Computer Fraud and Security
ISSN (online): 1873-7056

Digital Resilience and Public Safety: Why Secure Automation Matters Beyond IT

Sameer Lakade

Independent Researcher, USA

Abstract

The growing reliance of contemporary society on digital infrastructure would render secure automation not only an engineering problem but also a primary societal issue of public safety concern, with potentially far-reaching consequences for national security, economic stability, and societal well-being. The automated systems in areas such as healthcare delivery, transportation networks, financial infrastructure, and energy utilities have continuous integration pipelines, orchestration platforms, and machine-driven control loops running at an unprecedented scale and complexity. Although automation provides significant efficiency and opens up new services that were previously unavailable, it also introduces systemic risks, such as software supply chain breaches, malconfigured pipelines during deployment, and unauthorized code editing, which can lead to cascading failures with catastrophic real-world impacts. The article explores the intersection of Systems Infrastructure and Automation Engineering with digital resilience, national security frameworks, and public welfare requirements, and proposes a general Digital Resilience Framework that can integrate secure DevOps and Infrastructure-as-Code practices into critical societal domains. The framework focuses on reliable automation based on zero-trust architectures, policy-driven verification, cryptographic provenance, and resilient orchestration of multi-cloud and hybrid systems. This article argues that secure automation serves as the foundational layer on which the trust of digital society in the general population should be built, through interdisciplinary studies that combine engineering principles, cybersecurity standards, socio-technological governance frameworks, and policy frameworks. The article ends with recommendations on how to apply the principles of safety engineering, the supply chain verification rules, the ongoing monitoring of compliance, and the collaboration between the different sectors into the national strategies of digital resiliency, where automation security level should be managed in the same manner as the traditional engineering fields, such as enhanced governance, transparency, and moral accountability.

Keywords: Digital Resilience, Automation Security, Critical Infrastructure Protection, Supply Chain Security, Devsecops

I. Introduction

A. The Digital Infrastructure Imperative

The digital infrastructure has become the base on which contemporary civilization is working, and the isolated information technology systems are being replaced by highly dependent services that the society is deeply connected and controls the fundamental services and economic transactions as well as national security operations. Modern societies depend on approximately 16 essential infrastructure sectors, as outlined by the U.S. Department of Homeland Security. Digital automation forms the connective tissue that holds the sectors of these ecosystems together into operational systems [1]. In this respect, digital resilience can be defined as the ability of the automated systems to remain available, intact, and trustworthy to adverse events such as cyberattacks, cascading failures, and supply chain attacks. This resilience goes beyond technical strength to cover organizational readiness, regulatory compliance, and social trust with digital services that are playing a growing mediating role in access to healthcare, financial resources, and public safety systems.

B. Automation as Critical Infrastructure

Automated systems have been established with a degree of pervasiveness in key sectors never before seen, with healthcare organizations implementing continuous integration pipelines of electronic medical record systems to support in excess of 250 million patients worldwide, transportation networks organizing real-time traffic management across interconnected urban environments, financial institutions handling around 700 billion digital transactions yearly through automated clearing systems, and energy utilities managing smart grid infrastructure to support billions of connected end points [2]. The development of automation as a tool of productivity in the 1990s and as an essential societal need in 2025

thus implies a paradigm shift in how automation security has evolved to view automation technology as a vital element of corporate information technology needs or is seen as a public safety need, akin to the reliability of electrical grids or the integrity of water systems.

C. The Safety-Security Convergence

The old physical borders between information technology risk and physical public safety risk have eroded because digital systems have become a precondition for the most essential services. Automation failures have ripple effects in the economic, social, and humanitarian realms, as seen in cases such as damaged continuous deployment pipelines disrupting healthcare service provision, incorrectly set up infrastructure orchestration shutting down regional fuel supplies, and hacker attacks on supply chains, subjecting thousands of organizations to systemic risks. This intersection demands a transformation of the concept of automation as a social good, one that should be governed by community structures, communal responsibility systems, and regulatory tools that can create a balance between the speed of innovation and the safety and security needs of society.

D. Research Objectives and Contributions

The paper presents the Digital Resilience Framework as an organized interface between automation engineering practice and quantifiable societal safety impacts, defining the crucial point of convergence between Systems Infrastructure Engineering, national security requirements, and the interests of the people in risk management strategies.

II. Automation in Critical Infrastructure: Dependencies and Vulnerabilities

A. Sectoral Analysis of Automation Dependencies

1. Healthcare Systems

Medical facilities are run on intricate and multifaceted layers of automation, encompassing electronic medical record systems that cover approximately 96% of hospitals in developed countries, clinical decision support systems that handle millions of diagnostic requests each day, and pharmaceutical supply chain management applications that coordinate inventory across distributed networks. Patient telemetry infrastructure is based on persistent data ingestion pipelines that track the vital signs of patients remotely, and automation failure can pose a threat to the care delivery of at-risk groups. Recent case studies have demonstrated that disruptions in healthcare automation can slow down necessary processes, interrupt medication delivery, and negatively impact patient safety outcomes when deployment pipelines fail or configuration drift leads to system instabilities.

2. Transportation Networks

Automation in transportation includes air traffic control systems that serve a daily flight count of more than 100,000 across the world on a satellite navigation infrastructure, autonomous vehicle coordination platforms that coordinate fleet activities within urban settings, railway signaling systems that guarantee collision avoidance over thousands of miles of railways, and maritime logistics automation that guides container movements over international ports. These systems have such strong interdependencies with energy grids that deliver operational power and telecommunications networks that enable real-time coordination, which provides vulnerability channels that result in losses to multiple domains of the infrastructure simultaneously.

3. Financial Infrastructure

Examples of financial automation architecture are high-frequency trading algorithms that run millions of transactions in a second, digital payment networks that process global trade worth trillions of dollars each year, real-time gross settlement systems that handle interbank transactions, and fraud detection systems that analyze the patterns of transactions by applying machine learning models [3]. Regulatory compliance is achieved through automated compliance monitoring, and market-making is facilitated through algorithmic liquidity in the markets that support market stability. Nonetheless, the complexity of automation reintroduces the mechanisms of amplifying systemic risk in which the interactions of the algorithms are unexpected to cause market behaviours as well as new flash crash-like phenomena.

4. Energy and Utilities

Automation in the energy sector also coordinates smart grids to reach billions of connected endpoints, including systems for demand response balancing, the real-time balancing of generation and consumption, and industry control systems that

manage power generation plants. Additionally, SCADA systems monitor distribution infrastructure across large geographic areas [4]. Predictive maintenance algorithms maximize equipment reliability, while distributed energy resource management incorporates renewable generation sources. Energy automation is interdependent with water treatment facilities, natural gas distribution systems, and telecommunications infrastructure, creating systemic vulnerabilities that can lead to cascading failures spreading throughout essential services.

B. The Societal Cost of Automation Failures

The Colonial Pipeline ransomware attack in May 2021 revealed the implications of automation vulnerability by impacting six days of operational failure of fuel distribution across the southeastern United States, fuel distribution-related economic disruption estimated by hundreds of millions of dollars, and behavior of panic purchasing in the affected markets [13].

Sector	Core Automation Systems	Key Dependencies	Vulnerability Points
Healthcare	EMR Systems, Clinical Decision Support, Supply Chain Management, Telemetry	Data Pipelines, Remote Monitoring	Pipeline Failures, Configuration Drift
Transportation	Air Traffic Control, Navigation, Vehicle Orchestration, Signaling	Energy Grids, Telecommunications	Cascading Failures, Coordination Loss
Financial	Trading Algorithms, Payment Networks, Settlement Platforms, Fraud Detection	Machine Learning, Market-making	Algorithm Interactions, Flash Crashes
Energy	Smart Grids, Demand Response, SCADA, Predictive Maintenance	Water Systems, Gas Networks, Telecom	Cross-sector Propagation

Table 1: Automation Dependencies Across Critical Infrastructure Sectors [3, 4]

III. The Threat Landscape: Understanding Automation Risks

A. Supply Chain Vulnerabilities

Attacks on the software supply chain have grown exponentially, and modern applications are built with thousands of dependencies (which form large attack surfaces) that can be exploited by dependency confusion attacks, typosquatting, and malicious package injection. Systems of building are of high value to attackers because they have privileged access to production systems and can disseminate the artifacts of the attack throughout entire ecosystems. Studies have shown that approximately 80 percent of current codebases consist of open-source components, although many corporations lack provenance verification and assurance systems that verify the integrity and authenticity of binaries [5]. Transitive dependencies are even more dangerous, as vulnerabilities can spread across dependency chains of up to five or more levels, introducing blind spots where malicious code can still be introduced without being noticed until it is deployed into production systems supporting critical infrastructure.

B. Configuration and Orchestration Risks

Misconfigurations of infrastructure-as-code are frequent vectors of vulnerability, and researchers report that more than 60 percent of cloud systems have at least one critical misconfiguration scenario that exposes sensitive data or provides unauthorized access. Weaknesses in CI/CD pipeline security enable privilege escalation attacks when attackers compromise credentials, allowing them to deploy to production environments. The failures in managing secrets include disclosing API keys, database credentials, and cryptographic material in hard-coded values within configuration files, environment variables within version control systems, and the poor encryption of sensitive parameters. The complexity of multi-cloud orchestration geometrically increases the attack surface as organizations operate workloads on

heterogeneous platforms, each of which presents a distinct security concern, authentication policies, and policy implementation demands that conflict with maintaining a consistent security posture.

C. Operational Opacity and Observability Gaps

Modern automation systems are often black boxes with decision-making logic that is not well understood by operators and security staff, especially in AI-based orchestration systems, where the complexity of a model obscures the logic. Lack of telemetry and logging of the continuous deployment system impedes the detection of incidents and forensic investigations, and many organizations do not keep detailed audit trails of automation choices, configuration modifications and access patterns [6]. It takes days or weeks to be detected in a complex environment by an automation with malicious or unintended actions, giving attackers a strong opportunity to have a long dwell period and develop persistence mechanisms and exfiltrate sensitive information. The ability to differentiate between normal automation actions and abnormal activity at scale involves highly skilled baseline modeling and anomaly detection algorithms, which have been insufficiently executed by many organizations.

D. Human–Machine Coordination Failures

Automation complacency is a condition where operators become too trusting of automated systems and become less vigilant and less willing to take action in the case of failure. The phenomena of deskilling is the occurrence of automated systems that take over the tasks that involved the competency of the human operator and the situational awareness required to respond to an emergency situation effectively. Trusting AI-based orchestration without backups can lead to points of failure, which, in the event of a system failure, can result in service failures affecting critical operations.

Vulnerability Type	Attack Vectors	Exploitation Methods	Impact Scope
Third-party Dependencies	Dependency Confusion, Typosquatting, Malicious Injection	Build System Compromise, Artifact Distribution	Ecosystem-wide Propagation
Provenance Verification Gaps	Unsigned Binaries, Lack of Authentication	Binary Integrity Compromise	Production System Infiltration
Transitive Dependencies	Multi-level Dependency Chains	Hidden Code Insertion	Undetected Deployment

Table 2: Software Supply Chain Vulnerability Categories [5]

IV. The Digital Resilience Framework (DRF): Architecture and Implementation

A. Conceptual Foundation

By modifying traditional cybersecurity metrics, the Digital Resilience Framework establishes objective means of linking automation engineering practice with societal safety outcomes, thereby bridging the gap between technical implementation capabilities and policy goals related to the protection of critical infrastructure. Digital resilience does not only includes system availability or speed of recovering an incident but the overall ability of automated systems to uphold trustworthiness, operational integrity and confident in adversarial circumstances, cascading failures and supply chain compromises [7]. It is a translational architecture that links technical practitioners who build secure automation pipelines, policymakers who define regulatory needs, and civil society who stakeholders rely on secure digital services to perform some of the most important functions such as healthcare access, financial transactions, and transportation coordination.

B. Pillar 1: Secure Automation Core

1. Zero-Trust Architecture for Build and Deployment

Zero-trust principles essentially reorganize automation security by removing the assumption of implicit trust and implementing the continuous verification of the build and deployment lifecycles. Identity verification systems are used to authenticate all actors and artifacts involved in automation processes, and least privilege access controls are employed to

grant access to the minimum scope required for a particular action. Network segmentation plans separate the build environments and production systems, whereas microsegmentation further separates workloads to limit possible breaches. Encrypted pathways ensure security within communication among automation elements, and the use of secure storage artifacts, protected by cryptographic controls, guarantees the tamper-evident preservation of construct results, deployment configurations, and operational conditions data.

2. Cryptographic Integrity and Provenance

Software Bill of Materials generation is a procedure that generates extensive inventories recording all elements that constitute deployed systems and therefore, vulnerability tracing and dependency management across multifaceted software ecosystems [8]. The implementation of Supply Chain Levels of Software Artifacts defines the progressive security requirements in terms of integrity of the build platform, verification of source provenance, and non-falsifiable attestation of the build platforms. Digital signature mechanisms provide artifact authenticity by cryptographically binding the software packages to the authorized publishers and attestation systems generate verifiable claims on build environments, compilation parameters and testing results. Provenance tracking keeps end-to-end visibility of commits to the source code into production deployment, generating audit trails that can be used to perform forensic investigation and compliance verification.

3. Continuous Compliance Monitoring

Policy-as-Code integrates compliance needs and security controls with deployment pipelines, allowing them to automatically validate that configurations meet compliance frameworks before they reach production environments. To enable continuous assessment of the system's state against standards such as NIST cybersecurity frameworks, industry regulations, and organizational security standards, automated compliance validation generates evidence artifacts that authenticate audit processes. Real-time drift detection is used to identify unauthorized changes to configurations or those not functioning according to approved baselines, and to initiate automated remediation processes that restore compliance states or notify the security operations team of the need for investigation. Audit trail generation generates detailed documents of all automation decisions, access events and configuration changes that give forensic capabilities that can assist incident response as well as regulatory reporting requirements.

C. Pillar 2: Governance and Transparency

1. Public Auditability Mechanisms

Software provenance registries keep authoritative data stored in the form of version histories, build attestations, and cryptographic signatures of critical infrastructure components and allow stakeholders to check the authenticity of artifacts and trace integrity in the supply chain. A build attestation publication is the publicly available cryptographic evidence of secure build practices, which can be used by independent verification to understand that software artifacts were created by authorized processes out of trusted sources. Architectures based on Certificate Transparency principles generate append-only, tamper-evident logs of software releases, configuration changes, and security events, which build verifiable histories and identify any attempts to manipulate the logs.

D. Pillar 3: Resilience Engineering

1. Redundancy and Fault Isolation

Multi-region deployment plans distribute workloads across geographically distinct infrastructure zones, ensuring service continuity in the event of localized failures in individual regions through automated failover to healthy components.

DRF Pillar	Key Components	Security Mechanisms	Primary Objectives
Secure Automation Core	Zero-Trust Architecture, Cryptographic Integrity, Compliance Monitoring	Identity Verification, Least Privilege Access, Network Segmentation, Digital Signatures	Continuous Verification, Tamper-evident Preservation, Automated Validation
Governance & Transparency	Provenance Registries, Build Attestations,	Version Histories, Cryptographic Signatures,	Public Auditability, Supply Chain Traceability, Independent

	Transparency Logs	Append-only Records	Verification
Resilience Engineering	Multi-region Deployment, Fault Isolation, Automated Failover	Geographic Distribution, Redundancy Mechanisms	Service Continuity, Localized Failure Containment

Table 3: Digital Resilience Framework (DRF) Pillars and Components [7]

V. Cross-Sector Collaboration and Policy Integration

A. The Policy Imperative for Secure Automation

Secure automation has become a national policy issue that needs to be taken to the next tier beyond the conventional information technology governance to strategic frameworks that involve critical infrastructure protection and economic security and assurance of public safety. By aligning with overall cyber defense policies, automation security is created as an essential base capability to support the broader resilience goals, as attackers have continuously focused on the build systems, deployment pipelines, and orchestration platforms to reach their strategic goals such as service disruption, data exfiltration, and supply chain breach [9]. Conformance to data sovereignty efforts will see automation infrastructure respect jurisdiction, regulations and privacy protection, as well as operational efficiency across distributed systems. The principles of secure automation are integrated into digital resilience programs in national policies on infrastructure modernization, as it is clear that automation reliability directly reflects stability in society, economic sustainability, and the welfare of citizens in healthcare, transportation, financial services, and energy infrastructure.

B. Digital Resilience Centers of Excellence (DR-CoEs)

1. Mission and Structure

Digital Resilience Centers of Excellence foster ecosystems of collaboration among government agencies, private sector organizations, and academic institutions to drive research, development, and the dissemination of knowledge, helping to resolve automation security problems at scale. The concept behind public-private-academic partnerships is the ability of both policy expertise and operational experience to co-exist with fundamental research to create practical solutions to real-world resilience needs. Collaborative testbeds offer a regulated environment in which organizations test secure automation architectures, resilience mechanisms, and test emerging technologies prior to production deployment. Knowledge sharing processes broadcast best practices and incident lessons learned and technical advice that can guide the massive end-user embrace of the Digital Resilience Framework principles by organizations of differing maturity levels and resource limitations.

2. Core Activities

Simulations of large-scale automation failures and recovery operations are considered core activities that allow organizations to find weak points, test continuity plans, and enhance incident response capacity by simulating interdependent infrastructure systems with cascading disruptions. Open-source tooling the implementation of DRF is democratized through the development of reference architectures, reusable components, and integration frameworks, which minimize barriers to deployment by organizations that do not have the specialized expertise or large cybersecurity budgets. The training programs produce automation security experts capable of working with interdisciplinary skills across software engineering, cybersecurity, systems thinking, and policy analysis, which are needed to deploy resilient automation in critical infrastructure settings. Standardization initiatives further interoperable resilience frameworks that help to establish consistent security controls, shared assessment methods and compatible attestation across organizational boundaries and technology platforms.

C. Legal and Regulatory Mandates

1. Software Supply Chain Requirements

The regulatory requirements are also becoming increasingly focused on the mandatory publication of SBOM when software is used in situations of critical infrastructure to ensure transparency in the inventories of components used, their dependency relationships, as well as their known vulnerabilities to deployed systems [10]. Our digital signature requirements compel cryptographic verification of deployment artifacts, making it impossible to inject unauthorized code

and making attribution of software packages to approved publishers possible. Third-party audit and verification procedures have established independent evaluation procedures that confirm an organization has implemented the essential security controls, maintains proper documentation, and adheres to industry standards in secure automation practices.

2. Liability and Accountability Frameworks

Legal systems of responsibility define the accountability of any automation-related event and stipulate the duties of organizations that create, implement, and use automated systems that impact the security of the people and other essential services. Insurance schemes accommodate systemic automation failures through risk pooling across the industry, providing incentives to make security investments based on premium structures that reward the ability to demonstrate such resilience. Whistleblower protections of the whistle blowers also promote the reporting of security-related issues by protecting individuals who point out incompetence, insubordination or poor security-related measures in the organizations involved in the provision of important automation infrastructure.

D. Global Frameworks and International Cooperation

1. European Union NIS2 Directive (2022)

The NIS2 Directive increases cybersecurity requirements in vital and critical organizations and introduces a thorough knowledge of supply chain security risk management, mandatory reporting of incidents within and within the rigid time limits, and the interchange of information to enhance collective protection against threats to the automation of critical infrastructure.

Policy Domain	Strategic Focus	Implementation Requirements	Expected Outcomes
National Policy Priority	Critical Infrastructure Protection, Economic Security, Public Safety	Integration with Cyber Defense, Data Sovereignty Alignment	Societal Stability, Economic Continuity, Citizen Welfare
Legal Mandates	Software Supply Chain Transparency	Mandatory SBOM Publication, Digital Signatures, Third-party Audits	Unauthorized Code Prevention, Publisher Attribution
Liability Frameworks	Automation Incident Accountability	Legal Responsibility Definition, Insurance Mechanisms, Whistleblower Protections	Security Investment Incentives, Risk Pooling

Table 4: Policy Integration and Governance Frameworks [9]

VI. Implementation Considerations and Challenges

A. Technical Implementation Barriers

The integration of legacy systems is a daunting task with organizations trying to integrate new security frameworks into decades-old infrastructure that has been developed with technology that is outdated and old technology, which does not align with the current threat models and security structures. Such systems frequently lack cryptographic features, standard interfaces, and loggers to support a zero-trust design, so large-scale retrofitting or a gradual transition plan between continuity and improvements to security needs is often required. There is a performance overhead of performing continuous verification and monitoring, and cryptographic signature validation, provenance checking, and real-time compliance scan may add latency to automation workflows, thereby reducing throughput in high-velocity deployment settings. Binary Authorization of Borg at Google shows how massive production systems can apply code provenance verification and identity management, putting in place systems that ensure that any binary deployed in a distributed infrastructure is provenanced to be of known origin and that it will continue to be unaltered throughout the deployment lifecycle [11]. The complexity of multi-cloud/hybrid infrastructure orchestration grows exponentially because organizations need to administer workloads on heterogeneous platforms such as public cloud providers, private data

centers, and edge computing environments, each with its own authentication mechanisms, policy enforcement models, and security control implementations, which require coherent governance structures. The lack of skills in secure automation engineering limits the speed of implementation, as the number of requirements to hire professionals with interdisciplinary knowledge of software development, cybersecurity, infrastructure management, and compliance greatly outstrips the number of available employees. This leads to talent competition and pay inflation in sectors with critical infrastructure needs.

B. Organizational and Cultural Challenges

The conflict between the need to adhere to security requirements and the pace of development has created a continuous tension within the organization, where business needs are pushing the development of features at a very high rate, and security controls are adding verification and approval processes and testing requirements that increase deployment times. The culture of security consciousness among DevOps organizations must be based on fundamental changes in mindset where security can be viewed as a constraint rather than an essential part of engineering excellence and where the sustenance of the leadership commitment and incentive scheme as well as educational programs, should prove the business value of security. Zero-trust adoption change management is fraught with a set of assumptions about the network boundaries and trusted zones, and implicit models of authorization and needs a thorough update of the policy, workflow architecture and technology deployment that is planned and carried out across various departments with conflicting priorities and resource limitations.

C. Economic and Competitive Considerations

DFR implementation cost-benefit analysis is a problem in measurement because security investments are more likely to prevent losses than to produce revenue, and it involves complex "modeling of benefits and losses that uses pain prevention costs in the negative, the causes of reputational protection values, and regulatory compliance advantages after costs of installation. Studies of data breach economics indicate that security incidents cause significant direct expenses such as incident response, forensic investigation, legal expenses and regulatory fines, and indirect expenses such as customer loss, reputational loss, and operational disruption that together render proactive security investment justified [12]. There are still no market incentives for transparent and secure automation, which is not developed without mechanisms that allow customers to distinguish among providers on the basis of verifiable security practices.

Conclusion

Secure automation has become the parsimonious requirement of digital public safety in modern societies, where the critical infrastructure sectors rely on the constant integration pipelines, coordination platforms, and programmed control systems to provide the vital services that touch billions of individuals across the world. The paper confirms that the issue of infrastructure reliability has evolved beyond the conventional information technology issues and has become an issue of societal resilience and national security and therefore needs extensive frameworks that interrelate engineering practices with quantifiable safety outcomes and policy-level goals. The Digital Resilience Framework offered below gives a structured roadmap to the realization of reliable automation via five related pillars that include the use of secure automation cores to accomplish zero-trust architectures and cryptographic provenance, governance to ensure transparency and public auditability, resilience engineering practices, such as incorporating redundancy and chaos testing, AI-enhanced monitoring to provide predictive failure analysis and ethical automation frameworks to keep human oversight and regulatory alignment. Application of these principles requires that automation security be treated like civic infrastructure, and it be governed in a manner consistent with collective governance, standardization, and ethical review, as with other engineering professional fields that determine physical infrastructure that forms the basis of modern civilization. This paradigm shift in the perception of automation as a corporate information technology tooling to one of a common infrastructure that it must be jointly owned by government, industry, and civil society is core to the transformation in the way that democratic societies treat digital transformation and the governance of technology. The urgent plans involve setting up Digital Resilience Centers of Excellence that promote cross-sector collaboration, introducing compulsory software supply chain transparency demands, developing professional certification schemes to automation security specialists, and investing in open-source software to democratize access to secure automation frameworks inside firms with different resource limits and technical stages of development. The Future research directions include autonomous resiliency modeling, where systems dynamically adapt security postures in response to emerging threats, explainable AI frameworks, which can provide transparency to high-stakes automated decision-making

with an impact on public safety, and policy-aware orchestration systems, which incorporate regulatory requirements directly into automation logic to continuously verify compliance. The imminence with which society faces the challenge of automation security is compounded by the fact that more and more, societies are becoming reliant on digital infrastructure that mediate access to healthcare, financial provision, transportation, and energy resources, which places not only the opportunity, but the responsibility, upon current generations to lay the groundwork upon which populations can trust their systems to be both reliable and secure when serving the greater social good, but which they must also, to the extent that they can, safeguard fundamental rights, privacy, and democratic values in an increasingly automated world.

References

[1] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," U.S. Department of Homeland Security. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[2] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[3] Bank for International Settlements, "Fast payments – Enhancing the speed and availability of retail payments," 2016. [Online]. Available: https://www.bis.org/cpmi/publ/d154.pdf

[4] Keith Stouffer et al., "NIST Special Publication 800-82 Rev. 3: Guide to Operational Technology (OT) Security," National Institute of Standards and Technology, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[5] Blackduck, "2024 Open Source Security and Risk Analysis Report,". [Online]. Available: https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html

[6] Cloud Security Alliance, "Top Threats,". [Online]. Available: https://cloudsecurityalliance.org/research/topics/top-threats

[7] European Union Agency for Cybersecurity (ENISA), "Guidelines for Securing the Internet of Things: Secure Software Development Lifecycle,". [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[8] National Telecommunications and Information Administration, "Software Bill of Materials (SBOM),". [Online]. Available: https://www.ntia.gov/page/software-bill-materials

[9] Federal Register, "Improving the Nation's Cybersecurity," May 2021. [Online]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[10] Cybersecurity and Infrastructure Security Agency, "Software Bill of Materials (SBOM),". [Online]. Available: https://www.cisa.gov/sbom

[11] Google Cloud, "Binary Authorization for Borg: How Google verifies code provenance and implements code identity," 2020. [Online]. Available: https://price2meet.com/gcp/docs/security_binary-authorization-for-borg.pdf

[12] IBM and IBM Security, "Cost of a Data Breach Report," 2025. [Online]. Available: https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

[13] Jen Easterly, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," CISA, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years