** Specializes in stealthy, multi-year intrusions into government, diplomatic, and strategic infrastructure networks. Its operations often seek deep, covert access to systems that manage essential services.
- **Unit 74455 (SIGINT-related elements):** Involved in accessing and exploiting technical systems associated with critical infrastructure networks for **intelligence collection and potential pre-positioning.**
- **Support Units:** Maintain secure communication channels, command-and-control systems, and infrastructure used to sustain long-term access to foreign CNI.

Contracting Ecosystem

Russia relies on a diverse ecosystem of contractors, proxies, and criminal networks to support cyber operations targeting critical infrastructure worldwide.

- **State-sponsored APTs** execute the most sophisticated CNI-focused campaigns, including the development of ICS-targeted malware and reconnaissance of industrial networks.
- **Organized Crime Groups (OCGs)** conduct ransomware and intrusion campaigns that frequently target healthcare providers, energy companies, and municipal infrastructure. Although financially motivated, many operate with state tolerance or cooperation, indirectly furthering Russia's strategic aims.
- **Pro-Russian hacktivists conduct DDoS** attacks and information operations targeting infrastructure sectors in NATO states and Ukraine, often in alignment with broader Russian objectives.

While all three Russian intelligence services, FSB, SVR, and GRU, conduct offensive cyber operations, their emphases diverge markedly. FSB units generally prioritize domestic surveillance and long-term access operations. SVR focuses on strategic espionage and stealthy collection against high-value foreign targets, while GRU specializes in aggressive, high-tempo campaigns, including those with disruptive and destructive effects. Competition and occasional overlap between these services have accelerated capability development, steadily increasing Russia's capacity for both covert intelligence collection and real-world cyber disruption.

2.4.1.2 Operational Objectives and Tactics

Russia's cyber operations against critical infrastructure pursue several interrelated strategic objectives:

- **Intelligence Collection:** Targeting energy grids, water systems, transportation networks, and military logistics to gather operational intelligence and map vulnerabilities.
- **Disruption and Sabotage:** Demonstrated through attacks on Ukraine's electricity grid and other essential services, aimed at causing societal destabilization and pressuring adversary governments.
- **Pre-positioning for Contingency Operations:** Maintaining long-term access within foreign CNI enables potential future sabotage during crises or conflicts.

Russia employs a range of tactics, including spear-phishing, supply chain intrusions, exploitation of zero-day vulnerabilities, and the deployment of malware specifically designed for industrial control systems. These techniques are frequently synchronized with broader hybrid warfare strategies that combine cyber disruption with kinetic, political, and psychological pressure.

2.4.1.3 Target Profile and Geographical Focus

Russia's targeting priorities emphasize foreign critical infrastructure:

- **Ukraine:** The highest-priority target, with continuous attacks on power, telecommunications, military logistics, and government systems.
  Western Nations (U.S., U.K., EU Members): Targeted for both espionage and disruption, particularly sectors connected to energy, defense production, and logistics supporting Ukraine.
- **International Organizations:** Entities such as NATO and OPCW remain persistent intelligence targets, including their operational systems and supporting **infrastructure.**
- **Private Sector:** Particularly companies operating in energy, aerospace, telecommunications, and advanced technology sectors that contribute to national resilience.

Evolution and Trends in Russia's Cyber Capabilities

Russia's cyber capabilities against critical infrastructure have advanced significantly. The transition from general-purpose malware to heavily customized ICS-targeted tools demonstrates a strategic investment in precision sabotage. Russian operators are increasingly integrating AI and machine-learning elements into reconnaissance, vulnerability analysis, and automated decision-making for intrusion campaigns. A continued emphasis on persistent access reflects Russia's goal of maintaining operational readiness within adversary CNI. The Ukraine conflict highlights the fusion of cyber and conventional operations, with cyberattacks used to shape the battlespace, disrupt command systems, and degrade infrastructure supporting military operations.

2.4.2 China



China’s cyber strategy represents a comprehensive and multifaceted approach that integrates political, military, economic, and technological dimensions, with a pronounced focus on the security, manipulation, and potential disruption of foreign critical infrastructure systems. At its core, this strategy is guided by the concept of “informatization,” which emphasizes leveraging advanced information and communication technologies to enhance national power, shape strategic conditions, and secure national interests.

For China, cyberspace is not merely a platform for communication or economic activity; it is a decisive arena for national security, international competition, and shaping geopolitical outcomes. Beijing conducts its cyber activities through a civil-military fusion model, enabling seamless cooperation among state agencies, private technology firms, academic institutions, and the People’s Liberation Army (PLA). This structure allows for the expansion of its cyber capabilities, protecting domestic critical infrastructure while simultaneously developing offensive tools designed to penetrate, map, and potentially disrupt the infrastructure of foreign states. Chinese cyber units routinely engage in reconnaissance of electric grids, telecommunications backbone networks, satellite infrastructure, maritime logistics systems, and industrial control systems (ICS). Offensive objectives include preparing “access points” for future conflict, enabling coercive pressure, and degrading an adversary’s ability to coordinate military or political responses during crises.

2.4.2.1 China's Cyber Power: Key Institutions and Structure

China’s national cyber system has evolved from fragmented early efforts into a centralized structure capable of executing large-scale operations against foreign critical infrastructure. This development reflects Beijing’s understanding that control over essential services, energy, transportation, water systems, and communications forms the backbone of both national resilience and strategic advantage. China has constructed a layered architecture involving military cyber forces, civilian intelligence agencies, and central regulatory bodies, each contributing to the nation’s ability to infiltrate, monitor, or disrupt critical infrastructure abroad. These institutions include the newly established People’s Liberation Army Cyberspace Force, the Ministry of State Security’s cyber apparatus, and overarching bodies such as the Central Cyberspace Affairs Commission. Together, they form an integrated network designed to assert cyber sovereignty, shape international norms, and project digital influence.

People's Liberation Army (PLA) Cyberspace Force

Established in April 2024, the PLA Cyberspace Force is China's primary military body for cyber warfare, including cyberattacks on critical infrastructure systems globally. Operating under the Central Military Commission, it replaced the former Network Systems Department of the Strategic Support Force. Its focus includes offensive penetration of power grids, transportation networks, satellite infrastructure, and military-critical communication systems.

- **Offensive Operations Division.** This unit conducts intrusions into foreign critical infrastructure, including electric utilities, maritime logistics systems, air traffic control networks, and ICS/SCADA environments. Its missions include establishing persistent access, mapping interdependencies, and positioning malware for potential disruption or sabotage during crises.
- **Cyber Defense Division.** Responsible for securing PLA infrastructure and ensuring the resilience of China's own critical systems. The division develops defensive tools for industrial networks, hardens systems against foreign intrusion, and monitors for adversary reconnaissance activities targeting China's power and communication sectors.
  Cyber Intelligence Division. Conducts reconnaissance on adversary ICS networks, supervisory control environments, and emergency response systems. It collects detailed intelligence needed to exploit vulnerabilities in foreign critical infrastructure.
- **Electronic Warfare Division.** Integrates cyber and electronic operations against communication satellites, radar systems, and battlefield sensors, aiming to disrupt the command and control capabilities that depend on critical infrastructure networks.

Associated APT Groups

- **APT3 (Gothic Panda):** Known for targeting telecommunications and energy sectors with advanced intrusion methods.
  APT40 (Kryptonite Panda): Conducts extensive operations against maritime infrastructure, ports, and research institutions tied to critical supply chains.

Ministry of State Security (MSS)

The MSS oversees China's covert cyber-espionage and counterintelligence operations, including those targeting foreign critical infrastructure. Its cyber activities primarily operate through the 13th Bureau and various provincial units. These entities work with contractors, universities, and front companies to conduct espionage and preposition access points.

- **13th Bureau (CNITSEC).**
  Functions as the MSS cyber headquarters and engages in identifying vulnerabilities in global infrastructure systems, developing ICS-focused malware, and penetrating sectors such as banking, energy, and telecommunications.
- **Provincial MSS Cyber Units.** Conduct regional APT operations targeting local power distributors, port authorities, and industrial manufacturers. These units frequently collaborate with local technology firms to exploit supply chain access.
- **Chinese National Vulnerability Database (CNNVD).** Administered by CNITSEC, CNNVD has been used to selectively delay disclosure of vulnerabilities affecting industrial systems, enabling MSS teams to exploit them against infrastructure operators abroad.

Associated APT Groups

- **APT1 (Comment Crew):** Known for historic attacks on critical infrastructure-related industries.
- **APT10 (Stone Panda)**: Conducts supply-chain attacks to infiltrate infrastructure operators through managed service providers.
  APT27 (Emissary Panda): Targets ICS-rich sectors, including aerospace and defense manufacturing.
- **APT31 (Zirconium):** Conducts reconnaissance and infiltration of government and infrastructure-related systems.

Central Cyberspace Affairs Commission (CCAC) & Cyberspace Administration of China (CAC)

These bodies direct and enforce China's overarching cyber governance model, establishing policies that shape both domestic critical infrastructure security and international cyber posture.

- **CCAC sets** national policy and ensures cyber operations are aligned with strategic goals, including preparing for contingencies involving foreign infrastructure.
- **CAC regulates** data security, oversees the protection of critical infrastructure within China, and enforces mandates on domestic tech firms.
- **CNCERT/CC** monitors cyber incidents, coordinates responses, and conducts technical exchanges that indirectly support operations against foreign infrastructure by building expertise in industrial control environments.

Associated APT Activities. While not directly linked to APT groups, their regulatory authority creates an ecosystem that supports state operations through mandatory cooperation from the technology and infrastructure sectors.

Contracting Ecosystem

China's "military-civil fusion" strategy integrates civilian companies into cyber operations targeting critical infrastructure. State-owned enterprises, such as China Telecom, State Grid-affiliated companies, Huawei, and cybersecurity firms, contribute specialized access and capabilities. These entities often support reconnaissance and intrusion efforts targeting power grids, telecommunications backbones, undersea cables, railway networks, and industrial systems abroad. Universities and research institutes develop ICS malware, AI-driven vulnerability discovery tools, and methods for exploiting embedded systems, which are standard in water treatment, gas pipelines, and manufacturing plants.

Meanwhile, patriotic hacker groups, often indirectly guided by state actors, conduct opportunistic attacks against foreign infrastructure, adding plausible deniability while expanding China's cyber reach. While both the PLA's cyber units and the MSS engage in broad, infrastructure-oriented cyber operations, the PLA tends to emphasize military-aligned objectives, including strategic intelligence collection, network reconnaissance, and support to wartime operations. In contrast, the MSS usually focuses more heavily on covert intelligence acquisition, long-term penetration of foreign networks, and the theft of political, economic, and technological secrets. Competition and parallel development between the two systems, PLA elements consolidated under the Strategic Support Force (SSF), and the MSS's provincial and regional technical bureaus have accelerated China's cyber capability maturation. This dual ecosystem has driven specialization, operational resilience, and broader targeting scope, strengthening China's ability to integrate cyber operations with state objectives and, when desired, to produce real-world strategic effects.

2.4.2.2 Operational Objectives and Tactics

China's cyber operations center on strategic objectives tied to global competition and cyber sovereignty, with a significant component involving foreign critical infrastructure. These objectives include securing dominance in the digital domain, gaining leverage over strategic rivals, and shaping global governance norms. Espionage remains essential, targeting key sectors such as electric power, water systems, telecommunications carriers, and transportation hubs. Chinese APT groups have repeatedly breached infrastructure networks worldwide, conducting long-term reconnaissance and maintaining persistent access. Operations have included mapping grid architecture, extracting ICS configurations, and implanting malware with potential for later activation. China also invests heavily in capabilities to sabotage or disrupt infrastructure during crises. PLA-linked groups have developed tools capable of interfering with protective relays, manipulating SCADA interfaces, and disabling communication systems supporting emergency response or military deployment.

2.4.2.3 Target Profile and Geographical Focus

China's targeting of critical infrastructure is global, but with clear regional priorities. The Asia-Pacific region is a primary area of focus, particularly for states involved in maritime disputes or those hosting U.S. military assets. Operations include intrusions into regional power utilities, telecom operators, and transportation networks. Western democracies, including the United States and EU member states, are targeted for intelligence and prepositioning within their infrastructure sectors. Recent operations have focused on electric grids, pipelines, water systems, and telecommunications networks. Countries involved in China's Belt and Road Initiative (BRI) are also frequently targeted for surveillance of infrastructure projects, political developments, and energy logistics that impact China's overseas economic corridors.

Evolution and Trends in China's Cyber Capabilities

China's cyber capabilities continue to evolve, with increasing sophistication in operations targeting critical infrastructure. APT groups such as APT40 and PLA Unit 61398 conduct long-term campaigns involving advanced techniques and persistent access to ICS networks. Chinese operators are integrating AI and machine learning to automate vulnerability discovery in industrial systems, generate tailored phishing content for engineers, and assist in malware development for embedded devices. A growing emphasis on supply chain security is evident, including the exploitation of vulnerabilities in global equipment suppliers and the embedding of surveillance or access mechanisms in exported Chinese technologies used in power grids, telecommunications, and transportation. China also invests heavily in talent development, with academic institutions training specialists in industrial cyber operations, ICS malware analysis, and infrastructure-focused reconnaissance.

2.4.3 Iran



Iran's cyber operations against critical infrastructure are driven by geopolitical tension, retaliatory motives, and a desire to project strength amid economic isolation and military pressure. Although Tehran lacks a formal cyberwarfare doctrine, its behavior reveals a pattern of rapid, event-triggered escalation in which intelligence units and proxy groups shift quickly from espionage to destructive action. These campaigns frequently follow sanctions, military strikes, diplomatic crises, or perceived threats to Iran's strategic interests. As a result, Iranian operators have repeatedly targeted energy facilities, government services, telecommunications networks, and regional civilian infrastructure to impose costs, signal resolve, or deter adversaries.

Iranian tooling typically relies on modified commodity malware rather than sophisticated ICS-specific code, but its impact is often highly destructive. Threat actors deploy wipers, disruptive payloads, and ransomware-style tools designed to erase systems, halt operations, leak data, or send political messages. Landmark attacks such as the Shamoon wiper that devastated Saudi Aramco's operations and the 2022–2023 intrusions that disrupted Albanian government services—underscore Iran's willingness to inflict wide-scale operational damage on essential sectors. These incidents show a consistent pattern: Iran leverages cyberspace to retaliate beyond traditional military boundaries, targeting high-visibility civilian infrastructure where disruption will deliver maximum psychological and political effect.

Events like the 2009 Green Movement, the Stuxnet attack on Iran's nuclear program, domestic unrest surrounding the Mahsa Amini protests, and Iran's strategic alignment with Russia have further sharpened Tehran's focus on both offensive and defensive cyber capabilities. Today, Iran represents one of the most active state actors conducting destructive cyber operations against critical infrastructure. For defenders in the energy, government, and regional service sectors, this means preparing for an adversary whose campaigns are closely tied to geopolitical flashpoints, whose targeting is opportunistic yet calculated, and whose capacity for sudden, high-impact sabotage poses a persistent and escalating threat.

2.4.3.1 Iran's Cyber Power: Key Institutions and Structures

Iran's cyber institutions have evolved into an ecosystem designed not only to secure national networks but also to support offensive operations aimed at critical infrastructure abroad. The expansion of these agencies accelerated after Stuxnet, reflecting Iran's intent to build capabilities capable of penetrating, degrading, and disrupting adversarial energy, industrial, and governmental systems.

The IRGC Cyber Command, the Supreme Council of Cyberspace (SCC), and the Passive Defense Organization collectively shape offensive strategies, coordinate intrusion operations, and develop expertise in ICS/OT (Industrial Control Systems/Operational Technology) environments. These institutions represent a shift toward a more structured approach to cyber power, with the IRGC, in particular, emphasizing long-term access and the disruptive potential within foreign infrastructure networks.

Islamic Revolutionary Guard Corps (IRGC)

- **Basij Cyber Units**: Semi-formal cyber brigades under the IRGC's Basij Militia, composed of volunteers and paramilitary personnel. They focus on information operations, online harassment, social engineering, low-to-moderate intrusion activity, and surveillance of dissidents, while also supporting broader IRGC cyber objectives abroad.

- **Qods Force Cyber Units**: Specialized cyber elements embedded within the IRGC Qods Force, responsible for foreign intelligence collection, regional espionage, and support to IRGC covert operations. They coordinate with allied militias and conduct strategic targeting of governments, military entities, and infrastructure across the Middle East and beyond.

Major IRGC-linked APT groups include:

- **APT35 (Charming Kitten, TA453, Cobalt Mirage):** Conducts espionage and pre-sabotage intrusions, often probing critical infrastructure through credential harvesting and access operations.
- **APT42:** Focused on individuals tied to policy and civil society, but also known to map networks connected to sensitive research and ICS-adjacent institutions.
- **Nemesis Kitten:** Contract-run operators skilled in exploiting infrastructure vulnerabilities, often supporting IRGC objectives related to sabotage and access operations.
  Cotton Sandstorm (NEPTUNIUM): A high-capability actor with a history of targeting geopolitical adversaries' critical infrastructure, such as energy and governmental systems.

Ministry of Intelligence and Security (MOIS)
MOIS oversees technically sophisticated offensive operations with a strong emphasis on accessing and exploiting critical national infrastructure (CNI) sectors. Its units frequently target energy networks, telecommunications infrastructure, maritime systems, and government services.

Major MOIS-linked APT groups include:

- **MuddyWater:** Known for operations against government and telecom infrastructure in the Middle East, often using custom malware to penetrate large networks.
- **OilRig (APT34):** Specializes in the energy sector and has repeatedly targeted ICS-adjacent systems in Gulf states.
- **APT39 (Chafer, Cadelle, Rana Intelligence Computing):** This group specializes in surveillance and data theft, primarily targeting the telecommunications, aviation, travel, and government sectors. The U.S. government has sanctioned Rana Intelligence Computing Company as a front for APT39's operations.
- **Hexane:** Focuses on telecom and infrastructure providers, supporting long-term reconnaissance and access operations.
- **Agrius(TA455, Smoke Sandstorm, Pink Sandstorm):** Conducts espionage with the capability for destructive actions against industrial and maritime sectors.

- **DarkBit (DEV-1084):** Engages in disruptive and destructive cyberattacks, including operations against academic and industrial research infrastructure.

While both the MOIS and the IRGC conduct infrastructure-oriented operations, the MOIS tends to focus more heavily on the technical exploitation of networks and ICS components, competition between the two has driven innovation, increasingly enhancing Iran's capacity for real-world disruptive effects.

Contracting Ecosystem

Iran relies on a network of private contractors and academic institutions to expand offensive capacity, including ICS exploitation. Emennet Pasargad operates Cotton Sandstorm for the IRGC, enabling large-scale influence and intrusion campaigns. Ravin Academy, founded by MOIS veterans, trains cyber operators—many of whom specialize in penetration techniques for critical infrastructure. Earlier contractors, such as Mabna Institute and ITSecTeam, played foundational roles in developing Iran's initial offensive toolsets, including capabilities used against research institutions and industrial systems.

2.4.3.2 Operational Objectives and Tactics

Iranian operations now place significant emphasis on compromising, disrupting, or destructively targeting critical infrastructure. Espionage supports this goal by providing technical mapping, access credentials, and ICS reconnaissance.

Examples include:

- **OilRig's 2022 intrusion into Jordan's Foreign Ministry**, which leveraged custom malware often repurposed for infrastructure penetration.
  Domestic Kitten's mobile surveillance, supporting regime control through monitoring internal communication networks and sensors.
- **APT35's TelegramGrabber** collects data that can support follow-on operational planning, including infrastructure mapping.

Destructive Operations: Iran's destructive cyber operations increasingly mimic ransomware or hacktivist activity to obscure attribution. These attacks commonly target energy, government, telecom, and research infrastructure:

- **Shamoon (2012)** crippled Saudi Aramco's industrial operations.
  The **Albanian government attack (2022)** by OilRig and Hexane disrupted government services, demonstrating the capability against national-scale infrastructure.
- **DarkBit's 2023 attack on Israel's Technion Institute**, enabled by MuddyWater access, demonstrated Tehran's maturing destructive playbook.

The proliferation of fake hacktivist fronts such as "Homeland Justice" enables Iran to launch destructive operations against critical infrastructure while maintaining plausible deniability.

2.4.3.3 Target Profile and Geographical Focus

Iran overwhelmingly targets **critical infrastructure sectors**, using a mixture of espionage, pre-positioning, and destructive attacks.

Key sectors include:

- **Energy:** APT33, OilRig, and IRGC units have long targeted petrochemical plants, power grids, and energy ministries across the U.S., Gulf, and Israel.
- **Telecommunications:** Targeted for signals intelligence and disruption potential, with MOIS groups especially active.
  Transportation: Maritime and air transport sectors, especially in the Strait of Hormuz region, are targeted by APT35 and UNC3890 to support both strategic intelligence and potential disruption.
- **Government & ICS/OT Systems:** Evidence suggests that Iran seeks access to U.S. and Israeli industrial control systems, including those used in water facilities, utility providers, and municipal services.

Geographical Focus:

- **Middle East:** The primary arena, with heavy targeting of Israeli and Gulf infrastructure.
- **United States:** Significant increases in 2022–2023, including attempts to compromise energy and water facilities.
- **Europe/Balkans:** Less frequent but high-impact attacks, such as the Albanian government incident.

2.4.4 North Korea



North Korea's cyber strategy has evolved into a central pillar of its asymmetric warfare doctrine, with a growing emphasis on targeting foreign critical infrastructure to compensate for its conventional military disadvantages and persistent economic isolation. Under Kim Jong-un, Pyongyang has deliberately expanded its capabilities designed to disrupt the essential services of adversarial nations, such as energy grids, transportation networks, communications systems, and financial infrastructure. Cyber operations are used not only for national security and regime survival but also as a mechanism for strategic coercion and disruption.

The underlying doctrine prioritizes offensive, covert, and opportunistic operations that exploit attribution challenges in cyberspace. Compared to traditional cyber powers that emphasize defense, North Korea uses cyber tools to impose asymmetric costs, probe systemic vulnerabilities, and signal its capacity to disrupt essential civilian and military infrastructure. These activities allow Pyongyang to destabilize adversaries, test response thresholds, and impose psychological and economic pressure without triggering open conflict. Cyber operations targeting critical infrastructure fit within North Korea's broader gray-zone strategy, enabling the state to threaten societal stability and national resilience while remaining below the level of armed confrontation.

2.4.4.1 North Korea's Cyber Power: Key Institutions and Structures

North Korea's cyber activities, especially those directed against critical infrastructure, are managed through a highly centralized structure under direct regime control. The Reconnaissance General Bureau (RGB) serves as the primary authority for orchestrating cyber operations against foreign infrastructure systems. As the chief military intelligence body, the RGB oversees attacks on power grids, transportation management systems, telecommunications networks, and other essential services. It reports to the State Affairs Commission, underscoring the high strategic priority of cyber capabilities within national policy.

Main Cyber Units

- **Bureau 121 (Unit 121):** The Bureau 121 is North Korea's primary cyber warfare command within the Reconnaissance General Bureau, responsible for offensive cyber operations worldwide. It conducts strategic espionage and disruptive campaigns against critical infrastructure, often coordinating other specialized units.

- **Unit 180:** The Unit 180 specializes in financial cyber operations designed to generate illicit revenue for the regime. Its operators conduct bank intrusions, cryptocurrency theft, and economic manipulation to circumvent international sanctions.
- **Lab 110 (110 Research Center):** Lab 110 serves as North Korea's central cyber R&D and malware development hub. It creates tools, exploits, and destructive payloads used by multiple DPRK APT groups in global operations.

APT Groups

- **Lazarus Group:** Lazarus Group is the most notorious DPRK threat actor, responsible for destructive attacks like Sony and WannaCry. It conducts high-impact espionage, sabotage, and large-scale financial theft operations worldwide.
- **APT38:** The APT38 is a financially focused subgroup associated with Lazarus, specializing in high-value theft from banks and cryptocurrency platforms. It targets interbank transfer systems such as SWIFT with long-term, well-resourced intrusions.
- **Andariel: The** Andariel primarily targets South Korea's defense, energy, and transportation sectors to weaken military readiness and disrupt civilian infrastructure. It also carries out ransomware and criminal-style attacks to supplement state revenue.
- **APT37**: The APT37 (Ricochet Chollima) is an espionage-focused group that targets governments, militaries, and research institutions, especially in South Korea and Asia. It is known for using zero-day exploits and advanced infiltration techniques to gather intelligence.
- **APT43: The** APT43 blends espionage with financial operations, focusing on credential theft, surveillance, and cryptocurrency collection. It supports DPRK intelligence agencies by gathering strategic information and generating funds through crypto theft and laundering.
- **Kimsuky:** Kimsuky is a North Korean espionage group that targets think tanks, government agencies, and foreign policy experts. It specializes in credential harvesting and long-term information collection, often employing phishing and social engineering tactics.

While multiple RGB elements engage in infrastructure-oriented operations, Unit 121 remains North Korea's primary actor for disruptive and strategic intrusions, particularly against foreign critical infrastructure and government bodies responsible for national resilience. Its affiliated groups add complementary specialties that collectively expand Pyongyang's operational reach. Unit 180 focuses on financially driven intrusions, generating illicit revenue that sustains the regime's military and weapons programs. The Lazarus Group conducts high-impact, destructive operations across energy, healthcare, and major industrial sectors, demonstrating an apparent willingness to escalate.

APT38 extends beyond monetization into deep reconnaissance of global financial architecture, probing payment networks and interbank systems for opportunities that could enable both large-scale theft and systemic disruption. Andariel targets South Korean defense, energy, and transportation, aiming to erode military readiness and disrupt civilian services. Collectively, these units form a mutually reinforcing operational ecosystem within the RGB. Their overlapping missions and internal competition drive rapid innovation, steadily enhancing North Korea's capacity to move beyond espionage and theft toward coordinated, real-world disruption.

Contracting Ecosystem

A global, covert contracting ecosystem enables North Korea to support cyber operations targeting critical infrastructure while reducing attribution risk. Front companies, remote IT workers, and proxy developers embedded in foreign firms provide Pyongyang with access to global infrastructure supply chains and technical environments. These operatives, often positioned in China, Southeast Asia, Eastern Europe, and Africa, gain proximity to software and systems used in energy management, industrial automation, financial transaction routing, and other infrastructure-dependent sectors. Their work allows the regime not only to generate income but also to collect technical details that can later be leveraged in targeted penetrations of critical systems.

This hybrid ecosystem blurs distinctions between state actors, contractors, and criminal proxies, complicating defensive attribution and response. It also serves as a reconnaissance mechanism, mapping infrastructure networks that North Korea may exploit during times of geopolitical crisis.

2.4.4.2 Operational Objectives and Tactics

North Korea's operational goals increasingly prioritize exploiting and disrupting critical infrastructure in adversarial nations. Political objectives include intimidating opponents by demonstrating the ability to compromise essential services, undermine societal stability, and erode confidence in government protection of infrastructure. Military objectives involve infiltrating systems associated with defense logistics, satellite communications, and national-level command and control, enabling North Korea to gather intelligence or preposition destructive capabilities for future contingencies. Economic objectives focus on both revenue generation and disrupting financial infrastructure to weaken adversarial economies. To support these aims, North Korean operators employ a broad suite of tactics, including spear phishing for initial entry, the deployment of wiper malware targeting industrial networks, ransomware aimed at infrastructure operators, and supply-chain attacks on vendors servicing critical sectors.

Their technical toolbox includes ICS-specific malware, custom modules designed for SCADA environments, living-off-the-land techniques within operational technology (OT) networks, domain fronting, encrypted C2 channels, and multi-layer proxy chains. Operators excel at masking their activity within global infrastructure routing, making detection and attribution difficult.

2.4.4.3 Target Profile and Geographical Focus

North Korea's target profile demonstrates a deliberate and expanding focus on critical infrastructure worldwide. Energy providers, water treatment facilities, telecommunications operators, transportation systems, emergency services networks, and financial infrastructure have all been subject to probing, espionage, or active disruption. While financial targets (such as banks and cryptocurrency exchanges) remain central for revenue generation, infrastructure-focused operations aim to weaken adversaries' resilience and create strategic leverage.

Examples include intrusions into South Korean power and transportation networks as well as reconnaissance of U.S. and Japanese critical infrastructure sectors. North Korea's operations span regions including the Korean Peninsula, Southeast Asia, Europe, the Middle East, and parts of Africa, where defense postures vary and vulnerabilities are plentiful. Targeting patterns remain adaptive and opportunistic, shifting in response to political tensions, sanctions, and global crises. This agility allows Pyongyang to identify and exploit emerging vulnerabilities within rapidly evolving infrastructure ecosystems.

Evolution and Trends in North Korea's Cyber Capabilities

North Korea's cyber capabilities have evolved from basic website defacements to sophisticated operations aimed at compromising or disrupting critical infrastructure systems worldwide. Early campaigns focused on DDoS attacks, but by the mid-2010s, North Korean units had begun developing malware capable of penetrating industrial networks and high-value infrastructure environments. Recent advancements show a significant rise in sophistication. Operators now deploy modular malware targeting OT systems, leverage advanced evasion techniques, and use custom-built tools for industrial intrusions. They are increasingly capable of crafting ICS- and SCADA-specific payloads similar to those used by advanced global state actors. North Korea has also invested in exploiting emerging technological trends, including AI-assisted spear phishing, vulnerabilities in IoT devices tied to infrastructure, and weaknesses in blockchain-based systems that underpin digital financial infrastructure. Continued training, structural integration of cyber units within military intelligence, and persistent investment in offensive tools suggest that North Korea's ability to threaten critical infrastructure will grow, reinforcing its position as an enduring asymmetric threat.

2.5 Attack Vectors and Campaign Patterns

Attack vectors and campaign patterns describe how adversaries gain footholds in, move through, and achieve objectives within critical infrastructure environments. Understanding them is essential because these systems combine high-impact physical processes with long-lived, often legacy, digital control systems. Rather than a catalog of specific exploits, this section frames the conceptually distinct ways attackers bridge the cyber-physical gap, ranging from remote network intrusions and supply-chain compromises to insider-enabled access and physical tampering, often orchestrated as multi-stage campaigns that layer reconnaissance, initial access, privilege escalation, lateral movement, and timed disruption or data exfiltration.

Campaigns against utilities, transportation networks, and industrial control systems often exploit predictable operational rhythms (such as maintenance windows and patch cycles), weak segmentation between IT and OT, and bespoke protocols or unsupported devices, creating opportunities for persistence and cascading failures that can propagate across dependent services. Equally important are the stylistic patterns of commodity tooling versus tailored exploits, the blending of covert and noisy tactics, and coordination across geopolitical timeframes that reveal the attacker's intent, resources, and tolerance for collateral impact.

By focusing on the structural mechanics and temporal choreography of these vectors and campaigns, defenders can prioritize detection, hardening, and response strategies that reduce systemic risk and increase resilience across the critical infrastructure ecosystem. The following attack vectors are among the most common ones used by threat actors while targeting essential infrastructures (Figure 1).



Figure 1 - Attack vectors landscape

Credential & Remote-Access Abuse
Threat actors still prefer stealing or abusing credentials and remote-access tools (VPN, RDP, jump hosts). This vector provides quick, broad access to both corporate and operational networks, often bypassing endpoint controls. Operational implication: priority defenses are MFA, conditional access policies, removing unused admin accounts, and continuous monitoring of remote sessions. Rapid detection of anomalous login patterns (time, geography, device posture) is the single most actionable early-warning signal.

Spear-phishing & Social Engineering
Highly targeted phishing and voice/social manipulation remain the bread and butter for gaining a foothold, especially when human operators control OT systems. Attackers combine careful reconnaissance with crafted messaging to obtain credentials, approval, or trick staff into running maintenance tasks. Operational focus: Protect privileged operator channels, conduct frequent and realistic phishing drills, and instrument approval workflows to ensure every change has an auditable, multi-person trail.

- **Initial-Access Brokers & Third-Party Compromise**
  There is a marketplace for pre-built access credentials, persistent backdoors, or vendor compromises that lowers the bar for complex attacks.

  Attackers can buy a ticket to the network instead of building one. Operationally, treat third-party access as hostile until proven otherwise. This requires short-lived credentials, recorded and audited vendor sessions, and strict network segmentation between vendor tools and control systems.

- **Supply-Chain Injection**
  Compromising software updates, CI/CD pipelines, or bundled libraries lets attackers spread trusted malware widely and stealthily. The operational risk is systemic: a single upstream compromise can simultaneously affect multiple downstream operators. Controls: verify code provenance (signatures and SBOMs), tightly restrict build environments, and implement the ability to roll back to known-good artifacts quickly.

- **Device & Firmware Tampering**
  Tampering with firmware or compromising device boot chains enables attackers to achieve persistence that persists even after reimages and appears as normal device behavior. In critical infrastructure, long-lived field devices create attractive targets for cyberattacks. Operational mitigations include secure boot, firmware integrity checks, supplier audits, and strict inventory/chain-of-custody procedures for field device hardware and firmware.

- **Protocol & Controller Exploits (ICS/SCADA)**
  Attacks that target PLCs, RTUs, or field protocols (e.g., Modbus, DNP3, IEC families) are used when the objective is physical impact. These require detailed mapping of processes and timing, and often include malicious ladder logic or command injections. Defenders must monitor logic changes, baseline process metrics, and keep OT networks isolated with only tightly controlled gateways for data flow.

- **Living-off-the-Land & Fileless Techniques**
  To avoid detection, adversaries use legitimate admin tools and in-memory payloads rather than dropping obvious malware. In OT networks, where legitimate admin activity is already noisy, these techniques blend in. Operational detection must therefore focus on unusual sequences of legitimate commands, atypical scheduling patterns, and suspicious use of native tooling rather than on file signatures.

- **Data Exfiltration & Coercive Extortion**
  Attackers stage and extract targeted datasets (designs, safety logs, billing records) to maximize leverage for ransom or political pressure. Exfiltration is often through cloud storage, encrypted tunnels, or trusted third-party endpoints. Operational controls: monitor large or irregular data flows, enforce egress filtering, and classify & isolate the most sensitive data so it cannot be quietly staged.

- **Ransomware & Hybrid Extortion on OT-Adjoining Systems**
  Ransomware actors deliberately target IT systems that, if disrupted, force the shutdown or safe shutdown of OT operations (billing, authentication servers, remote management). They combine encryption with public data dumps to increase pressure. Operational readiness must include tested manual/air-gapped control modes, immutable backups, and rapid communication playbooks that include regulators and customers.

- **Availability Attacks & Cyber-Kinetic Blends**
  Attacks aimed at degrading availability, such as DDoS against control-plane services, GNSS/timing jamming, or deliberate routing manipulation, are used to cause operational chaos without necessarily affecting controllers. In wartime or high-tension scenarios, these are often coordinated with physical or electronic attacks. Defenders should plan redundant timing and comms sources, DDoS mitigation, and manual fallback procedures for critical control operations.

- **Insider & Contractor Abuse**
  Insiders, whether malicious or compromised, and contractors with privileged access can drastically shorten the attacker's path to impact. Operationally, enforce least privilege, use session recording for all privileged operations, apply just-in-time privileged access, and monitor for anomalous procedural deviations that suggest unauthorized assistance.

2.5.1 Typical Attack Choreography Against Critical Infrastructure

This chart visualizes a typical attack choreography against critical infrastructure, showing the common sequence of stages from reconnaissance and initial access through lateral movement to impact. The shaded peaks indicate where attackers most often concentrate their activity and where defenders should prioritize detection and containment (Figure 2).

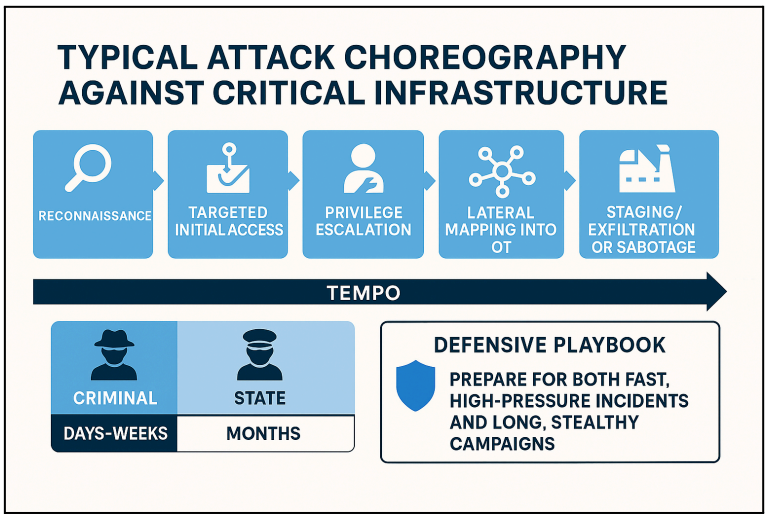


Figure 2 - Critical Infrastructure Cyber Attack Process Chart

2.6 Global Trends and Strategic Implications

Organizations today are navigating a security landscape defined by accelerating attacker capabilities, expanding identity exposure, concentrated third-party dependencies, and the rapid infusion of AI into both offense and defense. These shifts are reshaping how risk materializes and what effective resilience requires. The following trends and their strategic implications outline where leadership attention must focus to sustain operational integrity and reduce the impact of inevitable cyber incidents.

- **Faster, Cheaper Attack Buildouts**
  Access marketplaces and RaaS compress attacker timelines. Strategic implication: prioritize rapid containment capabilities over prevention-only investments.

- **Identity as the New Perimeter**
  As OT and IT converge, identity compromise is the pivot to catastrophic outcomes. Strategic implication: treat identity controls (MFA, conditional access, JIT privileges) as core infrastructure.

- **Supply-Chain & Third-Party Systemic Risk**
  A small set of vendors and platforms creates cascading vulnerability. Strategic implication: adopt sector-level contingency planning and limit single points of failure.
- **AI-Augmented Offense and Defense**
  AI enhances lure quality and reconnaissance, while also strengthening detection. Strategic implication: invest in explainable, human-in-the-loop AI detection and crisis-play automation.
- **Deterrence by Denial and Resilience**
  Attribution is often slow or ambiguous, so deterrence by denial, making attacks costly and fruitless, and rapid recovery are the most reliable defenses.
- **Strategic implication**
  Align board-level KPIs with resilience metrics (time-to-recovery, manual-control readiness).

3. Sectoral Cyber-Physical Risk Assessment

3.1 Energy

3.1.1 Power Generation Facilities

Critical to a Nation's Functioning

Power generation facilities, whether large thermal plants, hydroelectric dams, nuclear reactors, or renewable energy parks, are the starting point of the entire electricity value chain, and their reliability directly conditions the stability of the grid. These assets not only supply bulk power but also often provide essential ancillary services, such as frequency control, voltage support, and spinning reserve, that keep the grid synchronized and resilient. A loss of central generation units can force operators to implement load shedding, import expensive emergency power, or risk widespread outages if frequency deviates too far. Because new plants are capital-intensive and slow to build, a nation's generation portfolio is difficult to adapt quickly to sudden changes or attacks, making existing units extremely strategic. Some plants, such as extensive hydroelectric and nuclear power facilities, are also critical to water management or national prestige, further increasing their symbolic importance. In many countries, a small number of facilities provide a disproportionately large share of power, so damage to even a handful can dramatically constrain the entire economy.

Moreover, power generation facilities are often co-located near communities, rivers, or coasts, meaning that operational incidents can have environmental and safety consequences that extend beyond the power supply alone.

Key Elements (Physical and Digital)

Power plants combine heavy mechanical systems with intricate control and safety architectures, supported by on-site and remote digital systems. Their criticality arises not just from the turbines and boilers, but from the interlocking layers of protection, monitoring, and logistics that ensure their safety and efficiency.

Physical infrastructure (Power Generation)

- **Primary energy conversion systems**: Boilers, combustion chambers, steam turbines, gas turbines, hydro turbines, nuclear reactors, generators, and associated rotating equipment.
- **Auxiliary and safety systems,** cooling systems, condensers, pumps, valves, fuel supply and handling systems, emergency core cooling systems (for nuclear), fire suppression systems, and physical containment structures.
  Electrical interface: Step-up transformers, plant switchyards, busbars, breakers, and isolators connecting generation to high-voltage transmission.
- **Fuel and resource infrastructure**: Coal yards, gas pipelines, oil storage tanks, water intake and discharge structures, spent fuel pools, and waste storage where relevant.
- **Site and physical security**: Fencing, barriers, surveillance cameras, guard posts, vehicle checkpoints, and physical access control systems.

Digital infrastructure (Power Generation)

- **Plant control systems**, DCS, PLCs, reactor protection systems, turbine and boiler control systems, and safety-instrumented systems are responsible for maintaining operating parameters within safe limits.
- **Monitoring and diagnostics**: Condition monitoring systems, vibration analysis tools, predictive maintenance platforms, sensor networks, and historian databases.
- **SCADA and remote connectivity** systems link the plant to grid operators and corporate networks, including telemetry, remote dispatching commands, and load-following controls.
- **Business and maintenance IT**: Computerized maintenance management systems (CMMS), engineering workstations, document management, training simulators, and enterprise IT services.
  Cybersecurity and logging tools, Firewalls, intrusion detection/prevention systems, security information and event management (SIEM) platforms, and remote access gateways are used by vendors.

Cyber-Physical Vulnerabilities

The sector is vulnerable to multiple risks, including technical, infrastructural, and human factors (Figure 3).

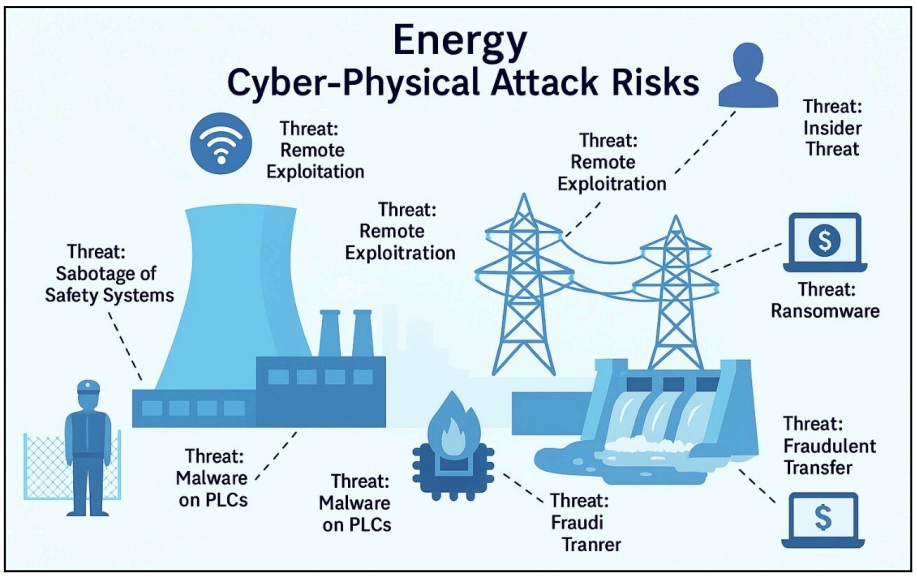


Figure 3 - Main cyber-physical attack risks against the Energy sector

Technical vulnerabilities

Power generation facilities face specialized technical risks because their control systems must balance safety constraints with real-time responsiveness and operational efficiency. Legacy DCS and safety systems may lack modern security features, such as strong authentication or secure protocol support, and are difficult to patch without extensive testing due to safety certification requirements. If engineering workstations or maintenance laptops are compromised, attackers can modify logic in PLCs or upload malicious configurations that subtly change setpoints or turn off protections. Remote access paths used by original equipment manufacturers (OEMs) for support often rely on VPNs or jump servers that, if misconfigured, can be exploited for deep access into plant networks. Nuclear plants and other high-hazard facilities may depend on “air-gapped” networks; however, in practice, removable media, engineering data transfers, and human bridging frequently compromise this isolation. Misconfigured network segmentation within the plant can allow non-critical systems, such as condition monitoring or administrative terminals, to be compromised and spread to safety-critical zones, thereby increasing the risk that attackers can influence core process controls or safety interlocks.

Infrastructure and systemic vulnerabilities

From an infrastructure perspective, major generation plants are inherently high-value targets whose geographic location and unique design make redundancy difficult. Many plants are situated near water bodies or coasts for cooling, exposing them to floods, storms, or environmental hazards that can coincide with cyber incidents, complicating response. Because specific units provide irreplaceable services, such as primary frequency regulation or black-start capability, losing them can severely limit grid operators' options during restoration.

Critical spare parts for turbines, generators, or control systems often have long lead times and depend on international suppliers, making recovery from physical damage slow if supply chains are disrupted. Operationally, plants may run at high capacity for long periods, pushing maintenance windows into tight schedules where security upgrades are deprioritized. If a coordinated attacker manipulates both digital controls and physical access (for example, disabling alarms while sabotaging cooling systems), the plant's layered defenses can be overwhelmed. Dependencies on external telecom links for dispatch and SCADA communications also introduce single points of failure: if communication is lost, operators may have limited visibility into grid conditions when deciding to ramp units up or down.

Human factor vulnerabilities

Human factors play a decisive role in the safety and security of power plants, as operators must interpret complex information streams and act under time pressure. Ingrained operating cultures often emphasize production targets and minimize outages, potentially leading staff to override automated protections or disregard security procedures perceived as slowing operations. Training for cyber threats may lag behind technical training on plant operations, leaving control room staff reliant on IT teams who are not present 24/7 in the control environment. Contractors and temporary workers, who are often employed during outages and maintenance campaigns, may be granted extensive physical and logical access with limited vetting or oversight, thereby increasing the likelihood of insider threats or inadvertent errors. Social engineering attacks, such as spear-phishing directed at engineers and plant managers, can yield credentials with high privilege, especially when combined with publicly available information about plant layouts and systems. In crises such as unexpected trips, grid disturbances, or severe weather, cognitive overload can cause operators to misinterpret alarms, miss subtle indications of cyber manipulation, or delay switching to manual modes that might limit damage. At the governance level, incomplete alignment between safety culture and cybersecurity can result in policies that appear robust on paper but are inconsistently enforced in practice.

Impact on National Security

A cyber-physical attack that degrades or turns off key power generation facilities can have far-reaching consequences, extending beyond temporary electricity shortages. Targeted manipulation of control systems could cause destructive overspeed events, overheating, or coolant failures, leading to turbine damage, fires, or, in extreme nuclear scenarios, even catastrophic consequences. These radiological releases pose a threat to public health and contaminate land and water for decades. Even without catastrophic accidents, the loss of large baseload plants can lead to reliance on emergency imports or expensive peaking units, triggering energy price spikes and economic distress for households and industries.

If attacks are coordinated across several plants, grid operators may be compelled to shed load on a massive scale, plunging cities into darkness and disrupting hospitals, data centers, and transport networks simultaneously. Public panic can escalate rapidly as fuel stations run dry, communication networks falter, and rumors quickly spread via social media, potentially sparking unrest and protests. Adversaries targeting generation assets may aim to undermine confidence in government competence and in the safety of specific technologies (for example, nuclear), influencing national energy policy debates. In a conflict scenario, shutting down key power plants can strategically weaken military installations and command centers that rely on grid power, erode deterrence, and signal an attacker's ability to penetrate deep into critical national infrastructure.

3.2 Healthcare

Critical to a Nation's Functioning

The healthcare sector is central to a nation's resilience, as it protects the population's health, preserves life, and underpins social stability and economic productivity. Beyond treating acute illnesses and injuries, healthcare systems manage chronic diseases, vaccination campaigns, maternal care, and emergency response, all of which keep morbidity and mortality at socially acceptable levels. When healthcare infrastructure is disrupted, not only do immediate medical outcomes worsen, but trust in institutions can erode rapidly, especially if people perceive that the most vulnerable children, older people, and those with disabilities are being abandoned. Healthcare is also closely linked to national security: a healthy population is a prerequisite for an effective workforce and capable armed forces. Hospitals serve as critical nodes in disaster response, pandemics, and mass-casualty events. The sector is susceptible to time because many interventions, such as surgery, intensive care, or stroke management, are extremely time-critical, leaving little margin for delay caused by IT or infrastructure failures. Moreover, public health systems act as an early warning and control mechanism against biological threats, whether natural, accidental, or deliberate, making their integrity essential for biosecurity. Any prolonged degradation of healthcare services can therefore trigger cascading effects across society, magnifying fear, disrupting the economy, and potentially destabilizing the political order.

Key Elements (Physical and Digital)

Healthcare infrastructure encompasses hospitals and clinics, along with complex logistics, supply chains, and information systems. These elements must work together seamlessly to deliver care, store and transport medical products, and maintain accurate patient records.

Physical infrastructure (Healthcare)

- **Hospitals and clinics**, Emergency rooms, operating theaters, intensive care units, wards, outpatient facilities, laboratories, and imaging centers.
- **Medical equipment**: Ventilators, infusion pumps, MRI and CT scanners, X-ray machines, surgical robots, dialysis machines, and bedside monitors.
- **Pharmaceutical and supply chain facilities**, Pharmacies, warehouses, vaccine cold chains, blood banks, and logistics centers for medical supplies and personal protective equipment.
- **Support infrastructure** Includes Power supply and backup generators, oxygen production and distribution systems, water and sanitation facilities, HVAC systems, and physical security/access control.
- **Ambulance and emergency services**: Ambulance fleets, emergency operations centers, and triage facilities that connect patients to hospitals.

Digital infrastructure (Healthcare)

- **Electronic health record (EHR) systems**, Patient databases, clinical information systems, radiology information systems, and laboratory information systems.
- **Clinical devices and networks**: Network-connected monitors, imaging devices, smart infusion pumps, lab equipment, and biomedical IoT devices.
- **Hospital information systems (HIS)**, Admission, discharge, and transfer systems, scheduling tools, pharmacy management, billing, and insurance processing.
- **Telemedicine and public health platforms**, Remote consultation tools, tele-ICU platforms, epidemiological surveillance systems, and health data exchanges between institutions.
- **IT infrastructure and communications**: Data centers, servers, hospital networks, Wi-Fi, secure messaging, VPNs for remote access, and cybersecurity monitoring tools.

Cyber-Physical Vulnerabilities

The sector is vulnerable to multiple risks, including technical, infrastructural, and human factors (Figure 4).

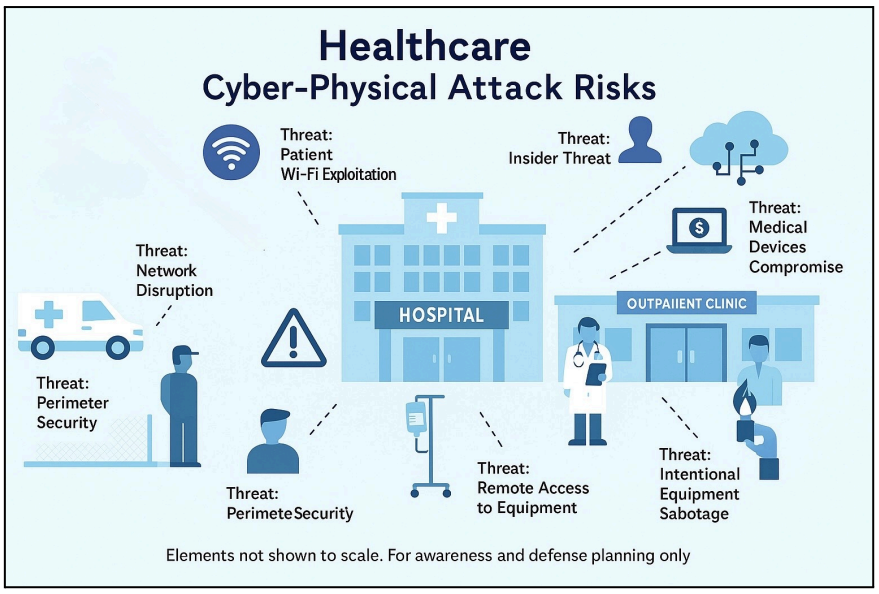


Figure 4 - Main cyber-physical attack risks against the Healthcare sector

Technical vulnerabilities

Healthcare environments often rely on a patchwork of legacy devices and applications, many of which were not designed with cybersecurity in mind, creating a broad technical attack surface. Medical devices may run outdated operating systems, use hard-coded credentials, or lack encryption, making them susceptible to remote compromise or misuse as pivot points inside the hospital network. EHR and HIS platforms are complex, heavily integrated systems that are difficult to patch or take offline, allowing vulnerabilities to remain exposed for extended periods, particularly in smaller hospitals with limited IT resources. The proliferation of Wi-Fi, BYOD policies, and remote access tools for clinicians enables flexibility but also increases entry points for attackers who might exploit weak network segmentation or misconfigured access controls. Ransomware is a particularly acute threat, given that hospital staff may feel compelled to pay to restore systems quickly when patient safety is at risk. Additionally, telemedicine and cloud-based health services introduce dependencies on external providers and internet connectivity, so denial-of-service attacks or outages can abruptly cut off critical services.

Infrastructure and systemic vulnerabilities

Healthcare infrastructure is inherently fragile because it operates close to capacity in many countries, meaning that even modest disruptions can push systems into crisis. Hospitals are heavily dependent on continuous power for life-support equipment and diagnostic devices; if grid power and backup generators fail or fuel supplies are interrupted, patient mortality can increase rapidly. The physical layouts of older hospitals may not incorporate modern security zoning, which can result in easier physical access to equipment rooms or network closets. At a systems level, regional healthcare often relies on a few central hospitals for specialist services, so disabling one or two key facilities can overload the rest, causing widespread service degradation. Supply chains for medicines, blood products, and medical devices are global and time-sensitive, making them vulnerable to disruptions by cyberattacks on logistics companies, manufacturers, or distributors. Public health surveillance systems often rely on timely data from local clinics. If these IT systems are compromised or manipulated, authorities may misjudge the spread of disease or fail to detect outbreaks. The combination of critical dependence on other sectors, particularly energy, telecommunications, and transportation, renders healthcare highly vulnerable to cascading failures that can be triggered elsewhere.

Human factor vulnerabilities

Human factors in healthcare cybersecurity are especially challenging because clinicians' primary focus is rightly on saving lives, not on digital hygiene. Under intense time pressure, staff may reuse passwords, share accounts, leave terminals unlocked, or circumvent security features they perceive as obstructive, such as multifactor authentication. Awareness of phishing and social engineering may be limited, and targeted emails impersonating hospital administrators, insurance companies, or suppliers can easily trick busy staff into clicking malicious links or opening infected attachments. Contractors and visiting specialists, who often need temporary access to medical systems, may receive only minimal security onboarding, yet gain significant privileges. At the management level, security investment can lag behind clinical priorities, leading to under-resourced IT and security teams, outdated policies, and limited incident response training. Stress, burnout, and staff turnover further erode resilience, as institutional memory about past incidents and lessons learned is lost. In crises, such as pandemics or mass-casualty events, human performance may degrade further, making it easier for attackers to exploit confusion, urgency, and the staff's willingness to bypass controls to treat patients more quickly.

Impact on National Security

A cyber-physical attack on the healthcare sector can have immediate life-and-death consequences while also undermining long-term social cohesion and trust in the state. Suppose hospital IT systems are encrypted or corrupted. In that case, clinicians may lose access to patient histories, medication records, imaging studies, and laboratory results, forcing them to delay surgeries, cancel appointments, or operate with incomplete information, which increases the risk of medical errors. Manipulation or disruption of network-connected medical devices, such as infusion pumps or monitors, could directly endanger patients in intensive care or operating theaters. At scale, regional or national disruptions to hospital networks can lead to increased mortality from otherwise treatable conditions, overwhelm emergency rooms, and create visible scenes of chaos that the public interprets as a systemic failure. If public health surveillance systems are compromised, authorities may fail to detect emerging epidemics, misallocate vaccines or countermeasures, or communicate inaccurate risk assessments, worsening the impact of biological threats. An adversary that times such attacks during a pandemic or natural disaster could amplify public fear, fuel conspiracy theories, and provoke protests against perceived mismanagement or cover-ups. In geopolitical terms, a nation that cannot guarantee the functioning of its healthcare system is less able to endure prolonged crises or conflicts, as its population becomes more vulnerable, its workforce less productive, and its government more exposed to domestic and international criticism.

3.2.1 Public Health Infrastructure

Critical to a Nation’s Functioning

Public health infrastructure, comprising surveillance systems, laboratories, immunization programs, and community health services, acts as the nervous system of a nation’s health defenses. It detects emerging threats, coordinates preventive measures, and orchestrates responses that protect entire populations rather than individual patients. This infrastructure is crucial for controlling communicable diseases, managing environmental health risks, and implementing large-scale interventions such as vaccination campaigns and health education initiatives. When functioning well, public health systems can prevent outbreaks from escalating into epidemics and epidemics from developing into pandemics, thereby avoiding substantial human and economic costs. They also provide the data and analysis that inform policy decisions on a range of issues, including food safety, air quality, and occupational health. If public health infrastructure is weakened or disrupted, the state loses its ability to see and shape the health status of the population, leaving it reactive instead of proactive in the face of threats. In the long term, this undermines life expectancy, productivity, and the sense of security citizens feel regarding their own and their families’ well-being.

Key Elements (Physical and Digital)

Public health infrastructure combines labs and field teams with large-scale data systems and communication channels to track and manage health risks. These components must be coordinated across local, regional, and national levels.

Physical infrastructure (Public Health)

- **Reference and regional laboratories** Offer Facilities for microbiology, virology, toxicology, and environmental testing, including high-containment laboratories.
- **Vaccination and campaign infrastructure**, Storage facilities and cold chain equipment, vaccination centers, mobile clinics, and outreach points.
- **Field investigation and response teams**, Epidemiological field units, contact tracers, community health workers, and logistics capabilities for deploying them.
- **Public health offices and coordination centers**, National and regional centers for disease control, emergency operations rooms, and training facilities.
- **Environmental and vector control assets**: Equipment for monitoring water and air quality, vector control (e.g., mosquito spraying), and sanitation interventions.

Digital infrastructure (Public Health)

- **Surveillance systems and databases**: Electronic disease surveillance platforms, case reporting systems, syndromic surveillance, and immunization registries.
  Data integration and analytics: Data warehouses, statistical analysis tools, modeling platforms, and dashboards for decision-makers.
  Laboratory information systems: Systems for managing test requests, results, sample tracking, and lab workflows, often integrated with national databases.
- **Communication and alerting platforms**, including systems for issuing health advisories to clinicians, the public, and international partners, such as web portals and mass notification tools.
- **Interoperability interfaces**, including APIs and data exchange services, link hospitals, clinics, labs, and government agencies, sometimes facilitating cross-border information sharing.

Cyber-Physical Vulnerabilities

Technical vulnerabilities

Public health information systems often evolve incrementally over many years, resulting in heterogeneous, sometimes poorly integrated platforms that are hard to secure uniformly. Legacy surveillance databases may lack robust access controls or encryption, making sensitive health data vulnerable to unauthorized access or tampering. Interfaces between hospital systems, laboratory information systems, and national surveillance platforms may rely on insecure protocols or custom integrations that are not regularly updated or tested. Poor input validation or weak authentication in web-based reporting portals can allow attackers to inject false data, exfiltrate records, or disrupt reporting flows. Analytical tools and dashboards may be hosted on shared infrastructure or cloud environments, where misconfiguration can expose data publicly. Because public health agencies often operate under tight budgets, they may struggle to maintain dedicated cybersecurity teams, leaving vulnerabilities undiscovered or unpatched.

Infrastructure and systemic vulnerabilities

Systemically, public health infrastructure is vulnerable because it depends on timely and accurate data flows from a multitude of sources that may have varying capabilities and incentives. Rural clinics or under-resourced facilities may lack reliable connectivity or secure systems, creating blind spots and delays that adversaries could exploit by targeting weaker nodes. Centralized national databases and coordination centers are critical hubs; if they are taken offline or their data is corrupted, the entire surveillance network may be effectively blinded. Laboratory networks rely on cold chains and logistics for sample transportation; disruptions to these physical processes, whether caused by cyberattacks on logistics companies or sabotage of storage facilities, can delay or invalidate testing. International reporting obligations, such as those under global health regulations, create additional dependencies on cross-border data sharing systems that may be targeted to sow geopolitical distrust. In emergencies, rapid scaling of systems, such as setting up new testing sites or contact tracing platforms, can introduce hastily deployed infrastructure with weak security controls, increasing systemic exposure.

Human factor vulnerabilities

Human factors in public health institutions range from data entry errors to political pressures that influence how information is interpreted and communicated. Field staff and local healthcare providers may lack training in secure data handling, resulting in the use of weak passwords, the use of personal devices for official communication, or the improper sharing of patient information via unsecured channels. Analysts and epidemiologists, though experts in their respective domains, may not be fully aware of cyber risks; they might take data at face value and overlook anomalies that suggest manipulation or exfiltration.

Leadership may face conflicting incentives, such as a desire to avoid panic or economic disruption, which can delay or distort public communications about emerging threats, making it harder to correct misinformation if systems are compromised. Social engineering targeting public health officials through fake emails, phone calls, or messages that appear to come from international organizations can lead to the disclosure of credentials or acceptance of malicious files. During crises, the pressure to move quickly may cause agencies to bypass security reviews for new tools, accept insecure cloud services, or share data more broadly than intended, all of which increase risk.

Impact on National Security

Attacks on public health infrastructure can compromise or eliminate a nation's ability to detect and respond to biological threats, transforming manageable events into full-scale crises. If surveillance data is manipulated, authorities may underestimate or overestimate the spread and severity of diseases, leading to inappropriate measures, either excessive restrictions that damage the economy and civil liberties or insufficient interventions that allow uncontrolled transmission.

Compromised laboratory systems may produce delayed or inaccurate test results, eroding public trust in health authorities and encouraging people to seek unverified alternatives or disregard guidance. Disruptions to vaccination registries and cold chains can derail immunization campaigns, potentially reviving controlled diseases or undermining herd immunity, with long-term health and economic costs. Adversaries could exploit such attacks to spread disinformation, amplifying conspiracy theories that vaccines are unsafe or that the government is concealing the truth, thereby deepening social divisions and weakening institutional legitimacy. In extreme cases, attackers may coordinate cyber operations against public health systems, potentially releasing biological agents, which could significantly increase casualties and complicate attribution. From a security perspective, a state that cannot reliably monitor and manage health threats is more vulnerable to coercion, less able to participate in international crisis management, and at greater risk of internal unrest driven by fear, unequal health impacts, and perceived governmental failure.

3.3 Financial

3.3.1 Banking Infrastructure

Critical to a Nation's Functioning

The banking infrastructure, encompassing commercial and retail banks, credit institutions, and their supporting systems, forms the backbone of credit creation, savings, and transaction services within an economy. Banks transform deposits into loans, allocate capital to productive activities, and provide liquidity that allows businesses to grow and households to invest in housing, education, and consumption. They also serve as the primary interface through which individuals and firms interact with the broader financial system, including payment networks and capital markets. If banking infrastructure is impaired, credit flows may seize up, investment may stall, and everyday transactions may become difficult or impossible, quickly affecting consumption and employment.

Banks also play a crucial role in implementing monetary policy, managing government debt, and enforcing financial crime controls, thus contributing directly to macroeconomic stability and national security. Because trust is the foundation of banking, any doubt about the safety of deposits or the integrity of systems can trigger runs and contagion across institutions. For these reasons, a resilient and secure banking infrastructure is indispensable to the smooth functioning of a nation's economy and to public confidence in the financial system.

Key Elements (Physical and Digital)

Banking infrastructure encompasses physical branches and cash services; however, in modern systems, the heart of banking lies in highly automated digital platforms that must operate with extreme reliability and security.

Physical infrastructure (Banking)

- **Branches and service points**: Retail bank branches, business centers, and customer service offices.
- **ATMs and cash infrastructure**. Cash machines, cash centers, vaults, and armored cars are used to distribute currency.
  Operations centers, Back-office processing facilities for payments, loan servicing, and reconciliation.
  Data centers and disaster recovery sites, Facilities hosting core banking systems and backup infrastructure.
- **Physical security**: Safes, vaults, secure rooms, surveillance, and access control for sensitive areas.

Digital infrastructure (Banking)

- **Core banking platforms**, Systems for accounts, deposits, loans, interest calculation, and general ledger.
  Customer channels: Online banking portals, mobile apps, telephone banking, ATM networks, and chatbots.
- **Risk and compliance systems**, Credit risk engines, AML and know-your-customer (KYC) systems, fraud monitoring tools.
  Internal IT services: Email, collaboration tools, HR systems, document management, and workflow automation.
  Connectivity and integration APIs, messaging systems (e.g., SWIFT), connections to payment systems, regulators, and third-party service providers.

Cyber-Physical Vulnerabilities

The sector (including banking, market operations $ exchanges, and Payment & Settlement Networks) is exposed to multiple vulnerabilities and attack risks, including technical, infrastructural, and human factors (Figure 5).

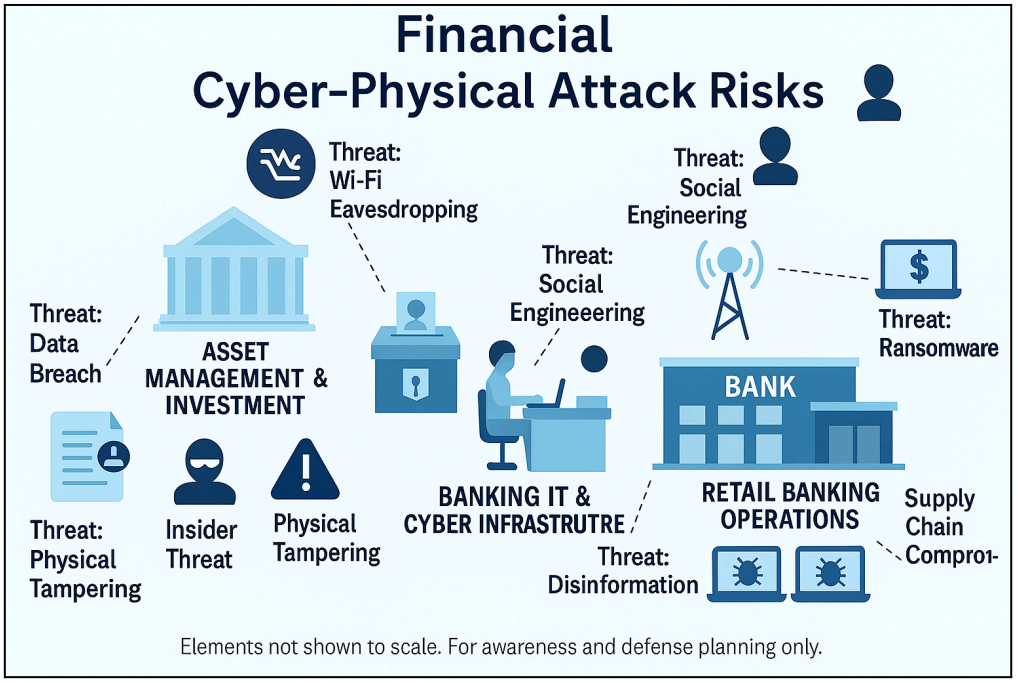


Figure 5 - Main cyber-physical attack risks against the financial sector

Technical vulnerabilities

Banking systems are complex, tightly integrated, and subject to constant change as products and channels evolve, which frequently introduces technical vulnerabilities. Legacy core banking systems often utilize outdated programming languages and architectures, rendering them vulnerable to security breaches and reliant on small pools of specialized staff. Integration layers that connect these cores to modern digital channels can contain misconfigurations or unvalidated inputs that attackers exploit to bypass controls or extract data. Online and mobile banking channels are exposed to the public internet and must handle large volumes of untrusted input; any weaknesses in authentication, session handling, or API security can enable credential stuffing, account takeover, or transaction manipulation. Endpoint security is another challenge, as staff workstations and remote access tools can be compromised through phishing, malware, or vulnerable software, allowing attackers to gain a foothold within the bank's network. Cryptographic systems must be implemented and managed correctly; if key management processes are weak, attackers could decrypt sensitive data or forge transaction authorizations.

Infrastructure and systemic vulnerabilities

From an infrastructure perspective, banks depend heavily on their data centers and communication networks to maintain service continuity across branches and digital channels. Concentration of core systems in a few locations means that physical incidents (such as fires, floods, or power failures) or targeted attacks on these sites can significantly disrupt operations despite logical redundancy. Many banks share infrastructure, such as cloud services, third-party processors, or shared ATM networks, creating systemic dependencies that may not be fully visible. Outsourcing IT operations or development work to external vendors can reduce costs. Still, it introduces risks if those vendors do not meet the same security and resilience standards as the organization.

Internally, tight cost controls may limit investment in redundant systems, testing, and disaster recovery drills, resulting in unproven failover procedures that may not function effectively under real-world stress. At a sector level, correlated vulnerabilities, such as the widespread use of the same software stacks or security products, can allow a single exploit to impact multiple institutions simultaneously.

Human factor vulnerabilities

Human behavior in banks is shaped by a combination of strict regulatory requirements and commercial pressures, creating distinct patterns of vulnerability. Front-line staff and call centers may be tricked by social engineering into revealing customer information or performing unauthorized actions, especially if attackers impersonate senior managers or regulators. Relationship managers and back-office staff often have broad system access and may not be fully aware of the cyber risks associated with their privileges. Insider threats, whether malicious or negligent, pose a critical concern due to the potential for unauthorized transactions or data leaks. Personal financial pressures, job dissatisfaction, or external coercion can motivate insiders to abuse their access. Training programs may focus more on compliance checklists than on practical security behavior, leading to rote box-ticking rather than genuine vigilance. Senior management decisions about incentives can exacerbate risk if they reward rapid business growth or aggressive sales without adequately valuing control functions, potentially sidelining security objections. Under crisis conditions, such as sudden market stress or regulatory deadlines, staff may bypass segregation of duties or dual controls to “get things done,” inadvertently opening paths for fraud or external compromise.

Impact on National Security

Attacks on banking infrastructure can rapidly undermine public confidence in the financial system and destabilize the broader economy. Suppose customers cannot access their accounts, withdraw cash, or execute basic transactions. In that case, they may fear for the safety of their savings and rush to withdraw funds, potentially triggering bank runs that spread across institutions. Loss or corruption of account data would create uncertainty over balances and obligations, possibly forcing authorities to impose transaction limits or provide blanket guarantees that strain public finances. Prolonged disruption to lending and credit assessment processes would slow investment and consumption, leading to increased unemployment and reduced tax revenues, with subsequent knock-on effects on social stability. If adversaries manage to exfiltrate and leak sensitive financial data, they may use it for blackmail, political influence operations, or targeted economic sabotage. In an international context, visible instability in a nation’s banking sector can lead to downgrades by rating agencies, capital flight, and currency devaluation, weakening the state’s ability to fund its policies and defend its interests. Politically, a major banking crisis triggered or exacerbated by cyberattacks can fuel narratives of elite incompetence or corruption, potentially empowering extremist movements or destabilizing democratic institutions.

3.3.2 Market Operations and Exchanges

Critical to a Nation's Functioning

Market operations and exchanges, encompassing stock exchanges, bond markets, derivatives platforms, and related infrastructure, are vital for capital formation, price discovery, and risk management in a modern economy. They enable companies and governments to raise funds, allow investors to allocate capital efficiently, and provide mechanisms for hedging risks, such as interest rate, currency, or commodity price movements. Transparent and orderly markets generate signals that inform business decisions, economic policy, and household investment; disruptions or manipulation, however, can distort these signals and lead to the misallocation of resources. Because many institutional investors, pension funds, and insurers rely on market valuations to manage long-term obligations, the integrity and availability of exchange infrastructure are closely linked to financial stability and citizens' future incomes. Markets are also highly globalized; a failure in one major venue can have ripple effects across international portfolios and cross-listed securities. For these reasons, ensuring that trading and post-trade operations are secure and resilient is central to maintaining confidence in the financial system and, by extension, in the nation's economic prospects.

Key Elements (Physical and Digital)

Market operations depend on specialized physical venues and, increasingly, highly automated electronic platforms that execute and settle trades in fractions of a second.

Physical infrastructure (Markets & Exchanges)

- **Exchange data centers and co-location facilities**. Physical sites housing trading engines, market data servers, and co-located participant equipment.
- **Trading floors and offices**, Broker-dealer premises, proprietary trading rooms, and oversight centers for monitoring markets.
- **Clearing and settlement facilities**, Offices, and data centers of central counterparties (CCPs) and central securities depositories (CSDs).
- **Network and communication hubs**: Points where high-speed communication lines converge, including fiber landing sites and telecom exchanges.
- **Physical security and resilience**: Power and cooling systems, backup generators, fire suppression, and secure access controls for critical venues.

Digital infrastructure (Markets & Exchanges)

- **Trading platforms and matching engines**, Electronic order books, matching algorithms, and connectivity gateways for various asset classes.
- **Market data systems**, Real-time price feeds, reference data systems, indices, and analytics platforms are used by market participants.
  Clearing and settlement systems, Platforms for trade confirmation, netting, margin calculation, collateral management, and securities settlement.
- **Surveillance and regulatory systems**: Market surveillance tools, suspicious activity monitoring, and reporting systems for regulators and exchanges.
  Connectivity and APIs, including FIX gateways, proprietary APIs, colocation links, cross-connects, and VPNs, enable members to connect with trading and post-trade systems.

Cyber-Physical Vulnerabilities

Technical vulnerabilities

The technical landscape of modern exchanges is characterized by extreme performance requirements and complex software stacks, which can mask subtle vulnerabilities. Trading engines and connectivity gateways must process vast numbers of orders with minimal latency, which often encourages highly optimized and sometimes brittle code, where security may be underemphasized. Interface specifications, such as FIX or proprietary protocols, can expose parsing bugs and input validation flaws if implemented inconsistently, allowing attackers to exploit these vulnerabilities and cause denial-of-service attacks or manipulate orders. Market data systems are a critical dependency; if they are corrupted or delayed, participants may trade based on incorrect information, which can amplify volatility and create opportunities for fraud. Clearing and settlement platforms handle sensitive transactional data and margin calculations; weaknesses in access control or data integrity protections could enable unauthorized position changes, false collateral records, or systemic mispricing of risk. External connectivity via APIs and co-location can also introduce attack vectors if authentication and encryption are not adequately enforced. Furthermore, reliance on third-party software components and libraries, including low-level networking and time synchronization tools, means that supply chain vulnerabilities can have a disproportionately large impact.

Infrastructure and systemic vulnerabilities

Systemically, market infrastructure is prone to concentration risks because a small number of exchanges and CCPs dominate trading and clearing in many jurisdictions. If a major exchange suffers a cyber attack that halts trading, the loss of that venue's price signals can cause confusion, widen spreads, and disrupt hedging strategies across the market.

CCPs, which stand between buyers and sellers, are central nodes for managing counterparty risk; their disruption or compromise could undermine confidence in the

ability to manage defaults and settle trades safely. The physical co-location of critical systems in a limited number of data centers creates exposure to localized incidents such as fires, power failures, or targeted physical attacks, even if logical redundancy exists. Interconnected markets, including dark pools, alternative trading systems, and overseas exchanges, can rapidly propagate errors and disruptions through arbitrage and algorithmic trading, making it challenging to contain incidents. Dependencies on telecom infrastructure, GPS time synchronization, and cloud services add further layers of systemic risk; failure or manipulation of any of these can degrade market functioning. Because markets are closely tied to investor sentiment, even brief technical incidents can have lasting impacts on confidence and risk perception.

Human factor vulnerabilities

Human actors in market infrastructure include exchange staff, regulators, traders, and IT operators, all of whom can be sources of vulnerability. Complex trading systems and regulatory rules can lead to misunderstandings or misconfigurations, such as incorrect risk limits or surveillance thresholds, allowing abusive practices or runaway algorithms to operate unchecked. Staff may inadvertently introduce errors when deploying software updates or configuration changes, which can cause outages or data inconsistencies at critical times. Social engineering targeting exchange employees, brokers, or regulators, especially those with administrative access, can lead to credential theft and subsequent deep compromise of core systems. The culture of speed and innovation in trading firms may prioritize performance and new features over thorough security testing, with management sometimes underestimating the risks of cutting corners. Regulatory agencies may be under-resourced relative to the complexity of the systems they oversee, limiting their ability to identify systemic vulnerabilities and enforce robust controls. During turbulent market conditions, stress and time pressure can degrade judgment, increasing the likelihood of errors and making staff more susceptible to manipulative narratives or urgent but fraudulent instructions.

Impact on National Security

Cyber-physical attacks on market infrastructure can disrupt capital flows, distort price signals, and erode domestic and international confidence in the nation’s economy. If an exchange is forced to halt trading or clears incorrect trades due to compromised systems, investors may suffer unexpected losses, and legal disputes over transactions could proliferate. Prolonged outages or repeated incidents can drive trading activity to foreign venues, weakening the domestic market’s role and potentially shifting jobs and tax revenues abroad.

Manipulation of market data or trading systems may allow adversaries to engineer artificial volatility, profit from insider knowledge of upcoming outages, or damage

specific companies or sectors deemed strategic. If CCPs or CSDs are compromised, the integrity of securities ownership records and collateral positions could be called into question, threatening the functioning of repo markets, central bank operations, and the balance sheets of large financial institutions. A severe loss of confidence in domestic markets can contribute to capital flight, higher borrowing costs for the government and private sector, and downward pressure on the national currency. Politically, such disruptions are apparent and can be framed as evidence of state weakness or regulatory capture, fueling populist narratives and tensions between authorities, financial institutions, and the broader public.

3.3.3 Payment & Settlement Networks

Critical to a Nation's Functioning

Payment and settlement networks ranging from central bank real-time gross settlement systems to retail card schemes and instant payment services are the infrastructure that allows money to move reliably through the economy. They facilitate the payment of wages, taxes, social benefits, and commercial invoices, as well as the settlement of financial market transactions and interbank obligations. If these networks function smoothly, economic actors can transact with confidence, secure in the knowledge that funds will be transferred correctly and promptly. When they malfunction, even briefly, the impact is immediate: businesses cannot pay their suppliers, individuals cannot afford essentials, and financial institutions cannot settle positions, which can freeze credit and trigger liquidity crises. Because payment systems are often operated or overseen by central banks, they are deeply intertwined with the implementation of monetary policy and the maintenance of financial stability. Retail payment networks also shape everyday experiences, influencing public perceptions of modernity, security, and trust in the financial system. Consequently, the resilience and security of these networks are critical not just for economic efficiency but for the perceived reliability and authority of the state.

Key Elements (Physical and Digital)

Payment and settlement networks rely on high-availability data centers and communication lines, combined with specialized software and security controls capable of handling large transaction volumes.

Physical infrastructure (Payments & Settlement)

- **Central and commercial data centers**, Facilities hosting RTGS systems, ACH platforms, card processing systems, and instant payment engines.
- **Network and communication hubs**, Telecom infrastructure, dedicated lines, and hubs linking banks, processors, and merchants.

- **Card acceptance infrastructure** includes Point-of-Sale (POS) terminals, ATMs, cash deposit machines, and physical hardware security modules (HSMs).
- **Backup and disaster recovery sites**: Secondary facilities for failover and business continuity.
- **Physical security and support**, including Power, cooling, physical access control, and secure vaults for cryptographic hardware.

Digital infrastructure (Payments & Settlement)

- **RTGS and ACH systems** are Central bank or operator platforms for high-value and bulk payments between financial institutions.
  Card networks and switching systems, as well as Authorization, clearing, and settlement platforms for debit, credit, and prepaid cards.
- **Instant payment and mobile money platforms**, Real-time retail payment engines, mobile wallets, and peer-to-peer payment services.
- **Messaging and integration**: Utilizing SWIFT or ISO 20022 messaging, APIs that link banks, merchants, fintechs, and central infrastructures.
  Security and risk management systems, Cryptographic key management, fraud detection engines, AML tools, transaction monitoring and reconciliation systems.

Cyber-Physical Vulnerabilities

Technical vulnerabilities

Payment and settlement systems are highly automated and time-sensitive, making them vulnerable to even minor technical faults or malicious disruptions. Legacy RTGS or ACH systems may be built on older mainframe technologies that are robust but challenging to modify, resulting in lengthy patch cycles and difficulties in implementing modern security measures. Messaging interfaces, such as SWIFT or ISO 20022 gateways, can be exploited if endpoint security is weak, allowing attackers to submit fraudulent payment instructions that appear legitimate. Card processing systems must interact with a multitude of merchant terminals and acquiring banks; any weaknesses in protocol implementations, encryption configurations, or tokenization schemes can be used for skimming or transaction manipulation. Instant payment platforms, which are always on, must handle high volumes with low latency, leaving little room for manual verification; if fraud detection rules are incomplete or misconfigured, attackers can quickly move funds before detection. Poorly secured APIs and mobile payment applications can expose account credentials, tokens, or personal data, enabling account takeover and unauthorized payments.

Infrastructure and systemic vulnerabilities

Systemically, payment and settlement networks are vulnerable because of their centrality and the limited number of core platforms in operation. A failure or compromise of the central RTGS system can prevent banks from settling high-value transactions, undermining interbank trust and causing institutions to hoard liquidity, which can freeze credit markets. Major card schemes or processors represent single points of failure for retail payments; outages can leave consumers unable to pay at supermarkets, fuel stations, or pharmacies, causing public frustration and panic. The growing reliance on instant payments and mobile wallets, particularly in countries where cash usage has declined significantly, increases the potential societal impact of outages or cyberattacks.

Dependencies on telecom providers, cloud services, and cross-border links further complicate resilience planning, as disruptions in these external services can have immediate effects on payment flows. Because payment systems are tightly time-bound, for example, with end-of-day cutoffs for settlement delays or failures, they can create cascading backlogs that are difficult to clear, amplifying the impact of relatively short disruptions.

Human factor vulnerabilities

Human operators and users introduce vulnerabilities at multiple points in payment and settlement networks. Bank staff responsible for payment operations may be tricked by sophisticated phishing or social engineering into approving fraudulent transactions, especially when attackers impersonate senior executives or essential clients and create a sense of urgency.

Operational teams managing RTGS or card processing platforms may inadvertently misconfigure systems or apply incorrect patches, which can result in outages or security vulnerabilities. At the merchant level, staff may mishandle POS terminals or fall for scams that involve swapping devices or installing skimming hardware. End users, including consumers and small businesses, often use weak PINs, share credentials, or respond to fraudulent messages that lure them into authorizing payments to attackers. Training on secure behavior may be infrequent or poorly tailored, leading to persistent risky practices. At a strategic level, decision-makers might prioritize cost efficiency over redundancy and security, reducing investment in backup systems, fraud analytics, and incident response capabilities, thereby increasing the potential impact of human mistakes when incidents occur.

Impact on National Security

A successful cyber-physical attack on payment and settlement networks can produce immediate, obvious disruptions that affect virtually every citizen and business, quickly becoming a national security concern. Suppose wages, pensions, and social benefits cannot be paid on time. In such cases, vulnerable populations may be unable to purchase food, medicine, and other essential items, thereby increasing social tension and undermining trust in the government. Widespread failures of card payments or mobile wallets at retail outlets can trigger panic buying, hoarding, or unrest, particularly if the public fears that the disruption is long-lasting or indicative of deeper financial system problems. In the interbank sphere, inability to settle high-value payments can lead to liquidity shortages, forcing central banks to provide emergency support and raising fears about the solvency of institutions. An adversary who combines technical attacks with disinformation campaigns suggesting, for example, that certain banks or the national currency are collapsing can amplify the psychological impact, encouraging runs and capital flight.

Such events may strain relations with trading partners, complicate international trade settlements, and weaken the country's position in global financial negotiations. Ultimately, sustained or repeated disruptions to payment systems can erode confidence in both the financial system and the state's capacity to protect its citizens' economic security, potentially fueling protests, political instability, and demands for radical policy changes.

3.4 Transportation

3.4.1 Air Transport: Airports and Aircraft Systems

Critical to a Nation's Functioning

Air transport is a fundamental pillar of national mobility, economic vitality, and international connectivity. Airports and aircraft systems enable the rapid movement of people, goods, medical supplies, and high-value cargo across vast distances, forming the logistical backbone of tourism, trade, diplomatic engagement, and emergency response. A nation's integration into the global economy depends heavily on reliable air corridors, safe air traffic management, and continuous availability of airport infrastructure. When air transport is disrupted, industries such as tourism, manufacturing, and global supply chains experience immediate strain, as just-in-time deliveries break down and inventory buffers evaporate. Airports also serve as emergency hubs during disasters, pandemics, and humanitarian crises, enabling evacuation, medical flights, and the rapid deployment of aid. Because aviation is highly regulated and safety-critical, public trust is essential; even minor incidents can cause widespread fear and political pressure.

A functional air transport system, therefore strengthens national competitiveness, ensures strategic mobility for leaders and armed forces, and cements the country's role in international diplomacy and trade. A failure in aviation infrastructure quickly cascades into economic losses, reputational damage, and erosion of public confidence in national governance.

Key Elements (Physical and Digital)

Air transport relies on a dense ecosystem of infrastructure, equipment, and digital systems that must work together flawlessly to ensure safe and efficient operations.

Physical Infrastructure (Air Transport)

- **Airports and terminals**, Runways, taxiways, aprons, passenger terminals, gates, cargo terminals, baggage systems, fuel farms, and fire-rescue services.
- **Air traffic control (ATC) facilities** include Control towers, approach control centers, area control centers, navigation beacons, and radio communication systems.
- **Aircraft and onboard equipment**: Airframes, engines, avionics, flight control systems, cabin systems, and communications equipment.
- **Ground support equipment (GSE)**: Tugs, jet bridges, de-icing trucks, refueling systems, loaders, and maintenance tools.
  Security and access systems: Perimeter fencing, surveillance cameras, passenger screening equipment, biometric access control, and internal security checkpoints.

Digital Infrastructure (Air Transport)

- **Air traffic management (ATM) systems** include Radar, ADS-B, multilateration, flight data processing systems, and ATC communication networks.
- **Aircraft digital systems** include Flight management systems (FMS), navigation databases, data link communications, aircraft health monitoring systems, and EFB tablets.
  Airport IT systems include Departure control systems, baggage handling software, airport operational databases, gate management systems, and passenger information platforms.
  Security and screening technologies: Biometric systems, API/PNR databases, automated border control, and cybersecurity monitoring tools.
- **Operational communications**: Ground-air data links, radio frequency networks, private aviation networks, SATCOM systems, and maintenance IT systems.

Cyber-Physical Vulnerabilities

The sector is vulnerable to multiple risks, including technical, infrastructural, and human factors (Figure 6).



Figure 6 - Main cyber-physical attack risks against the aviation and airport sector

Technical Vulnerabilities

Aviation faces a complex mix of legacy systems and modern digital technologies, making technical vulnerabilities particularly challenging to address. Many ATC systems were designed decades ago with minimal security, relying on assumed isolation rather than encryption or authentication. Protocols such as ADS-B broadcast unencrypted positional data, allowing attackers to spoof aircraft or inject false signals. Airports and airlines deploy heterogeneous IT systems with varying maintenance cycles; outdated servers, unpatched vulnerabilities, and misconfigured network segmentation can give attackers access to critical operational platforms. Aircraft increasingly rely on electronic flight bags, wireless maintenance connections, and onboard data networks; any compromise of these interfaces may provide opportunities to manipulate navigation databases, flight plans, or maintenance logs. Baggage systems, ticketing platforms, and passenger data systems are often interconnected with external partners, creating large attack surfaces where a single compromised vendor can propagate malware across multiple airports.

Infrastructure and Systemic Vulnerabilities

Air transport infrastructure is geographically concentrated and extremely sensitive to disruptions. Airports, unlike roads or ports, offer few practical alternatives; if runways are disabled by cyber-physical sabotage or operational IT systems fail, all flights must be canceled. ATC centers represent single points of failure: if a primary ATC site is taken offline by ransomware, fire, or data corruption, entire national airspaces may be forced to shut down. Fuel farms and refueling systems rely on automated valves and sensors; interference with these systems can disrupt airport operations or pose safety hazards.

Aircraft maintenance systems, which are increasingly digitized, depend on reliable access to digital manuals, maintenance schedules, and diagnostic data; if corrupted, an aircraft may be grounded for safety reasons. The heavy interdependence between airlines, airports, regulators, ground handlers, and weather systems amplifies cascading risk: a failure in one platform quickly disrupts others.

Human Factor Vulnerabilities

In aviation, human vulnerabilities arise from high-workload environments, complex procedures, and the need for intensive coordination among multiple actors. ATC operators and pilots work under constant pressure and may be more susceptible to phishing attacks, rushed decision-making, or accidental misuse of systems. Ground personnel often use shared devices or login terminals that, if left unlocked, can be exploited for unauthorized access. Maintenance workers may use USB devices, diagnostic tools, or laptops that bridge secure and insecure networks, creating pathways for malware to infiltrate these networks. Contractors frequently involved in baggage handling, catering, cleaning, and IT support often have wide physical access but usually lack adequate cybersecurity training. Leadership may underestimate cyber risks due to the sector’s strong historical emphasis on physical safety, leading to outdated security protocols and inadequate investment in digital resilience.

Impact on National Security

A cyber-physical attack on the aviation sector can produce immediate and obvious effects with long-lasting national security consequences. Disruption of ATC systems could force nationwide ground stops, stranding thousands of travelers, blocking cargo shipments, and halting medical or military flights. Manipulation of aircraft navigation data or onboard systems, while extremely difficult due to layered protections, could endanger lives and shake public trust in aviation safety. A sustained airport shutdown would paralyze tourism, trade, and essential supply chains, especially for time-sensitive goods such as vaccines, electronics, or perishables.

If an adversary uses cyber attacks to disrupt border control systems, passport checks, or biometric screening, national borders could temporarily lose integrity, complicating immigration control and enabling illicit movements. In extreme cases, coordinated cyber and physical attacks on airport infrastructure could trigger panic, lead to evacuations, and overwhelm emergency services, resulting in political pressure, diplomatic fallout, and calls for military escalation. Aviation's symbolic importance makes it an attractive target; any perception of insecurity can damage the nation's international image and economic attractiveness.

3.4.2 Railways

3.4.2.1 Rail and Subway Networks

Critical to a Nation's Functioning

Rail and subway networks are crucial to national mobility, facilitating efficient and high-volume transportation of passengers and freight across urban, regional, and intercity corridors. Rail systems support daily commuting for millions of workers, reducing road congestion and connecting residential areas with business centers, industrial zones, and educational hubs. Freight rail is vital for moving minerals, agricultural products, fuel, chemicals, and heavy goods that are difficult or uneconomical to transport by road. During crises, railways serve as logistical backbones for emergency supplies, evacuation operations, and military movements. Subway systems are indispensable in large cities, where urban mobility would collapse without their capacity. A failure in rail transport would immediately affect productivity, supply chains, and emergency readiness; as trains stop, economic activity slows, and pressure on roads increases, leading to accidents, delays, and environmental impact. The sector's smooth functioning is therefore crucial for national resilience, social stability, and economic competitiveness.

Key Elements (Physical and Digital)

Physical Infrastructure (Rail & Subway)

- **Rail tracks and tunnels**. Tracks, ballast, sleepers, tunnels, bridges, switches, and crossings.
  Stations and platforms: Passenger stations, ticket halls, ticketing machines, access gates, escalators, elevators, and ventilation systems.
- **Rolling stock**: Locomotives, passenger trains, freight wagons, subway cars, braking systems, and communication modules.
  Signaling and interlockings: Trackside signals, relay rooms, interlocking cabinets, and track circuits.
  Maintenance and storage depots, Workshops, fueling stations, stabling yards, and spare parts facilities.

Digital Infrastructure (Rail & Subway)

- **Train control systems**: Automatic train control (ATC), train protection systems, CBTC (communications-based train control), ERTMS/ETCS systems.
- **Rail operation centers**, Dispatch centers, traffic management systems, SCADA for power and ventilation, and real-time monitoring.
- **Passenger information and ticketing**: Ticketing databases, innovative card systems, contactless payment systems, passenger display boards, and mobile apps.
- **IoT and sensor systems** Condition monitoring sensors, predictive maintenance systems, trackside IoT devices, and remote diagnostics.
- **Communications networks** include GSM-R, LTE-R, fiber optics, radio communications, and secure internal networks.

Cyber-Physical Vulnerabilities

The sector is exposed to multiple vulnerabilities and attack risks, including technical, infrastructural, and human factors (Figure 7).

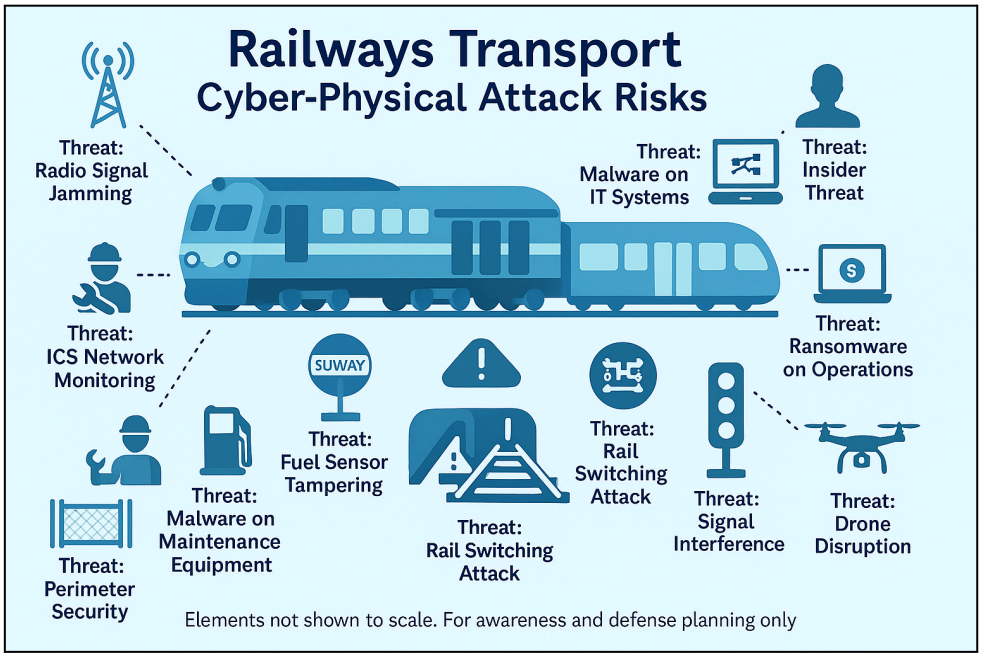


Figure 7 - Main cyber-physical attack risks against the railways sector

Technical Vulnerabilities

Rail and subway networks rely heavily on automated control systems that, if compromised, could disrupt safe operations. Legacy signaling equipment, such as relay-based interlockings, may lack authentication or encryption, allowing attackers to manipulate signals or switch positions if they gain network access. Modern CBTC and ERTMS systems, although more secure, rely on continuous wireless communication between the train and the track; jamming or spoofing these signals can cause delays or force emergency braking. SCADA systems controlling power distribution (for traction electricity) are often connected to corporate networks; malware infiltrating these systems can cause blackouts or stalled trains. Ticketing systems and passenger information platforms, if compromised, can lead to overcrowding, financial loss, and confusion. Vulnerabilities in predictive maintenance systems may allow attackers to manipulate condition data, resulting in premature failures or unsafe operation of rolling stock.

Infrastructure and Systemic Vulnerabilities

Rail networks span thousands of kilometers and include geographically dispersed assets that cannot be fully secured physically. Trackside cabinets, sensors, and signaling boxes may be vandalized or tampered with, and many are located in remote areas with minimal surveillance. Urban subway systems rely heavily on tunnel ventilation, lighting, and emergency systems; disruption of these via cyber-physical attacks could create dangerous conditions for passengers. Concentration of operations in a small number of rail control centers introduces systemic risk: if a control center is hit by ransomware, communication failure, or sabotage, the entire network could be unsafe to operate. Freight corridors carrying hazardous materials, fuel, chemicals, and explosives pose additional risks if attackers cause derailments or manipulate the route. Urban subways are especially sensitive to panic; disruptions can lead to overcrowding, stampedes, or accidents.

Human Factor Vulnerabilities

Human vulnerabilities stem from extensive coordination between conductors, dispatchers, maintenance crews, and contractors. Workers may use shared credentials, outdated laptops, or unsecured handheld devices when accessing rail control systems. Rail operators, under pressure to maintain schedules, may override alarms or disable safety procedures. Outsourced maintenance teams, particularly those for signaling and IT systems, may not adhere to strict cybersecurity standards. Social engineering attacks targeting dispatchers or IT staff can result in the acquisition of privileged credentials. In stressful conditions, such as peak hours, emergencies, or technical malfunctions human error becomes more likely, increasing opportunities for attackers to exploit confusion or insert malicious commands unnoticed. Leadership may focus heavily on physical safety while allocating insufficient resources to cybersecurity modernization.

Impact on National Security

A cyber-physical attack on a rail or subway network can severely disrupt national mobility and economic activity. Train collisions or derailments caused by compromised signaling systems could result in mass casualties and widespread fear, undermining trust in public transportation. Simultaneous shutdowns of stations or entire lines could paralyze major cities, preventing workers from reaching jobs and emergency services from moving efficiently. Freight disruptions could halt the movement of essential goods, fuel supplies, and industrial components, causing shortages and factory shutdowns. Attacks on subway ventilation or tunnel lighting systems could lead to life-threatening conditions during peak hours, prompting mass evacuations and potential riots. A targeted attack on trains carrying hazardous materials could have environmental and political repercussions.

In a geopolitical context, disabling rail networks limits military mobility, disrupts strategic logistics, and weakens national readiness. Public perception of insecurity in transportation can lead to social unrest, economic losses, and political instability.

3.4.3 Roads

3.4.3.1 Road Traffic Systems

Critical to a Nation's Functioning

Road networks are the most widely used and distributed transportation system, enabling mobility for individuals, goods, emergency services, and public transport. They connect urban, suburban, and rural regions, forming the backbone of national economic activity. Road traffic systems, including traffic lights, highway management centers, toll systems, and connected vehicle networks, ensure the smooth and safe operation of these vast networks. Disruption to road systems can lead to traffic congestion, accidents, delays in logistics, and the inability of emergency responders to reach critical sites. In cities, road transport is essential for day-to-day economic functioning; any prolonged failure can paralyze commerce, halt freight deliveries, disrupt food supply chains, and reduce worker productivity. Road networks also play a crucial role in disaster response, facilitating evacuation routes and the rapid movement of medical and security services. Because roads are ubiquitous and deeply integrated into public life, maintaining their functionality is crucial for national resilience, public safety, and societal stability.

Key Elements (Physical and Digital)

Physical Infrastructure (Road Systems)

- **Roadways and highways**: Roads, bridges, tunnels, overpasses, and underpasses.
- **Traffic control devices**: Traffic lights, signals, variable message signs, speed cameras, toll gates, and lane control systems.
  Vehicles: Private cars, buses, trucks, emergency vehicles, and connected/automated vehicles.
- **Roadside equipment**: Sensors, cameras, roadside cabinets, weather monitoring stations, and physical barriers.
- **Maintenance and support facilities**, Depots, garages, control centers, and highway patrol infrastructure.

Digital Infrastructure (Road Systems)

- **Traffic management centers (TMCs)**, Real-time monitoring systems, control dashboards, SCADA for lighting and tunnels.
- **Intelligent transportation systems (ITS)**, Vehicle detection sensors, automated incident detection, and intelligent traffic signaling algorithms.
- **Connected vehicle systems**, V2X communication networks, telematics platforms, GPS-based routing, and fleet management systems.
- **Toll collection systems**, Electronic tolling, ANPR systems, payment gateways, and enforcement databases.
  Public information systems: Traffic apps, congestion maps, digital signage, and emergency notification platforms.

Cyber-Physical Vulnerabilities

The sector is vulnerable to multiple risks, including technical, infrastructural, and human factors (Figure 8).

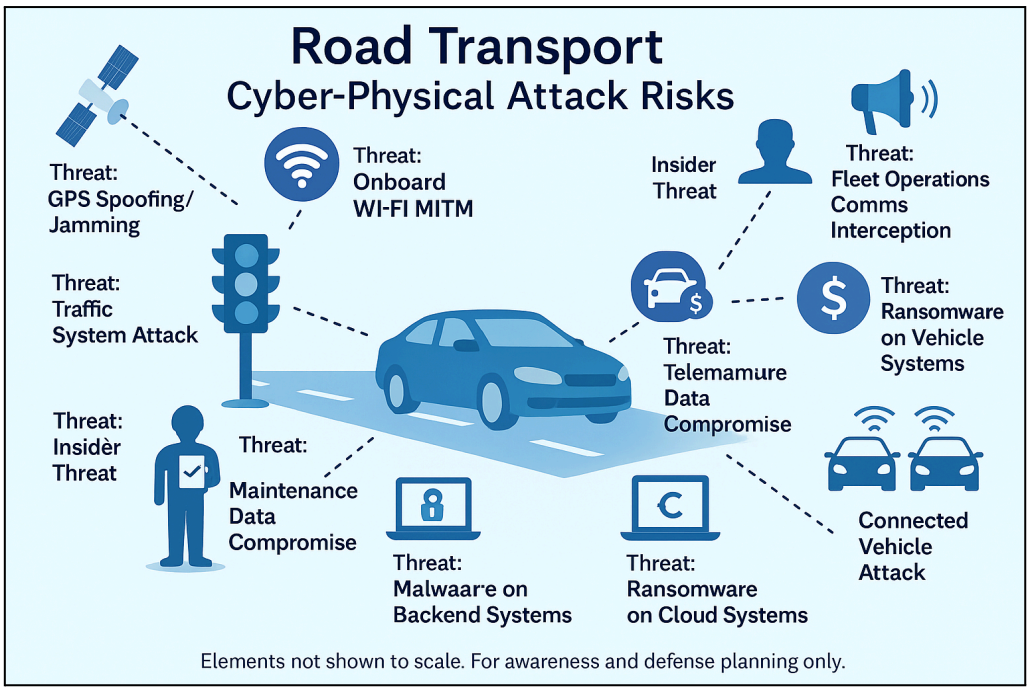


Figure 8 - Main cyber-physical attack risks against the road transport industry

Technical Vulnerabilities

Road traffic systems contain many legacy components that were not designed with cybersecurity in mind. Traffic lights, roadside sensors, and variable message signs often rely on outdated firmware, weak authentication, and unencrypted communications, enabling attackers to manipulate traffic flows. SCADA systems controlling tunnel ventilation or highway lighting may be reachable from corporate networks or remote maintenance links. Toll systems and ANPR databases can be targeted to alter vehicle records, disable toll collection, or track individuals. Connected vehicle systems introduce new vulnerabilities: compromised V2X messages could cause accidents, traffic disruptions, or unauthorized tracking of vehicles. Navigation systems and fleet management platforms are vulnerable to spoofing or data manipulation, which can lead to confusion, delays, or safety risks. Cyber attacks on routing algorithms may trigger artificial congestion or misdirect emergency vehicles.

Infrastructure and Systemic Vulnerabilities

Because road systems are geographically dispersed, physical security is often weak. Roadside cabinets housing signaling equipment may be exposed, unmonitored, and vulnerable to tampering. Bridges and tunnels heavily rely on digital control systems for lighting, ventilation, and emergency management; disruptions could lead to safety hazards, smoke buildup, or blocked escape routes during incidents.

Traffic management centers represent critical hubs; shutting them down through ransomware or sabotage can make regulators blind to real-time conditions, preventing coordinated response to accidents or emergencies. Freight corridors rely on road networks; disruptions can halt food deliveries, fuel shipments, and industrial supply chains. During natural disasters or emergencies, road systems must function as evacuation routes; any interference can dramatically worsen casualties.

Human Factor Vulnerabilities

Road traffic management staff may lack cybersecurity training, relying heavily on outdated procedures or shared accounts. Maintenance technicians often connect laptops directly to roadside equipment, creating a bridge between secure and insecure networks. Human error in configuring traffic signaling algorithms or incident response systems can significantly amplify the impact of cyberattacks. Contracted workers or private companies operating toll booths, cameras, or traffic systems may use weak access controls or insufficient security practices. Drivers, especially in connected vehicles, may fall victim to social engineering or install malicious apps that compromise navigation or telematics systems. Leadership may underestimate the cyber threats to road systems because they are traditionally viewed as physical infrastructure, rather than digital systems, resulting in underinvestment in resilience.

Impact on National Security

Cyber-physical attacks on road systems can trigger widespread societal disruption. Manipulated traffic lights could cause gridlock across major cities, hampering emergency response and paralyzing economic activity. Disruption of toll systems could cause financial losses, congestion, and public anger. Attacks on connected vehicle systems may cause accidents, injuries, or mass panic, particularly if multiple vehicles malfunction simultaneously. Highway tunnel failures, such as disabled ventilation, can cause hazardous smoke buildup during incidents, leading to casualties and chaotic evacuations. If freight transport is disrupted, food shortages, fuel shortages, and industrial shutdowns could occur within days. Large-scale road paralysis may provoke public frustration, protests, or loss of confidence in government capabilities, especially if attackers spread disinformation about the causes of the disruptions. During conflict, disruptions to the road system can hamper military logistics, reduce the mobility of security services, and weaken national defense readiness.

3.4.4 Maritime Transport

3.4.4.1 Seaports & Terminals

Critical to a Nation's Functioning

Seaports and maritime terminals are essential gateways for global trade, handling a large percentage of a nation's imports and exports, often exceeding 80% in many countries. Ports enable the movement of containers, bulk commodities, energy supplies, vehicles, and industrial equipment. Their continuous operation ensures that supply chains remain stable, prices remain predictable, and essential goods, such as food, medicine, and fuel, are readily available. Ports also support economic clusters, including logistics companies, shipyards, customs authorities, and industrial zones. A disruption to port operations would immediately impact the availability of consumer goods, manufacturing inputs, and energy resources, potentially causing shortages and inflation. Ports also support military deployment and naval logistics, making them critical for defense and national security. Their strategic location and economic importance make them high-value targets; maintaining their functionality is essential for geopolitical influence, financial resilience, and public welfare.

Key Elements (Physical and Digital)

Physical Infrastructure (Ports)

- **Terminals and berths**: Container terminals, bulk terminals, vehicle terminals, cranes, and mooring equipment.
- **Cargo handling equipment**: Ship-to-shore cranes, RTGs, straddle carriers, reach stackers, forklifts.
- **Port logistics infrastructure** includes warehouses, container yards, cold storage facilities, fuel bunkering systems, and pipelines.
- **Vessels and tugboats**, Pilots, tugboats, service vessels, and port authority fleets.
- **Security systems**: Access control, surveillance cameras, perimeter fencing, and customs inspection equipment.

Digital Infrastructure (Ports)

- **Terminal operating systems (TOS)** Systems for scheduling, crane control, yard planning, and container tracking.
  Port community systems (PCS) platforms link customs, shipping lines, freight forwarders, and authorities.
- **SCADA for port utilities** Systems controlling electricity, water supply, and fuel operations.
  Navigation and maritime systems: Radar, AIS, vessel traffic services (VTS), port call management systems.

- **Cybersecurity and access systems**, Identity management, surveillance analytics, and secure communication networks.

Cyber-Physical Vulnerabilities

The sector is vulnerable to multiple risks, including technical, infrastructural, and human factors (Figure 9).

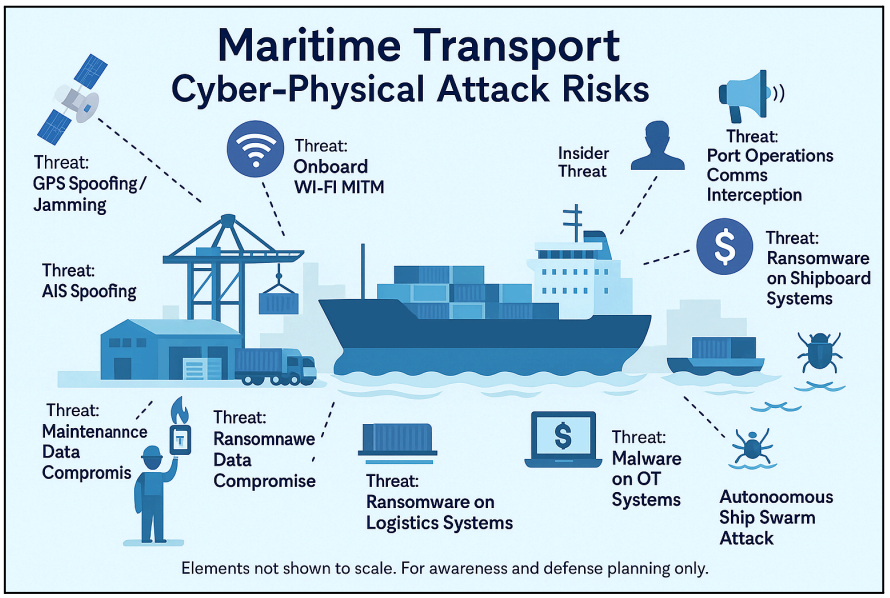


Figure 9 - Main cyber-physical attack risks against the maritime transport sector

Technical Vulnerabilities

Ports rely heavily on automated systems for crane operations, container routing, and customs data processing. TOS platforms often include outdated components, weak access controls, or insecure third-party integrations. Malware infiltrating these systems can stop crane operations, scramble container assignments, or corrupt customs records. SCADA systems controlling port utilities may expose unpatched weaknesses, allowing attackers to disrupt power or water supplies. Navigation systems, such as AIS, are inherently vulnerable to spoofing, allowing adversaries to create ghost ships, manipulate vessel positions, or deceive VTS operators. Port community systems, which connect multiple stakeholders, create a wide attack surface; compromise of one shipping line or freight forwarder can cascade into the entire port ecosystem.

Infrastructure and Systemic Vulnerabilities

Ports are vast and physically exposed, with multiple access routes and high reliance on contractors. Physical sabotage combined with cyber attacks could disable cranes or fuel systems. Because ports handle vast volumes of goods, even small disruptions can create days-long backlogs. Critical dependencies such as electricity, telecommunications, and road access create systemic fragility. A sustained outage of port IT systems can halt customs clearance, trapping cargo and causing nationwide supply chain disruptions. The port ecosystem depends heavily on global shipping schedules; an attack on one port can ripple across maritime routes, creating international knock-on effects.

Human Factor Vulnerabilities

Human vulnerabilities stem from the need for multi-organizational coordination and diverse security cultures. Dock workers, crane operators, customs officers, and IT staff may have varying levels of cybersecurity awareness. Contractors often access port networks using shared credentials or unsecured devices. Social engineering against freight forwarders or shipping agents can yield sensitive information or facilitate fraudulent cargo routing. High operational pressure may lead workers to bypass procedures, ignore alarms, or misuse access controls. Port leadership may prioritize operational continuity and throughput over cyber hygiene, delaying critical updates or incident rehearsals.

Impact on National Security

A cyber-physical attack on a port can cripple national supply chains. Shutting down crane systems or customs platforms can halt container movements, causing shortages of food, medicine, and industrial goods. Disruption of fuel terminals can impair national energy availability. Manipulation of navigation systems may cause accidents, collisions, or blocked waterways, disrupting not only trade but also naval operations. Economic losses can escalate rapidly as factories halt production and exporters miss shipping windows. Public frustration may rise as consumer goods become scarce and transport costs increase. A nation’s global reputation may be damaged if its ports are perceived as insecure or unreliable, which can affect foreign investment. In wartime or geopolitical conflict, port disruptions weaken naval readiness, hinder troop movements, and constrict defense logistics, undermining national sovereignty and strategic autonomy.

3.4.4.2 Ships and Maritime Navigation

Critical to a Nation's Functioning

Ships and maritime navigation systems facilitate the global flow of trade, ensuring the delivery of raw materials, energy, and manufactured goods. Tankers supply oil and gas; bulk carriers transport grain, coal, and fertilizers; container ships move electronics, clothing, pharmaceuticals, and industrial components. Without maritime transport, national economies would face immediate shortages and severe economic contraction. Ships are also vital for fisheries, offshore energy, naval operations, and coastal security. Navigation systems ensure safe passage through congested or hazardous waters; any failure can result in collisions, grounding, or environmental disasters. Because the maritime sector connects international trade routes, disruptions have global ripple effects, influencing food security, inflation, and diplomatic relations. Maintaining safe and functional maritime navigation is therefore crucial for maintaining economic stability, protecting the environment, and ensuring national sovereignty.

Key Elements (Physical and Digital)

Physical Infrastructure (Ships & Navigation)

- **Vessels:** Container ships, tankers, bulk carriers, ferries, fishing vessels, and naval ships.
- **Navigation equipment includes Radar, gyrocompass, autopilot, ECDIS systems, and GPS** receivers.
- **Mechanical system:** Engines, propulsion systems, steering gear, fuel systems.
- **Cargo handling systems**, Pumps, cranes, hatches, ballast systems, refrigeration units. **Crew and onboard facilities** include the Bridge, engine room, accommodation areas, and communications equipment.

Digital Infrastructure (Ships & Navigation)

- **ECDIS and navigation systems**, Electronic charts, route planning software, AIS, and marine VHF systems.
  Engine and machinery control systems, PLCs for engine monitoring, engine automation, and steering systems.
- **Shipboard networks**, Wi-Fi, crew networks, satellite links, WAN/LAN connectivity, and remote monitoring.
- **Fleet management systems**, tracking dashboards, fuel optimization tools, and cargo documentation systems.
- **Cybersecurity and communication systems**: Firewalls, secure satellite communications, and encryption tools.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Modern ships rely heavily on digital navigation systems that are vulnerable to manipulation. GPS spoofing can mislead vessels about their true position, risking grounding or territorial violations. ECDIS systems may run outdated operating systems and accept unverified chart updates, which can allow attackers to alter routes or conceal hazards. Engine control systems, if accessed through compromised networks, could be manipulated to disrupt propulsion, steering, or fuel management. Satellite communications, often used for remote monitoring, may be weakly secured, allowing for the interception or injection of malicious commands. Malware spreading through USB drives or laptops used by crew or contractors can infect bridge systems or engine room controls.

Infrastructure and Systemic Vulnerabilities

Ships depend on global communication networks, navigation satellites, and port infrastructure. A disruption in satellite links can impair navigation, weather updates, and emergency communications. Large vessels require precise coordination when entering ports; manipulation of navigation or pilotage systems can cause collisions or block critical chokepoints. Fleet management systems centralize sensitive information about vessel movements; breaches could expose trade patterns, cargo manifests, or naval deployments. Maritime supply chains are long and complex; compromised documents or false cargo data can disrupt customs, insurance, and port operations. Physical access to ships in ports is relatively easy; insiders could install malicious devices, sabotage sensors, or disable alarms.

Human Factor Vulnerabilities

Crew members may have limited cybersecurity training and may unknowingly connect infected devices or download unsafe software. High crew turnover leads to inconsistent security practices. Contractors, such as maintenance technicians or IT specialists, often bring laptops aboard, creating potential infection vectors. Shore-side managers may rely on email for operational coordination, making them targets for phishing campaigns that enable attackers to impersonate legitimate authorities. Under stressful maritime conditions, such as storms, congested waters, or time pressure, a crew may overlook signs of cyber manipulation or ignore best practices. Leadership in shipping companies may prioritize operational efficiency over cybersecurity investment, considering cyber threats as rare or low-impact until an incident occurs.

Impact on National Security

Cyber-physical attacks on ships and maritime navigation can disrupt global supply chains, cause environmental disasters, and provoke international incidents. Grounding or disabling a major vessel in a strategic waterway can halt maritime traffic for days or weeks, affecting global trade and national economies. Manipulation of ship propulsion or steering systems can lead to collisions or oil spills, harming the environment and posing a threat to coastal populations. If naval ships are targeted, adversaries may gain intelligence on military movements or compromise national defense readiness. Disruption of cargo shipments such as energy carriers or food imports can trigger shortages, inflation, and public dissatisfaction. A coordinated attack on multiple ships could overwhelm coast guards and naval forces, creating widespread insecurity in territorial waters. The geopolitical implications are significant, as maritime disruptions can strain alliances, escalate regional tensions, and undermine a nation’s credibility in securing its naval domains.

3.5 Telecommunications

3.5.1 ISPs and Telecom Operators

Critical to a Nation’s Functioning

Telecommunications form the invisible nervous system of a modern nation, enabling communication, information exchange, economic activity, and governmental coordination. Internet service providers, fixed-line operators, and mobile networks support a wide range of applications, from financial transactions and emergency calls to industrial operations, public services, and diplomatic communications. National productivity depends on the availability and resilience of networks that ensure constant connectivity for businesses, hospitals, schools, and government institutions. In the digital age, the functioning of nearly every sector, including transportation, energy, defense, healthcare, and finance, relies on high-capacity communication infrastructure. This means that even short outages can cause cascading failures across the economy and society. During crises, governments rely on telecom networks to issue alerts, coordinate emergency services, and maintain situational awareness, making these systems indispensable for national stability. A robust telecom sector, therefore, ensures not only social cohesion and economic competitiveness but also strategic autonomy, as foreign dependency in critical communications can become a geopolitical vulnerability. Any compromise in this sector threatens the nation's core functioning.

Key Elements (Physical and Digital)

Physical Infrastructure (Telecom Operators & ISPs)

- **Fiber-optic backbone networks**, Intercity cables, long-haul fiber, submarine cables, metropolitan networks, and distribution points.
- **Mobile network infrastructure**: Base stations, 4G/5G towers, antennas, small cells, repeaters, and edge computing nodes.
  Core network facilities: Data centers, switching centers, network operation centers (NOCs), POPs, and server rooms.
  Passive infrastructure: Towers, ducts, poles, power systems, cooling systems, and physical shelters.
  International gateways, Landing stations for submarine cables, satellite earth stations, and border routing equipment.

Digital Infrastructure (Telecom Operators & ISPs)

- **Core network systems**: Routers, switches, DNS servers, BGP configurations, MPLS systems, and IP transit platforms.
- **Subscriber management systems**, HLR/HSS, AAA servers, SIM provisioning, billing systems, CRM databases.
- **Mobile communication protocols**, 4G/5G network slices, IMS systems, signaling protocols, VoLTE infrastructure.
- **Security and monitoring systems**, IDS/IPS, firewalls, DDoS mitigation tools, threat intelligence platforms.
  Cloud and virtualization layers, NFV, SDN controllers, virtual EPC/5GC components, and orchestration systems.

Cyber-Physical Vulnerabilities

The sector (including Telecoms, ISP, Satellite, and Data Centers) is exposed to multiple vulnerabilities and attack risks, including technical, infrastructural, and human factors (Figure 10).



Figure 10 - Main cyber-physical attack risks against the Telecommunications industry

Technical Vulnerabilities

Telecom operators face systemic technical risks due to the complexity and scale of their networks. Internet routing relies on BGP, a protocol that lacks authentication and is prone to hijacking; adversaries can reroute traffic through malicious nodes, enabling espionage or disruption. DNS infrastructure can be targeted to take down primary services or manipulate user traffic. 4G/5G networks introduce vast software-defined components such as virtualized core networks that expand the attack surface and expose new vulnerabilities in orchestration layers, APIs, and virtual network functions. Legacy systems and unpatched routers at customer premises serve as entry points for attackers, who can use them to launch DDoS attacks. Supply chain vulnerabilities also pose a significant threat, as telecom equipment depends on foreign manufacturers; compromised firmware or hidden backdoors could silently enable long-term espionage or remote manipulation of core systems.

Infrastructure and Systemic Vulnerabilities

The telecom sector is highly centralized, with key dependencies on data centers, international gateways, and network operation centers. A failure at one major core routing center can disrupt connectivity for entire regions. Submarine cable landing stations are single points of failure; physical sabotage or cyber manipulation at these sites can sever the country's connection to global internet traffic. Power dependencies are also critical: telecom towers and core sites require continuous electricity and backup systems; attacks targeting energy supply or backup generators can cripple connectivity. Towers and roadside cabinets are often poorly monitored and vulnerable to physical tampering.

The increasing use of 5G network slicing for critical services (e.g., emergency communications, IoT, autonomous vehicles) means that any slice malfunction or targeted attack could disrupt entire mission-critical applications.

Human Factor Vulnerabilities

Human vulnerabilities stem from the vast workforce required to build, maintain, and manage telecom systems. Field technicians often access sensitive sites with limited cybersecurity oversight, using laptops or diagnostic tools that may be vulnerable to compromise. Engineers managing routing protocols or network configurations can make mistakes that cause outages or inadvertently open vulnerabilities. Employees may fall victim to phishing attacks, which can grant unauthorized access to billing systems, customer databases, or core network tools. Contractors, especially those with physical access to towers or data centers, may bypass procedures or connect insecure devices. Leadership may underestimate cyber risks if telecom outages are infrequent, resulting in outdated security policies, delayed patching, or insufficient oversight of suppliers.

Impact on National Security

A cyber-physical attack on a telecom network can be catastrophic. A shutdown of mobile networks would disrupt emergency services, hinder law enforcement, and paralyze social communication, leading to confusion and panic. Manipulation of routing or DNS systems could isolate regions, disrupt government communication, or enable mass surveillance by adversaries. Attacks on submarine cables or international gateways could sever national infrastructure's connection to the global internet, freezing financial markets, halting international trade, and crippling cloud-based services. The dissemination of disinformation through compromised telecommunications channels could provoke riots, political instability, or social unrest. Disruption of 5G slices used for industrial automation could halt factories, disable autonomous vehicles, or interfere with healthcare IoT devices. In wartime, telecom degradation would weaken command and control for defense forces, limit intelligence gathering, and impede rapid mobilization, making the nation vulnerable to coordinated hostile actions.

3.5.2 Satellite Communications

Critical to a Nation's Functioning

Satellite communications (SATCOM) provide essential connectivity for remote regions, aviation, maritime transport, defense operations, and emergency services, making them indispensable for national resilience and strategic autonomy. Unlike terrestrial networks, satellites provide nationwide coverage, including areas without fiber or cellular infrastructure, supporting border surveillance, weather forecasting, disaster response, and military command and control networks. During natural disasters, when ground-based systems fail, SATCOM often becomes the primary means of maintaining communication between authorities and affected populations, enabling the coordination of rescue operations and the distribution of aid.

For the aviation and maritime sectors, satellites power navigation, safety messages, and real-time tracking, ensuring secure and efficient traffic flow. SATCOM also underpins financial networks, broadcast media, and governmental communication, including secure diplomatic channels. Because satellites operate beyond national borders, they form part of the strategic space domain; their disruption can weaken sovereignty, impede intelligence sharing, and expose the nation to geopolitical threats. In a digitally dependent world, the stable functioning of satellite communications is therefore critical for national continuity, economic stability, and defense capability.

Key Elements (Physical and Digital)

Physical Infrastructure (Satellite Communications)

- **Satellites in orbit**, GEO, MEO, LEO constellations for communication, positioning, and data relay.
  Ground stations and gateways, Earth stations, tracking antennas, uplink/downlink infrastructure, teleport facilities.
- **User terminals**: Maritime SATCOM terminals, aircraft SATCOM equipment, VSAT dishes, military field terminals.
  Space control facilities, Satellite operation centers, mission control centers, tracking and telemetry systems.
- **Supporting power and physical assets, including** cooling systems, backup generators, antenna towers, and physical shelters.

Digital Infrastructure (Satellite Communications)

- **Satellite communication protocols**, Uplink/downlink modulation, frequency allocation, and encryption systems.
- **Network management systems**, Telemetry processing, command systems, satellite health monitoring software.
- **Ground network integration**: Routing equipment, VPN tunnels, WAN optimization tools, and gateway servers.
  User access systems, Authentication servers, traffic management systems, and allocation platforms.
- **Cybersecurity systems** include RF monitoring, anomaly detection, encryption key management, firewalls, and intrusion monitoring.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Satellite networks face unique vulnerabilities due to their complex architecture and long operational lifespan. Many satellites rely on legacy operating systems and communication protocols that cannot be easily updated once in orbit. Weak encryption or outdated command systems can allow adversaries to intercept or manipulate satellite telemetry. Jamming and spoofing of satellite signals remain significant risks; attackers can disrupt GPS accuracy, interfere with SATCOM broadcasts, or degrade links used by aircraft and ships. Ground stations may expose unpatched interfaces, allowing intruders to interfere with tracking antennas or route malicious commands to satellites. SATCOM terminals, widely deployed in remote or unmonitored environments, often rely on default credentials, unencrypted communication channels, or insecure firmware, enabling attackers to gain unauthorized access. Supply-chain vulnerabilities also pose threats, as satellite components may contain compromised microchips or backdoors.

Infrastructure and Systemic Vulnerabilities

SATCOM systems rely on a small number of high-value assets, satellites, and ground stations that form single points of failure. Damage to even one primary satellite can degrade national coverage or disrupt specialized services such as military communications or maritime safety broadcasts. Ground stations are physically concentrated and often located in isolated areas, making them vulnerable to sabotage or natural disasters. Interdependence with terrestrial networks creates additional systemic risk: if satellite gateways or routing systems are compromised, attackers could reroute traffic or disable key links, thereby compromising the network's integrity.

Highly congested orbits increase the risk of collisions, which could trigger cascading space debris events that disable multiple satellites simultaneously. Because satellite constellations often rely on international cooperation, geopolitical tensions can limit access to key space infrastructure during crises.

Human Factor Vulnerabilities

Human vulnerabilities arise from highly specialized staff managing sensitive satellite operations. Engineers in mission control centers may use shared workstations or legacy software tools that lack modern security protections. Social engineering attacks targeting satellite operators, ground station technicians, or third-party contractors can result in privileged access to mission-critical systems. Technicians working in isolated ground station facilities may have limited oversight, increasing the risk of insider manipulation or credential misuse. In crises such as solar storms or anomalous satellite behavior, operators may bypass security protocols to issue rapid commands, creating windows of vulnerability. Strategic decisions, such as the procurement of foreign-made satellite components, can introduce long-term human-driven risks associated with supply-chain dependencies or geopolitical exposure.

Impact on National Security

A cyber-physical attack on satellite communications can severely undermine national security by disrupting essential services, impairing military readiness, and destabilizing economic activity. Loss of SATCOM can isolate remote regions, disrupt maritime and aviation safety systems, and block critical communication for disaster response teams. Manipulation of satellite navigation signals, such as GPS spoofing, can mislead ships, aircraft, or ground vehicles, resulting in collisions, border disputes, or strategic military miscalculations. Interference with military SATCOM links can degrade command and control operations, hinder surveillance missions, and compromise situational awareness during conflict. A large-scale outage affecting banking networks, television broadcasting, or energy control centers could provoke public chaos, fuel disinformation campaigns, or lead to political unrest. In geopolitical crises, satellite disruption may be interpreted as an act of aggression, potentially escalating tensions or triggering military responses. As satellites also support intelligence operations, their compromise could expose classified data, weaken alliances, and erode national deterrence.

3.5.3 Data Centers and Cloud Infrastructure

Critical to a Nation's Functioning

Data centers and cloud infrastructure constitute the computational and storage backbone of modern economies, hosting critical services for government, finance, healthcare, telecommunications, and virtually every industry. These facilities enable digital operations, secure data storage, real-time analytics, and seamless access to cloud-based platforms used by citizens and businesses. Government databases, e-commerce platforms, emergency systems, industrial control systems, and national research programs all depend on reliable data centers.

Any prolonged outage can halt economic transactions, disrupt public services, or impede emergency response operations. Cloud platforms, including public, private, and hybrid, extend this reliance by centralizing computing power in large-scale data environments, which reduces costs but increases dependency on shared infrastructure. National digital sovereignty is directly linked to the integrity of these systems; if compromised or controlled by hostile actors, the nation risks losing control of sensitive data, critical operations, and strategic intellectual property. Therefore, the continuity and resilience of data centers are fundamental for national stability, economic strength, and societal functionality.

Key Elements (Physical and Digital)

Physical Infrastructure (Data Centers & Cloud)

- **Server hardware**: Compute servers, storage arrays, high-performance computing racks.
- **Critical facility systems:** cooling systems, HVAC units, raised floors, fire suppression systems.
- **Power infrastructure**: Transformers, UPS systems, generators, redundant electrical lines.
- **Physical security**: Controlled access, surveillance systems, biometric authentication, secure cages.
  Networking equipment Includes Routers, switches, fiber links, and perimeter network devices.

Digital Infrastructure (Data Centers & Cloud)

- **Virtualization platforms**, Hypervisors, virtual machines, and container orchestration (such as Kubernetes).
- **Cloud management systems**, IAM, orchestration dashboards, and workload automation.
- **Storage and database systems** include object storage, relational databases, and distributed file systems.

- **Security monitoring and logging**, SIEM platforms, anomaly detection, access logs, and threat intelligence.
- **APIs and cloud services** Compute APIs, storage APIs, serverless platforms, container registries.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Data centers and cloud systems face relentless attacks due to the concentration of valuable data and computational power. Vulnerabilities arise from misconfigured cloud settings, exposed APIs, weak IAM policies, and unpatched hypervisors. Multi-tenancy in cloud environments increases the risk of side-channel attacks, container escapes, or privilege escalation. Supply-chain compromises can introduce backdoors into firmware, BIOS, or server components. Ransomware targeting backup systems or storage arrays can render entire data centers inoperable. DDoS attacks can overwhelm cloud services, disrupting access to government or financial platforms. Mismanaged encryption keys may expose sensitive data, while shadow IT applications may create unmonitored footholds for attackers. Virtual machines, if not properly isolated, can be leveraged to pivot between internal systems.

Infrastructure and Systemic Vulnerabilities

Data centers represent highly centralized infrastructure; a disruption, whether from fire, sabotage, ransomware, or power failure, can disable hundreds of services at once. Power dependencies are critical: if backup generators fail or UPS systems malfunction, even minor outages can cause catastrophic downtime. Cooling systems are essential; attacks targeting HVAC control systems can cause servers to overheat, resulting in widespread equipment failure. Physical access remains a major vulnerability: unauthorized access to server rooms can lead to tampering, hardware theft, or installation of rogue devices. Cloud platforms, which rely on distributed regions, can experience cascading effects if regional networks fail or if software updates propagate faulty configurations. As nations increasingly depend on foreign cloud providers, geopolitical tensions may threaten data sovereignty and access to critical digital assets.

Human Factor Vulnerabilities

Human vulnerabilities span administrators, engineers, contractors, and even users. Misconfigurations such as publicly exposed storage buckets, weak access roles, or overly permissive firewall rules remain one of the most common causes of cloud breaches. Administrators may fall victim to credential theft, enabling attackers to gain control over cloud consoles or data centers.

Contractors responsible for maintenance may connect insecure devices to server racks or bypass procedures due to time pressure. Engineers managing automation scripts may inadvertently introduce vulnerabilities into production systems. Leadership may prioritize rapid digital transformation over secure architecture, resulting in poorly integrated systems or incomplete security assessments. Users storing sensitive information in unsecured cloud environments further widen the attack surface.

Impact on National Security

A cyber-physical attack on data centers or cloud infrastructure can cripple national capability at an unprecedented scale. If a central cloud region goes offline, government platforms, citizen services, emergency dispatch systems, banking platforms, healthcare systems, and corporate applications can all fail simultaneously. Sensitive citizen records, financial data, and confidential government files could be leaked, manipulated, or destroyed, undermining public trust and causing political instability. Disruption of industrial cloud services can halt manufacturing, logistics, and energy operations, weakening economic resilience. Ransomware targeting national clouds could force governments to suspend services or negotiate under pressure. In extreme cases, a coordinated attack could paralyze communication, disrupt intelligence systems, and hobble military command networks. Public panic may rise if essential services fail simultaneously, potentially leading to protests or civil disorder. At the geopolitical level, cloud failures can compromise alliances, weaken national deterrence, and expose vulnerabilities that adversaries can exploit.

3.6 Government and Public Administration

3.6.1 Government IT & Cyber Infrastructure

Critical to a Nation’s Functioning

Government IT and cyber infrastructure form the backbone of public administration, enabling essential state functions such as taxation, healthcare services, national registries, social welfare programs, justice systems, and public safety operations. These systems provide the digital framework through which citizens interact with the state, submitting documents, receiving benefits, accessing identification services, or completing legal obligations. A functional government IT environment ensures continuity of governance, transparency, and smooth coordination across agencies. It also supports national crisis management, enabling the sharing of real-time information, emergency communication, and coordinated decision-making during disasters or security incidents. Without resilient digital infrastructure, government services would slow down or collapse, causing significant disruptions to social stability, economic operations, and public trust. In an era where digital governance is integral to state legitimacy, the reliability, security, and resilience of government IT systems have become vital components of national functioning and political stability.

Key Elements (Physical and Digital)

Physical Infrastructure (Government IT)

- **Government data centers** host servers, national databases, cloud platforms, and secure storage environments.
  Networking infrastructure: Routers, switches, fiber links, secure lines for classified networks.
- **Secure government facilities**, Sensitive compartmented information facilities (SCIFs), secure server rooms, and communication bunkers.
- **End-user equipment** Includes Government workstations, laptops, mobile devices, and secure communication phones.
  Backup sites and continuity facilities Include Disaster recovery centers, redundant computing sites, and emergency communication hubs.

Digital Infrastructure (Government IT)

- **National databases**: Identity registries, tax databases, health records, land registries, justice databases.
- **Government cloud and applications**, E-services portals, internal communication systems, and workflow management software.
  Cybersecurity platforms, threat intelligence systems, SIEM platforms, access control management, and encryption frameworks.
- **Identity and authentication systems,** eID platforms, digital certificates, and multi-factor authentication systems.
- **Secure communication systems,** encrypted messaging, classified communication networks, diplomatic channels.

Cyber-Physical Vulnerabilities

The sector is exposed to multiple vulnerabilities and attack risks, including technical, infrastructural, and human factors (Figure 11).

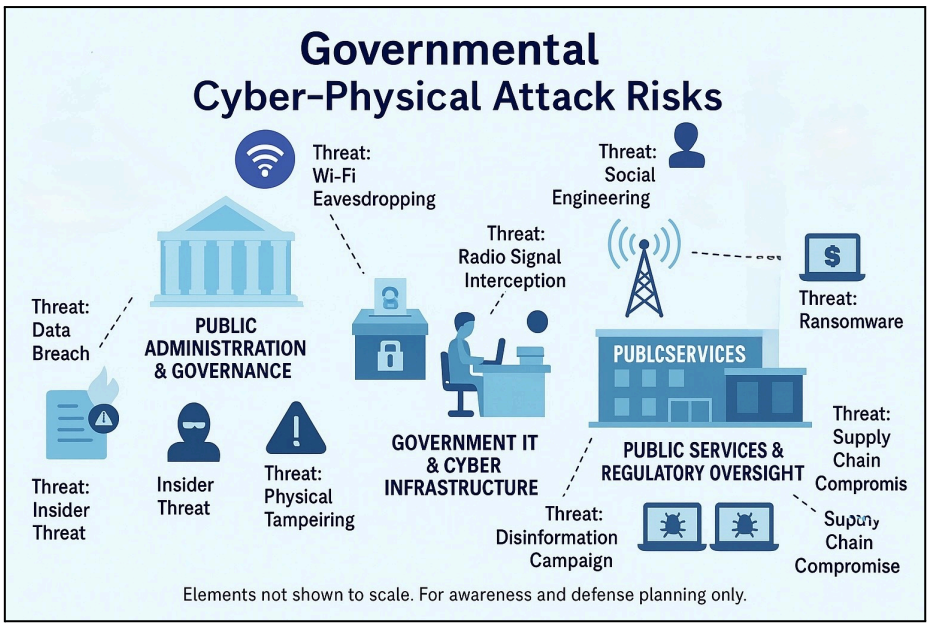


Figure 11 - Main cyber-physical attack risks against the government sector

Technical Vulnerabilities

Government networks are prime targets for state-sponsored hackers, cybercriminals, and hacktivists due to the sensitive data and strategic functions they hold. Legacy systems and outdated software that continue to run in government agencies create exploitable entry points. National identity and citizen databases may rely on outdated architectures that lack strong encryption or modern access controls. Interconnected government platforms can create cascading vulnerabilities: a breach in one department may enable attackers to gain lateral movement across multiple agencies. Email systems, frequently targeted by phishing, can be used to distribute malware or gain unauthorized access to confidential information. Supply-chain attacks pose serious risks, as compromised software updates or third-party service providers may introduce backdoors into government networks. Weak authentication, misconfigurations, or poorly secured cloud migrations further increase exposure.

Infrastructure and Systemic Vulnerabilities

Government IT infrastructure is highly centralized, making it vulnerable to widespread disruption. A cyberattack on national data centers can cripple multiple public services simultaneously, including taxation, social welfare, and healthcare systems. Internet or telecom outages can disconnect government agencies from each other, hindering emergency response and leadership coordination. Physical risks, such as fires, sabotage, or power failures, can compromise essential government operations. Centralized identity systems create systemic vulnerabilities; if compromised, they may allow impersonation, fraudulent access to services, or manipulation of records.

Dependencies on foreign platforms, cloud services, or overseas data storage introduce geopolitical risk, as access may be restricted or monitored during periods of diplomatic tension.

Human Factor Vulnerabilities

Human weaknesses remain among the most significant risks to government cyber resilience. Public officials may fall victim to phishing, social engineering, or credential theft, thereby granting attackers unauthorized access to sensitive systems and information. Poor cybersecurity awareness among civil servants can lead to unsafe practices, including the use of weak passwords, insecure file sharing, and the use of personal devices for official work. Contractors and temporary staff often have wide access to internal systems but limited oversight, increasing insider risks. Political turnover can cause inconsistent cybersecurity policies, underfunding, or misaligned priorities. In crisis scenarios such as natural disasters or political unrest, government employees may bypass procedures, inadvertently creating security gaps. Leadership decisions, particularly those concerning procurement or system modernization, can introduce long-term vulnerabilities if not informed by security expertise.

Impact on National Security

A cyber-physical attack on government IT systems can undermine state authority, disrupt essential public services, and destabilize national security. If identity systems are compromised, attackers could impersonate officials, manipulate citizen records, or disrupt elections. A successful breach of tax or welfare systems could halt payments to citizens, triggering social unrest, economic instability, and political backlash. Disruption of justice or law enforcement databases could compromise investigations, delay court proceedings, or hinder efforts to prevent crime. In a coordinated attack, ransomware could shut down multiple ministries, paralyzing decision-making and crisis management. Compromised diplomatic communication systems could expose classified negotiations or military plans, damaging alliances and national credibility. Public trust in government could deteriorate rapidly if citizens lose access to essential services or discover that confidential data has been leaked online. In extreme cases, such attacks could create political instability, fuel protests, or embolden hostile nations to escalate hybrid aggression.

3.6.2 Public Services and Regulatory Oversight

Critical to a Nation's Functioning

Public services and regulatory oversight ensure the orderly functioning of society by enforcing standards in healthcare, transportation, energy, education, safety, and commerce. These entities maintain stability, protect public welfare, and guarantee that essential services operate safely and fairly. Regulators monitor compliance, issue licenses, enforce laws, and collect critical data that informs national decision-making.

Public services, ranging from water management to waste disposal and social support programs, have a direct impact on daily life and public health. If regulatory systems fail, industries may operate unsafely, markets may become chaotic, and public trust can deteriorate rapidly. These institutions also coordinate crisis management, ensuring rapid response to threats such as pandemics, environmental disasters, or industrial accidents. Their ability to collect reliable data, communicate transparently, and enforce laws is central to maintaining social order, economic fairness, and citizen protection.

Key Elements (Physical and Digital)

Physical Infrastructure (Public Services & Regulators)

- **Administrative offices,** Municipal buildings, inspection centers, service delivery points.
- **Inspection and monitoring equipment:** Environmental sensors, testing facilities, safety inspection tools.
- **Service delivery infrastructure:** water treatment plants, waste management facilities, and social service centers.
- **Archival and documentation sites include Physical archives, storage facilities, and emergency** coordination rooms.
- **Communication facilities** Include Hotlines, broadcast systems, and emergency notification centers.

Digital Infrastructure (Public Services & Regulators)

- **Centralized administrative platforms**, Citizen service portals, licensing systems, and regulatory databases.
- **Data reporting systems**, Environmental monitoring platforms, and compliance reporting dashboards.
- **Automated enforcement systems**, Traffic enforcement systems, safety compliance platforms, financial regulatory tools.
- **Internal IT networks**, Workstations, document management systems, and workflow platforms.

- **Security tools**: Access control systems, encryption tools, and monitoring systems.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Public service systems often rely on outdated IT platforms that lack sufficient cybersecurity features. Regulatory databases may contain sensitive information but lack encryption or proper access segmentation.

Automated enforcement systems, such as environmental sensors or traffic monitors, can be tampered with to falsify compliance results or avoid penalties. Misconfigured citizen-facing portals can expose personal data, enabling fraud or identity theft. IoT devices used for water quality monitoring or waste management often run insecure firmware, making them vulnerable to takeover. Weak APIs or poor integrations between public agencies create exploitable gaps. Attackers may manipulate regulatory data to give unfair advantages to businesses, harm public health, or sow confusion.

Infrastructure and Systemic Vulnerabilities

Public service agencies often operate decentralized networks, creating inconsistencies in security practices across regions. Physical facilities such as water plants, waste management centers, or administrative buildings may lack robust surveillance or access control. During emergencies, these systems face increased demand, making them more susceptible to overload or targeted attacks. Regulators depend heavily on accurate data; if attackers manipulate reporting systems, oversight becomes ineffective. The failure of public communication systems, such as emergency alerts, could cause widespread confusion or panic. Dependencies on private contractors create further systemic risks, as many services rely on outsourced IT or operational functions.

Human Factor Vulnerabilities

Employees often work with large volumes of data and may unintentionally expose sensitive information through email, external drives, or insecure cloud platforms. Social workers, inspectors, or regulators in the field may use mobile devices that are poorly secured or easily lost. Leadership may prioritize service continuity over cybersecurity, resulting in delayed upgrades or overlooked vulnerabilities. Staff turnover increases the likelihood of orphaned accounts, poor documentation, or loss of institutional knowledge. Citizens interacting with public portals may fall victim to phishing or fraud if digital services lack secure verification mechanisms. Insider threats, whether malicious or accidental, pose significant risks due to broad access to personal and regulatory data.

Impact on National Security

A cyber-physical attack on public services or regulators can lead to unsafe environments, public health crises, and economic instability. Manipulation of water quality data could lead to contaminated water reaching households, triggering illness and public outrage. Disruption of waste management could lead to environmental hazards, toxic exposure, or logistical breakdowns. If regulatory systems fail, industries may circumvent safety requirements, thereby increasing the risk of industrial accidents, transportation failures, or pollution incidents. A compromise of citizen services portals could expose personal data, fuel identity fraud, or undermine trust in government institutions. Emergency communication failures could cause chaos during disasters, leading to casualties or delayed rescue operations. Regulatory manipulation can also be used as a tool of economic warfare, destabilizing markets and eroding public confidence. Large-scale disruption to public services can provoke protests, social unrest, or political crises, severely weakening national stability.

3.6.3 Elections and Civic Systems

Critical to a Nation's Functioning

Elections and civic systems are fundamental pillars of democratic governance, ensuring legitimacy, political stability, and public trust in state institutions. Election processes, including voter registration, ballot casting, vote counting, and result reporting, must function transparently and securely to maintain public confidence in the democratic process. Civic systems, including population registries, digital IDs, census databases, and civic participation platforms, support the political and administrative processes that maintain societal cohesion. Disruption or manipulation of these systems can erode trust, trigger political instability, and undermine the foundational principles of democracy. Elections also shape national leadership and long-term strategic decisions, making them attractive targets for foreign influence, cyber espionage, and disinformation campaigns. Their smooth functioning is therefore essential not only for public order but for safeguarding national sovereignty and preventing internal conflict.

Key Elements (Physical and Digital)

Physical Infrastructure (Elections & Civic Systems)

- **Polling stations,** Voting booths, ballot boxes, registration desks, and physical monitoring equipment.
- **Election administration facilities**, Offices of election commissions, storage for ballots and voting machines.

- **Citizen documentation centers**, Population registry offices, ID issuance centers, census processing sites.
- **Transportation & logistics**: Vehicles transporting ballots, secure ballot storage facilities.
  Security personnel and observation teams, Including Poll watchers, police support, and observers.

Digital Infrastructure (Elections & Civic Systems)

- **Voter registration databases**: Centralized or localized systems containing voter records and eligibility data.
  Electronic voting machines (where applicable), Voting terminals, tallying modules, and firmware.
- **Vote counting and aggregation systems,** Central tally servers, results reporting platforms, and election dashboards.
- **Civic management platform, Census** databases, public consultation systems, digital ID services.
- **Cybersecurity tools**, Monitoring systems, encryption frameworks, and incident response platforms.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Election systems often include outdated software, insecure APIs, or unpatched vulnerabilities. Voter databases may be targeted for deletion or manipulation, altering voter eligibility. Electronic voting machines, when used, may be vulnerable to insecure firmware, weak encryption, or physical tampering risks. Central tallying systems could be targeted by DDoS attacks, malware, or data manipulation, delaying results or causing public confusion. Websites used for result reporting are often hosted on vulnerable platforms prone to defacement or misinformation. Civic databases and census systems may have weak authentication or lack proper encryption, exposing sensitive demographic data that can be used for political targeting or fraud.

Infrastructure and Systemic Vulnerabilities

Elections rely heavily on physical logistics; disruption of ballot transportation, storage facilities, or polling stations can compromise the process. Power outages, communication failures, or infrastructure sabotage on election day can disenfranchise voters or halt the vote-counting process. A small number of central systems typically aggregate votes; if compromised, the entire election outcome can be called into question. External dependencies, such as cloud hosting providers or foreign technology suppliers, create geopolitical vulnerabilities.

Civic systems such as digital IDs or population registries may act as single points of failure; if compromised, they can invalidate voter authentication or enable fraudulent entries.

Human Factor Vulnerabilities

Election workers, often temporary staff, may lack strong cybersecurity awareness, making them vulnerable to phishing or social engineering attacks. Poll workers may mishandle equipment or overlook tampering due to high voter volume and time pressure. Officials may use insecure channels for sensitive communication, allowing attackers to intercept or manipulate information. Political actors or insiders may attempt to influence or sabotage systems for partisan gains.

Public perception can be exploited by disinformation and amplified by mistakes made by election officials. Leadership failures such as poor planning, inadequate cybersecurity investment, or a lack of transparency can amplify the impact of attacks or technical failures.

Impact on National Security

A cyber-physical attack on elections or civic systems can destabilize the nation by undermining democratic legitimacy and sparking political conflict. Manipulation or disruption of vote counting could provoke accusations of fraud, mass protests, or political violence. Attacks on voter databases could disenfranchise communities, escalate tensions, and lead to legal disputes. Disinformation campaigns targeting election results could divide the population and weaken confidence in democratic institutions. A breach of civic databases may expose millions of citizens to identity theft or surveillance, fueling distrust in government. In extreme cases, disputed election outcomes can lead to constitutional crises, paralysis of governance, or long-term political fragmentation. Foreign interference in elections can alter geopolitical alignments, weaken alliances, and undermine national sovereignty. Ultimately, the integrity of electoral and civic systems is essential to maintaining internal stability, public trust, and international credibility.

3.7 Defense and Military

3.7.1 Military Infrastructure

Critical to a Nation's Functioning

Military infrastructure forms the core of national defense, ensuring the state's ability to deter aggression, respond to threats, and maintain territorial integrity. It includes bases, command centers, logistics hubs, weapons depots, training facilities, and digital networks used for strategic communications and operational planning. These systems uphold national sovereignty by ensuring readiness, enabling rapid mobilization of forces, and maintaining situational awareness through surveillance and intelligence networks. Military installations also support international commitments, peacekeeping missions, and crisis response operations, reinforcing geopolitical influence. Beyond defense, military infrastructure often plays a crucial role during natural disasters or internal emergencies, offering logistical support, medical capabilities, and manpower. Any disruption to these systems, whether through cyberattacks, sabotage, or physical damage, can degrade a country's ability to protect itself, risking national instability, weakened deterrence, and potential exploitation by adversaries. The continuous operation of military infrastructure is therefore fundamental to sustaining national security, projecting strength, and ensuring the safety of citizens.

Key Elements (Physical & Digital)

Physical Infrastructure (Military)

- **Military bases and installations**: Army, Navy, Air Force bases; training grounds; logistics hubs.
- **Command and control centers**, Operation rooms, communication bunkers, war rooms, Joint Operations Centers (JOCs).
- **Weapons and ammunition depots**, Storage facilities, missile silos, armored vehicle depots, and naval arsenals.
- **Critical platforms**: Aircraft, naval vessels, armored vehicles, missile batteries, and radar systems.
- **Energy and logistics systems**: Fuel depots, maintenance hangars, transport fleets, secure electrical infrastructure.

Digital Infrastructure (Military)

- **Battle management systems** C4ISR platforms, real-time situational awareness tools, and mission planning software.
- **Secure communication networks**, Encrypted radio, satellite systems, classified networks, tactical data links (Link 16).

- **Weapons system software**, Guidance systems, fire control software, aircraft avionics, and naval combat systems.
  Cyber defense and monitoring systems, Intrusion detection, cyber operations centers, threat intelligence platforms.
- **Logistics and maintenance systems**, Digital supply chains, predictive maintenance tools, and encrypted databases.

Cyber-Physical Vulnerabilities

The sector is exposed to multiple vulnerabilities and attack risks, including technical, infrastructural, and human factors (Figure 12).

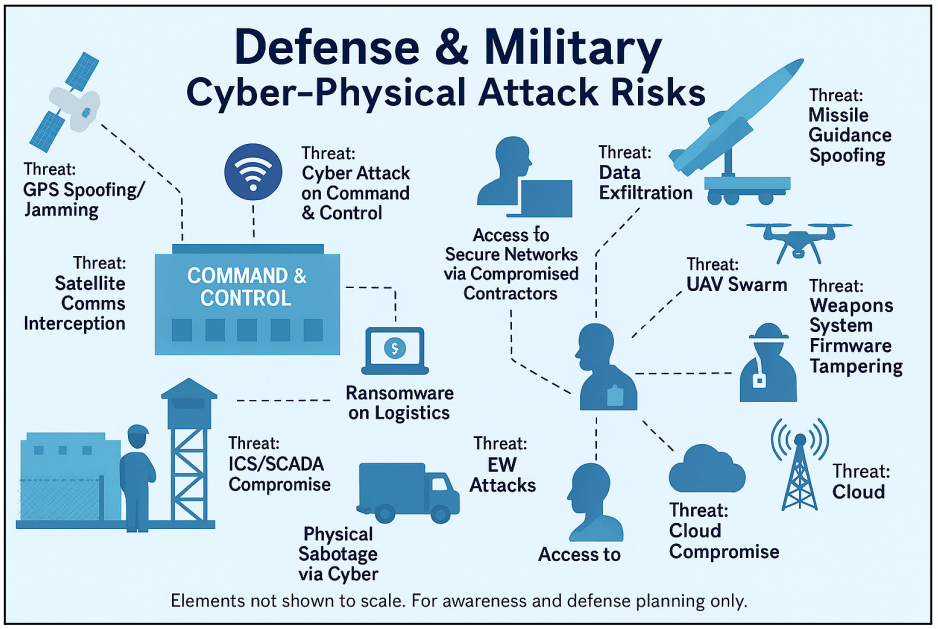


Figure 12 - Main cyber-physical attack risks against the defense and military sector

Technical Vulnerabilities

Military systems are increasingly relying on software-defined weapons, digital communications, and network-dependent command structures, which create complex technical risks. Outdated or unsupported operating systems on critical platforms such as aircraft avionics or naval radar can expose exploitable vulnerabilities. Weapons systems may rely on embedded components sourced from global suppliers, increasing the risk of compromised firmware or hidden backdoors. Encrypted communications can be degraded through jamming, spoofing, or cryptographic attacks, impairing coordination. Drones and unmanned systems can be hijacked if communication links are weak or if GPS signals are spoofed. Complex military networks integrating legacy and modern systems often create configuration gaps that adversaries can exploit.

Infrastructure and Systemic Vulnerabilities

Military bases and command centers represent high-value targets whose disruption can severely impair national defense. Fuel depots, power supplies, and logistics hubs, often located far from urban centers, may have limited surveillance and can be physically sabotaged. Radar and early-warning systems form single points of failure: if disabled, adversaries could gain air or naval advantage. Satellite dependency for communication and navigation creates systemic risks if satellites are jammed, destroyed, or compromised through hacking. Interoperability between branches of the military and allied forces increases the attack surface, as vulnerabilities in one system can compromise entire command networks. Natural disasters or internal crises can stretch military infrastructure, making it more vulnerable to coordinated attacks.

Human Factor Vulnerabilities

Human vulnerabilities arise from highly specialized yet widely distributed personnel. Soldiers and officers may fall victim to targeted spear-phishing campaigns, which can enable intrusions into classified networks. Maintenance crews or contractors may unintentionally install compromised components or bypass security protocols under operational pressure. Insider threats are significant due to access to weapons, logistics, and critical networks. In times of war or crisis, the pressure to act quickly may lead operators to circumvent security procedures or rely on insecure communication channels. Leadership decisions such as cost-driven procurement, delayed modernization, or insufficient cybersecurity training can create long-term exposure.

Impact on National Security

A cyber-physical attack on military infrastructure could cripple national defense, weaken deterrence, and embolden hostile actors. Disrupting command and control networks can paralyze decision-making or create confusion among deployed units, increasing the risk of battlefield losses or strategic miscalculations. Sabotage of weapons systems, such as disabling missile batteries or corrupting aircraft navigation, could leave territories undefended. Manipulation of logistics systems may delay troop mobilization or disrupt supply chains, undermining operational readiness. A successful attack on nuclear or strategic facilities could trigger panic, international tension, or accidental escalation. If adversaries compromise classified networks, they may obtain intelligence on troop movements, vulnerabilities, or military plans. In extreme cases, military paralysis could invite aggression, territorial incursions, or hybrid warfare campaigns that destabilize the nation and weaken alliances.

Digital Infrastructure (Defense & Aerospace)

- **Design and simulation systems**, CAD software, digital twins, and simulation models for weapons and aircraft.
  Manufacturing automation systems, Robotics platforms, programmable logic controllers (PLCs), and industrial control systems.
- **Secure networks and development environments**, Encrypted communication platforms, and classified design networks.
  Software for avionics and weapons embedded systems, flight control algorithms, and missile guidance software.
  Cyber defense systems, Security monitoring, vulnerability scanning, and secure software repositories.

3.7.2 Intelligence and Security Agencies

Critical to a Nation's Functioning

Intelligence and security agencies play a central role in safeguarding national sovereignty, protecting citizens, and countering threats such as terrorism, espionage, organized crime, and foreign interference. These agencies collect, analyze, and disseminate information crucial for decision-making by political and military leaders. They also secure the state against cyberattacks, monitor hostile activities, and support international alliances. Intelligence agencies ensure the stability of democratic institutions by preventing covert manipulation, disinformation, or destabilizing operations conducted by adversaries. Their ability to operate discreetly and securely is essential for anticipating threats before they materialize. A failure in intelligence operations can expose the nation to surprise attacks, internal unrest, or strategic blind spots, jeopardizing national safety. Thus, the continuity and security of intelligence infrastructure are vital to national defense, crisis prevention, and geopolitical stability.

Key Elements (Physical & Digital)

Physical Infrastructure (Intelligence & Security Agencies)

- **Secure headquarters and field offices**, Surveillance units, interrogation facilities, and analysis centers.
- **Operational equipment** Includes Surveillance devices, communication tools, and secure vehicles.
  Archival and classified rooms, Secure vaults, SCIFs, and evidence storage facilities.
  Training facilities, Counterintelligence schools, cyber operations centers, analytical training hubs.

- **Physical communication hubs** Include Satellite uplinks, radio towers, and secure fiber networks.

Digital Infrastructure (Intelligence & Security Agencies)

- **Classified databases and archives**, Intelligence repositories, biometric data systems, and strategic assessments.
  Cyber operations platforms, Offensive and defensive cyber tools, intrusion detection, malware analysis labs.
- **Encrypted communication systems**, Secure messaging, diplomatic communication channels, and agent communication networks.
- **Surveillance and data analysis tools**, AI analytics, OSINT platforms, SIGINT systems, and geospatial mapping tools.
- **Counterintelligence monitoring systems**, Insider threat detection, anomaly monitoring, behavioral analytics.

Cyber-Physical Vulnerabilities

Technical Vulnerabilities

Intelligence agencies rely on highly sensitive digital systems that are constantly under threat from nation-state actors. Zero-day vulnerabilities in classified networks may allow intrusions that go undetected for months. Intercepted communications or compromised encryption protocols can expose agents and operations to potential risks. Surveillance systems may be manipulated to falsify data or hide hostile activity. Malware targeting intelligence databases could exfiltrate large volumes of classified information. Quantum computing advances pose future risks to encrypted channels. Agencies increasingly rely on commercial software and cloud solutions, which increases their potential exposure to supply-chain attacks or software compromise.

Infrastructure and Systemic Vulnerabilities

Centralized intelligence repositories create single points of failure; a breach or destruction of classified databases can compromise decades of intelligence. Secure facilities may be targeted for physical intrusion, sabotage, or insider manipulation. Intelligence agencies rely on foreign satellite networks, fiber cables, or cloud services, creating geopolitical dependencies. Disruption of communication hubs can sever contact with field agents, compromising ongoing operations. Inter-agency information sharing may introduce vulnerabilities if foreign partners suffer breaches. Infrastructure supporting surveillance or counterterrorism operations may be exposed to jamming, signal interference, or geographic disruption during crises.

Human Factor Vulnerabilities

Intelligence operations involve significant human risk. Agents, analysts, and field officers can be targeted by espionage, bribery, blackmail, or coercion. Insider threats pose a catastrophic risk because a single insider can leak massive amounts of classified information or compromise operations. Human error, such as mishandling classified documents or using insecure communication channels, can expose sensitive missions. Leadership may underestimate emerging cyber threats or fail to modernize outdated analytic or communication systems. Contractors, translators, or external experts may inadvertently introduce vulnerabilities due to insufficient clearance or poor security practices.

Impact on National Security

A cyber-physical attack on intelligence agencies can be one of the most devastating forms of national security compromise. Exposure of classified operations may endanger lives, reveal strategic capabilities, or expose espionage networks worldwide. Manipulation of intelligence data can mislead leaders, resulting in flawed strategic decisions or misguided military actions. Disruption of surveillance systems could allow terrorist plots or foreign espionage to go undetected. If diplomatic communication channels are compromised, sensitive negotiations or alliance strategies may be exposed, damaging geopolitical relationships. A leak of biometric databases may compromise the identities of undercover agents or enable adversaries to identify intelligence operatives abroad. Public disclosure of intelligence failures or breaches can erode trust in government, fuel political instability, and weaken national morale. At the highest level, failures in intelligence infrastructure can leave the nation blind to external threats, undermining deterrence and exposing the country to strategic surprise.

4. Conclusion

Cyber-physical attacks have become one of the defining national security challenges of the digital age. Repeated incidents over the past decade have demonstrated the vulnerability of critical infrastructure, including energy systems, transportation networks, water facilities, healthcare services, and communications, to sophisticated cyber threats. Whether aimed at sabotage, strategic coercion, or intelligence collection ahead of future military operations, these attacks underscore the extent to which national stability now depends on the integrity of interconnected digital and physical systems.

Threat actors ranging from nation-states to highly organized cybercriminal groups understand that targeting critical infrastructure can inflict far-reaching security, economic, and psychological consequences. Importantly, the human factor plays a decisive role at every stage: operator error, insufficient cyber hygiene, under-resourced security teams, and gaps in organizational culture often create openings that even the most advanced technologies cannot fully compensate for. The success or failure of many cyber defenses ultimately hinges on trained personnel, effective decision-making under pressure, and sustained awareness across all layers of an organization. Despite heavy investment in defensive capabilities and regulatory frameworks, critical infrastructure remains exposed to evolving threats due to system interdependencies, legacy equipment, and the persistent challenge of human vulnerabilities. The resulting risk extends far beyond temporary service disruptions. Cyberattacks on critical infrastructure can undermine public trust, destabilize national governance, weaken military readiness, and erode the societal cohesion essential for national resilience. In an era where cyber warfare blurs the boundaries between civilian and military domains, protecting critical infrastructure has become a strategic imperative. Enhancing national security and stability will require not only advanced technical measures but also stronger cross-sector collaboration, rigorous training for the human operators at the center of these systems, and proactive national-level planning to anticipate and mitigate emerging threats. Only by addressing both technological and human dimensions can nations safeguard the infrastructures that underpin their security and sovereignty.

5. About the Author



I am a cyber intelligence expert with over a decade of experience across academia, high-tech, military, and law enforcement environments. My core expertise includes intelligence strategy, collection, research, and analysis, with a strong specialization in leading cyber intelligence research initiatives and Cyber HUMINT operations targeting criminal and terrorist activity in cyberspace.

My research interests center on cybercrime, cyberterrorism, and cyber-geopolitical intelligence. Throughout my career, I have trained numerous civilian analysts, military personnel, and law enforcement officers in cyber intelligence research and operational practices, including work within Deep and Dark Web environments, as well as intelligence collection, analysis techniques, and methodological frameworks.

6. References

1. Longo, A., et al. (2025). Cyber–Physical Resilience: Evolution of Concept, Definition, and Assessment Methodologies.
   (URL) https://www.mdpi.com/2079-9292/14/8/1684

2. NIST (2022). Guide to Operational Technology (OT) Security — SP 800-82 Rev. 3.
   (URL) https://csrc.nist.gov/pubs/sp/800/82/r3/ipd

3. NIST (2014/updated). Cybersecurity Framework (CSF).
   (URL) https://www.nist.gov/cyberframework

4. ENISA (2025). Threat Landscape 2025.
   (URL) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

5. NATO (2024). Hybrid Threats and Hybrid Warfare.
   (URL)
   https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

6. CIDOB (2022). Hybrid Attacks on Critical Infrastructure.
   (URL)
   https://www.cidob.org/en/publications/hybrid-attacks-critical-infrastructure

7. ODNI (2025). Annual Threat Assessment of the U.S. Intelligence Community.
   (URL) https://www.dni.gov/index.php/what-we-do/annual-threat-assessment

8. NATO StratCom COE (2021). Russia's Strategy in Cyberspace.
   (URL)
   https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

9. NKSC Lithuania (2025). Comparative Study of Russian Offensive Cyber Capabilities (2022–2025).
   (URL)
   https://www.nksc.lt/doc/rkgc/A_Comparative_Study_of_Russian_Offensive_Cyber_Capabilities_from_2022_to_2025.pdf

10. CISA / NSA / FBI (2025). Chinese State-Sponsored Actors Targeting Critical Infrastructure (AA25-239A).
    (URL) https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

11. NJCCIC (2024). China-Linked Cyber Operations Targeting U.S. Critical Infrastructure.
(URL) https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure

12. INSS (2018). The Iranian Cyber Threat.
(URL) https://www.inss.org.il/publication/iranian-cyber/

13. CSIS (2025). Evaluating Iran's Cyber Strategy – A Playbook for Winning the Cyber War (Part 4).
(URL) https://www.csis.org/analysis/playbook-winning-cyber-war-part-4-evaluating-irans-cyber-strategy

14. CISA / Treasury / FBI (2020). FASTCash 2.0 – North Korea's BeagleBoyz Robbing Banks (AA20-239A).
(URL) https://www.cisa.gov/sites/default/files/publications/AA20-239A_FASTCash2.0_508.pdf

15. Abraham, D., et al. (2025). Cyber-Attacks on Energy Infrastructure — Literature Review.
(URL) https://www.mdpi.com/2076-3417/15/17/9233

16. E-ISAC & SANS (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid.
(URL) https://www.sherpain.net/SW_upload_file/SW_qna/a615bde86d160330091226.pdf

17. Ghafur, S., et al. (2019). The Impact of the WannaCry Attack on the NHS.
(URL) https://pmc.ncbi.nlm.nih.gov/articles/PMC6775064/

18. UK National Audit Office (2018). Investigation: WannaCry Cyber Attack and the NHS.
(URL)https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

19. IMF (2024). Global Financial Stability Report — Cyber Risk and Financial Stability.
(URL)https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3.ashx

20. Doerr, S., et al. (2022). Cyber Risk in Central Banking (BIS Working Paper 1039).
(URL) https://www.bis.org/publ/work1039.pdf

21. ICAO (2020+). Aviation Cybersecurity Strategy.
(URL) https://www.icao.int/aviation-cybersecurity-strategy

22. IMO (2025). Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ 3/Rev.3).
(URL) https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/MSC-FAL.1-Circ.3-Rev.3.pdf

23. UNIDIR (2025). Subsea Telecommunications Cables as Critical Infrastructure.
(URL) https://unidir.org/publication/achieving-depth-subsea-telecommunications-cables-as-critical-infrastructure/

24. ENISA (2025). Cybersecurity for Commercial Satellite Operations — From Cyber to Outer Space.
(URL) https://www.enisa.europa.eu/news/from-cyber-to-outer-space-a-guide-to-securing-commercial-satellite-operations

25. ODNI & CISA (2024). Securing Election Infrastructure Against Foreign Malign Influence.
(URL) https://www.dni.gov/files/FMIC/documents/products/Securing-Election-Infrastructure-Against-The-Tactics-Of-Foreign-Malign-Influence-Operations-Apr2024.pdf