INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

IGF Internet Governance Forum

Dear colleague,

You are invited to comment on the draft version of a report that will be presented at the XXth Internet Governance Forum in Lillestrøm, Norway in a launch workshop on Tuesday 24 June at 09.00 hour CEST in Workshop Room 6. The document is open for comments until **Wednesday 11 June 23.59 UTC**.

In this document the United Nations' Internet Governance Forum Dynamic Coalition Internet Standards, Security and Safety (IS3C) presents the outcomes and recommendations of its research conducted in close cooperation with the French internet registry Association Française pour le Nommage Internet en Coopération (Afnic).

The draft report addresses the critical intersection of emerging threats around Internet of Things (IoT) security and post-quantum cryptography (PQC). With an estimated 75 billion connected devices projected by 2025, the rapid expansion of IoT has introduced unprecedented connectivity but also heightened security vulnerabilities, regulatory challenges, and ethical concerns. The advent of quantum computing further complicates this landscape by posing a significant threat to current cryptographic systems, necessitating proactive, forward-looking strategies.

IS3C looks forward to your views on this topic.

Kind regards,

Wout de Natris - van der Borght

Coordinator IS3C

Table of Contents

Socio-political Impacts of IoT and PQC Policies

Executive Summary

This report, a collaborative study by the United Nations Internet Governance Forum's Dynamic Coalition Internet Standards, Security, and Safety Coalition (IS3C) and the French Association for Cooperative Internet Naming (Afnic), addresses the emerging threats around Internet of Things (IoT) security and post-quantum cryptography (PQC). With an estimated 75 billion connected devices projected by 2025, the rapid expansion of IoT has introduced unprecedented connectivity but also heightened security vulnerabilities, regulatory challenges, and ethical concerns. The advent of quantum computing further complicates this landscape by posing a significant threat to current cryptographic systems, necessitating proactive, forward-looking strategies.

The study starts with a comprehensive analysis of existing IoT vulnerabilities, including the pervasive issue of insecure devices leading to large-scale cyberattacks (e.g., Mirai botnet, Jeep Cherokee hack, St. Jude Medical cardiac device hack). It highlights how a lack of standardized security regulations, weak default credentials, outdated firmware, and human factors contribute to widespread vulnerabilities. Furthermore, the report emphasizes the critical risk posed by supply-chain attacks on IoT cloud infrastructure, where a single breach can compromise vast numbers of devices.

The report then maps the global, regional, and national policy landscapes, detailing initiatives from the European Union (e.g., Cyber Resilience Act, EN 18031-1/-2/-3:2024 series), the United Kingdom (NCSC guidelines), France (ANSSI, Cyber-score Act), the United States (NIST PQC Standardization Project, Quantum Computing Cybersecurity Preparedness Act), South Korea, Singapore, and Saudi Arabia. It underscores the IETF's role in defining global cryptographic standards for IoT security, including hybrid cryptographic modes and lightweight key exchange mechanisms.

The report provides a comprehensive overview of the PQC policy landscape in the US and EU and shows distinct yet converging approaches. The United States, driven by National Security Memorandum 10 and the Quantum Computing Cybersecurity Preparedness Act, has adopted a more mandated, top-down approach, with NIST leading the standardization of PQC algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium) and setting a 2035 target for federal system migration. In contrast, the European Union's strategy, while politically weighty, is currently more recommendation-based, leveraging existing cybersecurity governance structures like the NIS Cooperation Group to coordinate national strategies and promote hybrid cryptographic schemes.

Several EU Member States, including France (ANSSI advocating hybrid solutions and a three-phase transition), Germany (BSI providing guidance and participating in the QUANTITY project), and the Netherlands (publishing "The PQC Migration Handbook"), have also launched proactive national programs, demonstrating a shared commitment to PQC readiness. Both regions emphasize public-private collaboration and international coordination to ensure a harmonized and effective global transition to quantum-resistant security, recognizing the shared imperative to protect critical digital infrastructure.

The report also emphasizes the social, legal, economic, and environmental implications of the PQC transition. Societally, PQC is crucial for maintaining trust in digital infrastructure, preserving long-term privacy against "harvest now, decrypt later" attacks, and securing critical services. Legally, data protection regulations like GDPR may soon compel the use of quantum-resistant encryption. Economically, while the transition will incur significant costs for upgrading systems and hardware, delaying it would lead to much higher costs from potential quantum-enabled breaches. Environmentally, PQC could increase energy consumption due to more complex algorithms and potentially contribute to e-waste if devices cannot be upgraded, though it also indirectly supports digital transformations with environmental benefits.

The report concludes with strategic recommendations for national governments, regulators, industry, and service providers. Key recommendations include:

- **For Governments and Regulators**: Developing national PQC roadmaps with clear timelines, fostering public-private partnerships, funding PQC research and talent, mandating or incentivizing crypto-agility, leveraging public procurement also with a focus on IoT devices, raising national awareness, addressing cybersecurity workforce gaps, updating legal frameworks, and promoting international collaboration.

- **For Industry and Service Providers**: Creating comprehensive cryptographic inventories for IoT devices, developing quantum-readiness plans and phased PQC migration roadmaps, performing risk assessments and prioritization, adopting hybrid solutions during the interim, and piloting and testing PQC implementations. Specific to IoT, recommendations include integrating quantum-resistance into "security by design," developing lightweight PQC algorithms, and utilizing hardware acceleration.

Ultimately, the report stresses the urgent need for a coordinated, multi-stakeholder approach to transition to PQC, ensuring the long-term security, resilience, and privacy of the rapidly expanding IoT ecosystem against future quantum threats.

Part 1

2. Introduction

The rapid expansion of the Internet of Things (IoT) has started in an era of unprecedented connectivity, fundamentally reshaping global communication, industry, and daily life. With an estimated 75 billion connected devices projected by 2025, IoT is increasingly integrated into critical infrastructure, healthcare, smart cities, and industrial automation[1]. However, this digital transformation raises heightened security vulnerabilities, regulatory challenges, and ethical concerns that require urgent attention. As the digital landscape evolves, the emergence of quantum computing further complicates the security paradigm, necessitating forward-looking strategies to ensure resilience against post-quantum cyber threats.

This report of a collaborative study between the UN Internet Governance Forum's Internet Standards, Security, and Safety Coalition (IS3C) and the French Association for Cooperative Internet Naming (Afnic), examines the critical intersection of IoT security and post-quantum cryptography (PQC). It provides a comprehensive analysis of existing vulnerabilities, assesses policy and regulatory frameworks' responses, and offers strategic recommendations to enhance security at the national and international levels. By addressing current cybersecurity challenges and the long-term implications of quantum computing, this study contributes to ongoing global efforts to build a secure, inclusive, and sustainable digital environment.

2.1 Scope and Objectives

This study critically examines the current state of IoT security, identifying systemic vulnerabilities and their broader implications for privacy, trust, and societal stability. IoT security lapses have resulted in large-scale cyberattacks, data breaches, and threats to critical infrastructure. The study assesses existing security policies and regulatory measures, analyzing their effectiveness in mitigating risks across different sectors and regions. It further explores the role of consumer protection mechanisms, industry standards, and cross-border cooperation in strengthening the provision of security in IoT ecosystems.

As quantum computing advances, its potential to compromise widely used cryptographic protocols poses a significant challenge. This study evaluates the implications of post-quantum cryptography (PQC), examining policy developments in key regions such as the European Union and the United States, and highlights the need for coordinated global efforts to integrate PQC into IoT security frameworks, ensuring a seamless transition that minimizes risks while maintaining interoperability.

Following the technical and policy analysis, the study provides strategic recommendations for government policymakers, industry leaders, and international organizations. It advocates harmonized security standards, enhanced regulatory oversight, and the promotion of a security-first culture in IoT development and deployment. Recognizing the diverse security capabilities of legacy and next-generation IoT devices, it emphasizes the need for tailored approaches that balance security, innovation, and inclusivity.

2.2 Relevance and Significance

The urgency of enhancing IoT security cannot be overstated. The proliferation of inadequately secured IoT devices has led to widespread vulnerabilities, including botnet-driven cyberattacks, unauthorized data exploitation, and threats to public safety. Concurrently, the accelerating progress of quantum computing necessitates a proactive approach to cryptographic transition, as current encryption standards may soon become obsolete. The convergence of these challenges requires a comprehensive strategy that not only addresses immediate threats but also future-proofs security mechanisms against quantum-era risks.

This study serves as a resource for government and business decision-makers, technical experts, and regulatory bodies, offering evidence-based insights and actionable strategies to safeguard IoT ecosystems. By fostering international collaboration, it seeks to mitigate risks, enhance resilience, and contribute to a secure digital future that aligns with broader goals of sustainable development and global cybersecurity governance.

3. Internet of Things (IoT) Security

The increasing adoption of smart home devices has introduced new security challenges, making these environments attractive targets for cyberattackers. Unlike traditional IT systems, smart homes consist of heterogeneous IoT devices that communicate over various protocols, often with limited security mechanisms. The devices usually handle very sensitive personal and even non-personal data, which, if accessed, can contribute to vulnerabilities at both individual and community levels.

Such data can include personal health data, community religious information, and even trade secrets at an industrial and national scale. For example, the Mirai botnet attack of 2016 disrupted critical Internet services, causing major disruptions.[2] It primarily targeted consumer IoT devices such as IP cameras, home routers, and digital video recorders (DVRs). The botnet exploited the fact that many IoT devices used default or weak passwords. It scanned the Internet for vulnerable devices and then used a table of common default passwords to gain access. At its peak, the Mirai botnet infected over 600,000 IoT devices, turning them into a network of bots. The infected devices were used to launch massive Distributed Denial of Service (DDoS) attacks against various targets, including DNS provider Dyn, which resulted in widespread Internet outages. This attack inspired several other attackers to this day.

In the automotive sector, the 2015 Jeep Cherokee hack exposed the risks of connected vehicles, leading to a recall of 1.4 million vehicles[3]. The attack focused on the Jeep Cherokee's Uconnect infotainment system, which acted as an IoT gateway in an Internet-connected feature of the vehicle. Researchers Charlie Miller and Chris Valasek discovered they could remotely access the Jeep's systems through the Uconnect feature's cellular connection. Once they gained access, they could control various features of the car, including its air conditioning, radio and windshield wipers, and even disable the brakes and transmission.

The St. Jude Medical Cardiac devices hack exemplifies how IoT vulnerabilities can have life-threatening implications in medical contexts. The affected devices were implantable cardiac defibrillators and pacemakers which are in effect IoT devices by design because they have wireless connectivity in order to facilitate remote monitoring and adjustment by healthcare providers. The devices used a proprietary radio frequency protocol called "Merlin@home" to communicate with a home transmitter, which then connected to St. Jude's servers over the Internet.

In 2016, the cybersecurity firm MedSec and investment research firm Muddy Waters reported vulnerabilities in these devices.[4] The researchers found that the devices' communication protocol lacked proper authentication and encryption. This could potentially allow an attacker within radio range to intercept and manipulate communications between the device and its monitoring equipment. Attackers could potentially a) drain the device's battery faster than normal; b) alter the device's pacing or shock settings; and c) access

sensitive patient information stored on the device. Approximately 465,000 patients in the U.S. had these potentially vulnerable devices implanted. The US Food and Drug Administration (FDA) confirmed the vulnerabilities in January 2017, leading to a recall in order to update the devices' firmware.[5] Unlike many IoT devices, updating implanted medical devices is complex and risky, making it difficult to patch vulnerabilities quickly. The company also had to enhance its cybersecurity monitoring and response practices.

These incidents illustrate the pervasive nature of IoT vulnerabilities and their potential to cause significant social disruption and economic damage, with costs often amounting to hundreds of millions of dollars across various industries and public spaces. A primary driver of these vulnerabilities is an inherent weakness in IoT security mechanisms because many of these devices are designed primarily with efficiency and affordability in mind, often at the expense of robust security measures. They have restricted processing power, memory, and battery life, limiting their ability to support strong encryption and authentication protocols. Additionally, the absence of standardized security regulations in the industry creates inconsistencies in security implementation[6]. The heavy reliance on Internet connectivity further expands the attack surface, exposing smart home networks to remote exploitation of security vulnerabilities and flaws, and unauthorized access.

Human factors also contribute to IoT security challenges. Low levels of cybersecurity awareness among users of industrial, personal, and smart-home IoT devices leads to poor security habits, such as weak passwords, default configurations, and neglected firmware updates. This was seen in incidents involving botnets like Mirai and Mozi, where the combination of default credentials and outdated firmware provided effortless access for attackers, emphasizing the critical need for greater education, simplified user interfaces for security management, and automatic update mechanisms to mitigate human-related risks.

3.1 Current Security

There is currently a lack of global and regional harmonization of security standards regarding IoT. While several IoT devices can exist in single homes forming complex and heterogeneous smart home systems, these systems are developed by different manufacturers adhering to different standards, or, in some cases, no standards at all. This makes it difficult to achieve security system harmonization within a home environment.

Existing literature often focuses on isolated cases rather than comprehensive approaches to IoT security across different devices and applications. While policies and technical standards exist that could be applied to IoT security, they must be mapped out to identify specific gaps. These standards include data and information security policies, cybercrime policies criminalizing unauthorized access, and data protection principles that position users in the centre of the information-processing ecosystem. However, challenges remain, particularly in implementing existing policies effectively and mitigating the overwhelming increase in the

IoT attack surface which limits the capacity for safeguards. The heterogeneity of standards across the IoT industry further compounds these issues.

To appreciate the urgency of fortifying IoT security, it is useful to look at how vulnerabilities have been exploited by threat actors on a large scale. IoT botnets, networks of compromised devices such as cameras, routers, and other smart devices, illustrate the ease with which unprotected systems can be hijacked for malicious ends. Early examples like the Mirai botnet leveraged default or weak credentials to orchestrate massive distributed denial-of-service (DDoS) attacks. Similarly, the Mozi botnet capitalized on poor authentication mechanisms to gain persistence in IoT networks.

By examining botnets such as Mirai, Matrix, Raptor Train, VPN Filter, Hide n' Seek, and Mozi, we see how fundamental security flaws, ranging from outdated firmware to the absence of encryption, can be turned against end-users and organizations alike, prompting a renewed focus on firmware integrity, patching protocols, and international coordination.

Mirai

Mirai is the most relevant case of IoT botnets for three reasons: impact, accessibility, and adaptability. First unleashed in 2016, the malware's ability to conscript hundreds of thousands of poorly secured cameras and routers enabled record-shattering DDoS assaults that disrupted the widely-read cybersecurity blog KrebsOnSecurity, the cloud computing company OVH, and the Dyn DNS Internet domain names information and updating service, in an outage that crippled major sites across the United States.[7]

Within weeks, the authors of this malware published Mirai's source code on an underground forum, handing would-be attackers a ready-made toolkit that scans the Internet for IoT devices still running factory-default credentials or outdated firmware. Because the code was open and modular, threat actors could "plug-and-play" new exploits as soon as researchers disclosed them. That is why Mirai has more named variants than almost any other botnet family including Satori, Okiru, Moobot, RapperBot, BotenaGo, Wicked, and dozens more.[8] [9] Each iteration tweaks the original scanning logic or swaps in fresh common vulnerabilities and exposures (CVEs), keeping the malware relevant as vendors patch older bugs in the system. Recent examples show this cycle is continuing: an eight-month-old campaign is using an unpatched vulnerability in widely deployed CCTV cameras to expand a Mirai offshoot, turning surveillance devices into attack nodes and potential spying tools.[10]

Likewise, the cloud-based content delivery network Akamai used its intentionally insecure decoy systems (known as honeypots) to record Mirai operators exploiting two 2024 command-injection flaws in GeoVision[11] appliances. This was only days after their system bugs became public, underscoring how quickly new code could be folded into the Mirai "template."[12]

Mirai's importance therefore lies not just in the devastation caused by a single botnet but in the ecosystem it spawned. Its easily reused architecture, huge pool of still-unpatched IoT

endpoints, and proven money-making potential (from DDoS-for-hire to credential-harvesting add-ons) make it the default starting point for many modern IoT malware authors. Until manufacturers eliminate default passwords, guarantee timely firmware updates, and adopt secure-by-design principles, Mirai's lineage will continue to flourish, providing attackers with an ever-growing range of devices that can be weaponized for denial-of-service, espionage, or credential leaks that become stepping stones into other systems.

Matrix

First documented by Aqua Nautilus cybersecurity researchers in November 2024, the Matrix campaign demonstrates how readily available scripts and default passwords can be combined to conscript into a single distributed-denial-of-service (DDoS) platform vast numbers of poorly protected IoT devices, ranging from home routers and IP cameras to lightly secured enterprise servers.. By systematically scanning the Internet for devices that still use factory credentials or remain unpatched against well-known vulnerabilities,[13] the operator can automate infection, command-and-control enrolment, and attack execution with minimal cost and basic technical knowledge.[14]

Raptor Train

Uncovered by Lumen's Black Lotus Labs in September 2024, Raptor Train is considered by their researchers to be one of the largest China-linked IoT botnets observed so far. They attributed the operation to the state-sponsored "Flax Typhoon" advanced persistent threat (APT) which targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan. They did this after tracing a multi-tier command-and-control (C2) architecture that had infected hundreds of thousands of small-office/home-office (SOHO) and other IoT devices worldwide, routers, network-attached storage (NAS) units, NVR/DVR video recorder camera systems, and IP cameras.[15]

The malware (a Mirai-derived variant) uses "brute-force" trial-and-error attacks against weak credentials and exploits unpatched vulnerabilities to gain persistence. Once implanted, each device becomes a proxy node in a covert network used to relay espionage traffic, harvest credentials, and transfer sensitive data to infrastructure controlled by the operators, while also offering DDoS capability on demand. U.S. court documents released in early 2025 describe how the botnet provided cover for broader cyber-intrusion campaigns and how a joint FBI/Department of Justice operation remotely removed the malware from more than 200,000 U.S. devices, cutting communications with the C2 layer without affecting device functionality.[16]

VPN Filter

VPN (virtual private network) Filter highlights the evolution of IoT malware into sophisticated frameworks that embed advanced spying functions[17]. More than just a typical botnet, VPN Filter's modular design gives attackers the capability to extract sensitive data, manipulate web traffic, and even render devices inoperable through destructive commands. By exploiting outdated firmware and default credentials on a wide range of network appliances,

VPN Filter can remain persistently hidden and gather information from unsuspecting home users and small businesses alike, turning compromised devices into long-term surveillance platforms.[18]

Hide n' Seek (HMS)

Initially discovered in early 2018, the Hide n' Seek IoT botnet relies for spreading on a peer-to-peer communication infrastructure that continually mutates to evade detection. Its primary tactic is to intercept or passively observe user activity on infected IoT devices such as cameras and digital video recorders (DVRs). The data captured can be used for targeted espionage, identity theft, and unauthorized monitoring of consumer or enterprise environments. Hide n' Seek's stealthy propagation mechanisms demonstrate how quickly a botnet can extend its monitoring capabilities across millions of endpoints once a single vulnerability is exploited.[19]

Mozi

Mozi operates by leveraging known weak points in routers and cameras, ultimately performing both data transfers and denial-of-service attacks[20]. After gaining a foothold, the botnet can siphon personal or proprietary data from home networks and small offices, relaying it to remote attackers who can then monetize or further exploit the harvested information. Mozi's capacity to remain active in embedded systems for extended durations illustrates a troubling trend: once an IoT device is compromised, it can silently extract and transfer sensitive data without immediate detection.

Many of the compromised devices compromised by botnets capture and store personal data. As the above examples reveal, attackers can exploit insecure devices to extract sensitive information user credentials, often weaponizing this data to spy on targets or gain access to other systems. In doing so, they pose direct threats to users' privacy and autonomy, potentially using stolen data against the very individuals who rely on IoT devices for convenience and connectivity.

3.1.1 Supply-Chain Attacks on IoT Cloud Infrastructure

When we talk about Internet-connected devices today, we are not just referring to the hardware in a consumer's living room or on an industrial shop floor. Most IoT products rely on a vendor-operated cloud service for pairing, authentication, data storage, and remote control. Even when the user and the device are in the same room, every command is typically routed through this shared backend. That architectural convenience creates a single, high-value target: if attackers breach the IoT connectivity platform or any vendor-managed backend, every device enrolled in that service instantly becomes vulnerable. One successful intrusion can therefore cascade across an entire personal network or business operation, leaking information, propagating malware automatically, and

embedding persistent footholds on end-points long after the cloud compromise is discovered and contained.

The 2021 Verkada security camera breach exemplifies the far-reaching consequences of IoT server vulnerabilities.[21] Hackers exploited exposed administration credentials to gain “super-admin” high level access to Verkada's systems, compromising live feeds and archives from 150,000 cameras in sensitive locations such as hospitals, schools and police departments. This single point of failure affected thousands of organizations and individuals, exposing the risks of this kind of centralized IoT ecosystem. The incident resulted in multiple lawsuits and potential fines for Verkada under the EU’s General Data Protection Regulation (GDPR), with ongoing financial repercussions. This case starkly illustrates how a seemingly minor security oversight in IoT infrastructure can lead to widespread privacy violations and significant legal and economic consequences. ThroughTek’s IoT platform Kalay SDK based in Taiwan powers remote access, firmware updates, and video streaming for over 100 million consumer cameras and baby monitors worldwide. The cybersecurity technology company Bitdefender identified four chained CVE vulnerabilities[22] that let an attacker move from the Kalay cloud to any enrolled device, obtain authentication keys, and ultimately gain root shell user interface access, all without users’ involvement. Because dozens of brands (Owlet, Wyze, Roku, etc.) simply embed the SDK platform, one unpatched library version became a systemic liability: compromising the platform once meant silently installing backdoors across many product lines at scale.[23]

The Verkada and ThroughTek incidents reveal a hard truth: in the IoT era, the security perimeter often goes well outside the customer’s premises. A single weakness in a cloud control plane or third-party SDK can compromise tens of thousands of otherwise isolated devices, turning convenience into collective exposure.

Effective defence, therefore, begins upstream. Vendors must treat their cloud infrastructure and software supply chain with the same rigor traditionally reserved for on-device security: continuous penetration testing, zero-trust access controls, signed firmware and update pipelines, and a transparent Software Bill of Materials (SBOM) for every component they ship.

Regulators, meanwhile, should incentivize timely patching and breach disclosure, ensuring that the burden of security does not rest solely on end-users who have little visibility into back-end risks. Only by hardening the connective tissue that links devices to the Internet can we prevent the next “single point of failure” from cascading into a global privacy, safety, and financial crisis.

3.2 The Global, Regional, and National Policy Landscapes

Several countries and international organizations have introduced regulations and standards since 2022 aimed at strengthening IoT security and addressing the fragmented landscape of cybersecurity policies. These efforts focus on standardization, security labelling, and compliance frameworks to ensure consumer protection and industry accountability. Below is an overview of the most relevant IoT security policies and initiatives across different regions.

3.2.1 International Standards and Guidelines

ISO/IEC 27400:2022: Provides foundational security and privacy principles for IoT solutions, outlining risk management strategies for manufacturers and service providers.

ISO/IEC 27402:2023: Establishes baseline security requirements for IoT devices, ensuring compatibility with global cybersecurity frameworks.

ETSI EN 303 645: Developed by the European Telecommunications Standards Institute (ETSI), this standard sets a cybersecurity baseline for consumer IoT devices, widely recognized as a model for future IoT certification schemes.

1. **European Union**

EN 18031-1/-2/-3:2024 series specifies cybersecurity requirements for radio equipment, ensuring network protection, data privacy, and fraud detection. The regulation comes into force on 1 August 2025.

Cyber Resilience Act (Regulation 2024/2847): Mandates security-by-design requirements for digital products, including IoT devices, and requires regular security updates.

Delegated Regulation (EU) 2022/30: Introduces new cybersecurity requirements for radio-connected IoT devices, ensuring improved resilience against attacks. This entered into force on 1 February 2022, but its requirements become binding on 1 August 2025.

2. **United Kingdom**

The UK's approach to PQC for IoT is integrated in its broader strategy to counter future threats. Spearheaded by the UK's National Cyber Security Centre (NCSC), the primary policy is outlined in guidance such as '*Timelines for migration to*

post-quantum cryptography.[24] This framework sets a 2035 deadline for transitioning all systems, including IoT, to PQC standards. While not a separate IoT-specific policy, the NCSC's guidelines acknowledge the unique challenges for IoT, such as long device lifecycles and resource constraints, and emphasize vendor responsibility for updates to commodity devices. The strategy encourages early planning, cryptographic discovery, and alignment with international standards like those from NIST to ensure a secure transition for the IoT sector.

3. **France**

The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) which is responsible for setting cybersecurity standards, conducting assessments, and providing expert guidance, issued strategic recommendations advocating a hybrid approach that combines classical and post-quantum cryptographic methods. In 2021, it also promoted the adoption of algorithm-resistant algorithms that can be deployed on existing digital systems.

France introduced a 'cyberscore', established through the Cyber-score Act, mandating cybersecurity certification for public-facing digital platforms to provide consumers with a clear security rating to inform their choices. Initially targeting the largest merchant websites, it requires audits by ANSSI-qualified providers, resulting in a visual label indicating the platform's security and data practices. With the publication of products' cybersecurity provision, particularly regarding IoT products, consumers can grade the reliability of the digital services they use, fostering greater awareness to protect themselves.

4. **United States**

NIST (Cybersecurity for IoT Program: A framework by the National Institute of Standards and Technology (NIST) providing tailored security guidelines for consumer IoT products.

U.S. Cyber Trust Mark (2025): A voluntary labelling programme indicating whether IoT devices comply with cybersecurity best practices, including secure data transmission and software updates.

5. **South Korea**

South Korea: Certification of IoT Cybersecurity (CIC): A three-tier cybersecurity certification system ensuring IoT security across smart homes, healthcare, finance, and industry.

6. **Singapore**

Singapore: Cybersecurity Labelling Scheme (CLS): A four-level rating system helping consumers assess IoT device security, encouraging manufacturers to implement stronger cybersecurity practices.

Singapore-Germany MRA (2024): Extended cybersecurity labelling recognition for Wi-Fi routers, smart cameras, and health IoT devices, improving cross-border security compliance.

Singapore-South Korea: KISA-CSA Mutual Recognition Arrangement (2023): South Korea's KISA and Singapore's Cyber Security Agency (CSA) signed an MRA to recognize each other's IoT security certifications.

7. **Saudi Arabia**

The Communications, Space and Technology Commission (CST) revised national IoT regulations to enhance security, promote investment, and improve regulatory oversight for smart devices.

3.2.2 Role of the IETF in IoT and PQC Standardization

In parallel to national and regional regulations, the Internet Engineering Task Force (IETF) plays a key role in defining global cryptographic standards for IoT security. Between 2024 and 2025, the Crypto Forum Research Group (CFRG) and relevant working groups including the TLS (transport layer security) WG, the LAKE (Lightweight Authenticated Key Exchange) WG and the SUIT (software updates for IoT) WG, have advanced protocols that integrate both post-quantum and lightweight cryptography into constrained environments. Notable initiatives include:

- Hybrid cryptographic modes for TLS 1.3, enabling simultaneous use of classical and post-quantum algorithms[25].
- Lightweight key exchange and secure firmware update mechanisms through LAKE and SUIT, designed for resource-limited IoT systems[26].

To facilitate a smooth migration to post-quantum cryptography (PQC), cryptographic agility frameworks are being proposed. For example, the IETF's Internet-Draft draft-reddy-uta-pqc-app outlines a quantum-resistant profile for **TLS** and **DTLS 1.3**[27], recommending hybrid key exchange mechanisms, post-quantum certificates, and deployment strategies to enable PQC integration into secure communication protocols while maintaining interoperability with existing infrastructure.

The IETF works closely with NIST to ensure that algorithms like Kyber and Dilithium, selected by NIST for standardization, are accompanied by interoperable protocol designs across TLS, IPsec, and DNSSEC (Domain Name System Security Extensions). This alignment ensures future-proof, scalable integration of PQC into real-world IoT deployments.

3.2.3 Global Compliance and Future Trends

Manufacturers are gradually being encouraged to align their IoT products with global cybersecurity standards in order to ensure regulatory compliance and maintain market access. While progress is slow, there is a clear shift towards strengthening digital trust, with policies increasingly emphasizing security by design, transparency in data handling, and standardized cybersecurity labelling. Additionally, as quantum computing advances, support for adopting post-quantum cryptography (PQC) for IoT security is gaining traction, though widespread implementation remains at an early stage. Stricter compliance enforcement and international cooperation are expected to play an increasing role in shaping a resilient, future-proof IoT ecosystem over the coming years.

3.3 Social Implications

Widespread IoT vulnerabilities, often originating from inadequate security measures and the massive proliferation of connected devices, have far-reaching social consequences that go well beyond technical or economic domains. IoT botnets, which harness these vulnerabilities to hijack networks of compromised devices, exemplify how insecure infrastructures can erode public trust, disrupt daily life, and threaten essential services.[28]

There are four key aspects of these social consequences.

Firstly, the preponderance of insecure IoT devices worldwide enables large-scale cyber attacks that can have immediate, tangible impacts on society. Botnets such as Mirai and its variants have demonstrated the ability to take down major websites and online services, hampering communications and commerce for millions of users. When these attacks target critical infrastructure such as energy grids and transportation systems, they risk impeding access to essential goods and services, which in turn heightens social anxiety and undermines the reliability of increasingly digitized public utilities.

Secondly the prevalence of IoT vulnerabilities raises concerns about privacy and surveillance. As botnets infect a wide variety of consumer devices, ranging from cameras to wearable sensors, an attacker who gains unauthorized control can secretly collect data, monitor household activities, or even engage in blackmail. These intrusions affect not only the individual user’s sense of security but can also chip away at broader societal norms around data protection. Over time, recurring breaches can condition the public to accept surveillance or data compromise as inevitable, creating a climate of diminished autonomy and distrust.

Thirdly social inequalities can be exacerbated by IoT-based attacks. Communities with fewer resources to invest in robust devices or security updates become disproportionately vulnerable. This fosters a “digital divide” whereby individuals or regions lacking cybersecurity

awareness or funding face higher risks of compromise. Botnets rely on uniform, predictable weaknesses, often default passwords or unpatched software, and thus communities unable to maintain regular updates or adopt stronger security practices end up bearing the brunt of large-scale attacks.

Finally, the wave of IoT botnet incidents underscores a broader challenge of collective responsibility and governance. Because IoT devices are produced and deployed globally, any single weak point can become a launchpad for worldwide attacks. The sheer scale of botnets that leverage these vulnerabilities highlights the need for coordinated policy responses, stronger regulatory oversight, and cross-border collaboration. Addressing the social implications of IoT botnets, therefore, demands not solely technical fixes, such as better encryption or stronger authentication, but also user education, standardized security practices, and international frameworks aimed at encouraging device manufacturers to embed security by design.

Today's IoT botnets thrive in an environment of inconsistent device security and low user awareness. Their rise reveals how one compromised router or camera can threaten an entire ecosystem, from home networks to national infrastructure. These vulnerabilities can undermine public trust in connected technologies, generate privacy harms, and exacerbate societal inequalities if left unchecked. Consequently, addressing the social dimensions of IoT security is vital to cultivating an inclusive, stable digital future and ensuring that technological advances do not undermine the very communities they aim to serve.

3.4 Broader Privacy Threats and Emerging Concerns

Beyond these specific botnets, the very nature of IoT connectivity raises systemic privacy challenges. IoT devices in homes, hospitals, and industrial plants generate vast quantities of data, ranging from camera feeds to real-time health statistics, which if they are intercepted,provide a treasure trove for cybercriminals. Increasingly, state-sponsored attackers and organized crime groups see IoT networks as advantageous targets. Once they compromise them for surveillance, they can remain inside a victim's environment indefinitely, capturing continuous streams of sensitive personal or organizational information.

Moreover, because IoT manufacturers frequently prioritize time-to-market over robust security, devices often run outdated firmware and lack standardized encryption. These shortfalls allow attackers to intercept data in transit or undertake "man-in-the-middle" exploitation that feeds into larger surveillance networks. Compounding these issues is the user behaviour factor: consumers commonly neglect to update device passwords or firmware, creating persistent, widely distributed pockets of vulnerabilities that also support botnet expansion.

4 Policy Recommendations

Addressing the IoT's multifaceted risks requires coordinated efforts involving multiple stakeholder groups at the national, regional, and global levels, including consumers, the technology industry, standards developers, government policymakers, regulators, and parliamentarians. The following recommendations are designed to guide each audience towards building a more resilient and trustworthy IoT ecosystem in anticipation of forthcoming significant technological shifts. Specifically, they are categorised to address actions needed to empower consumers to protect themselves, actions needed for industry practice to protect consumers by default, policy actions at national levels, and policy actions that need international cooperation.

1. Recommendations for policy actions to enable consumers to protect themselves
    1. Governments should expand educational cybersecurity curricula to include IoT risks in the era of PQC.
    2. Governments and industry should engage with consumer advocacy groups for shared learning, support, and public coordination on cybersecurity initiatives.
    3. The government should require industry to develop simple reporting mechanisms for consumers as well as a cyber score index, including real-time notification about product anomalies and security flaws.
    4. Governments and other stakeholders such as the private sector and civil society should enhance protection awareness through disseminating regular guidance, updates and toolkits for consumers at grassroot levels.
2. Recommendations on actions needed for industry and governments to protect consumers by default are guided by the fact that even when they are aware of the risks, consumers may not always proactively defend themselves against cybersecurity incidents. Researchers working on consumer attitudes to cybersecurity report that despite users knowing and experiencing cyber vulnerabilities, they still maintain convenient behaviours and carelessly transact sensitive data, including personal financial data. This means that awareness policies should go hand in hand with security by design policies.
3. The study makes the following recommendations:
    1. Industry and governments (where governments are the providers of digital technology and services) should implement by default strong security, privacy protection, and ethical design in IoT products and services.
    2. Industry should establish well-coordinated and trusted certification schemes for consumer privacy and security.
    3. Service providers and app developers for IoT devices should limit data collection to service essentials. Depending on risks, data permissions outside services should be made illegal, even where consumer access is granted.
4. Policy actions at the national level:

    At national levels, governments should require industry adoption of recognised security, encryption, and authentication standards.

5. Transversal policies requiring international cooperation

1. Participate in joint protocols for rapid response in case of mass data breaches and product recalls. This can be done through cross-border cooperation platforms among Computer Emergency Response Teams (CERT) and regulators.
2. Advocate enhanced cooperation to help the least developed countries migrate to safer PQC security standards.

Part 2

4. Social Impacts of Post-Quantum Cryptography Policies

4.1. Introduction

Quantum computers pose a serious threat to current cryptographic systems. As these technologies advance, widely used public key algorithms like RSA and ECC risk becoming obsolete, jeopardizing sensitive data across government, finance, healthcare, and critical infrastructure. This report examines the emerging policies in the United States (US) and European Union (EU) aimed at facilitating the transition to post-quantum cryptography (PQC), and analyzes the societal, legal, economic, and environmental impacts of this transition. The report will also provide actionable policy recommendations for industry, governments, regulators and organizations, with a special focus on the Internet of Things (IoT).

Post-Quantum Cryptography (PQC), also known as quantum-resistant cryptography, refers to the development and deployment of cryptographic algorithms that are secure against attacks launched by both classical and quantum computers.[29] These algorithms are designed to run on existing classical computing infrastructure but are based on different mathematical problems believed to be hard for quantum computers to solve, including problems related to lattices, error-correcting codes, hash functions, and systems of multivariate polynomial equations.[30][31]

It is important to distinguish PQC from quantum cryptography. PQC focuses on creating new algorithms which are resistant to quantum attacks but implementable on classical computers. Quantum cryptography, conversely, leverages quantum mechanics directly for cryptographic tasks, such as Quantum Key Distribution (QKD), which uses quantum properties to securely exchange keys and detect eavesdropping.[32] While QKD offers theoretical security benefits, it typically requires specialized hardware and infrastructure, faces distance limitations, and is generally considered complementary to, rather than a replacement for, PQC for widespread application.[33]

The development and transition to PQC represent an important paradigm shift in cybersecurity. Unlike many previous cryptographic upgrades that responded to existing vulnerabilities or performance limitations, PQC is a proactive defense against a future and potentially catastrophic, threat.[34] This proactive stance is driven by the unique nature of the quantum threat and its potential to retroactively compromise data secured today. This forward-looking approach presents its own challenges for policymakers and organizations, requiring justification for investment and resource allocation against a threat that has not yet fully materialized but whose potential impact necessitates immediate preparation.

4.2. Mapping US-EU PQC Policies

This section maps the key post-quantum cryptography policies and government initiatives in the United States and the European Union. It highlights regulations, frameworks, and recommendations, including the European Commission's 2024 PQC roadmap recommendation and the U.S. NIST's 2024 algorithm standards release. Understanding these policies is crucial for grasping how different jurisdictions are preparing for the societal shift to quantum-resistant security.

4.2.1. United States PQC Policy Landscape

The United States has taken a strategic, multi-pronged approach to PQC, beginning at the highest levels of government. In May 2022, the White House issued **National Security Memorandum 10 (NSM-10)**, *"Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"*[35]. NSM-10 sounded an alarm about the risks to online security presented by quantum and set the stage for urgent migration to quantum-resistant cryptography. It explicitly stated that the U.S. "must prioritize the timely and equitable transition of cryptographic systems to quantum‑resistant cryptography, with the goal of mitigating as much of the quantum risk as feasible by 2035."

This goal was echoed in later guidelines and 2035 has been put forward repeatedly as a target date for having most systems migrated off quantum-vulnerable cryptographic systems.

Following NSM-10, the **Quantum Computing Cybersecurity Preparedness Act** was passed by Congress in December 2022[36]. This bipartisan legislation (Public Law 117-260) requires federal agencies to begin the process of migrating to PQC. It mandates the Office of Management and Budget (OMB) to oversee agencies' efforts and to report on progress, ensuring accountability in the transition to PQC. A key provision of the Act which is triggered as soon as NIST has completed its PQC standardization, compels agencies to act on those new standards. The Act also emphasized the importance of establishing an inventory of federal information systems using encryption that could be broken by a quantum computer, laying the groundwork for prioritizing critical systems[37].

In response to the Preparedness Act and NSM-10, the OMB issued Memorandum M-23-02 in November 2022, titled *"Migrating to Post-Quantum Cryptography."* This memo provides detailed instructions for federal executive branch agencies on how to kick-start the migration process. It requires agencies to **catalog their cryptographic assets** by creating a **prioritized inventory of cryptographic systems**[38]. Starting May 4, 2023, and recurring at least annually until 2035, agencies must identify systems that use cryptography which is vulnerable to a cryptanalytically relevant quantum computer (CRQC) and report these to OMB. The CRQC can be defined as a computer that is capable of breaking current cryptographic algorithms used for data security and protection. When it comes to High Value Assets (HVAs), the inventory should prioritize high-impact systems handling sensitive data are to be prioritized in this inventory process, in recognition of how critical information (e.g. classified data, critical infrastructure controls) must remain secure well into the future.

OMB M-23-02 also instructs federal agencies to **establish requirements for crypto agility and migration planning** in their security architectures. Agencies were encouraged to start **testing candidate PQC algorithms** (in cooperation with NIST and other bodies) even before the standards were finalized. The memo set a tone of urgency: given the time required to complete transition, certain preparatory steps must be undertaken to mitigate the risk of "harvest now, decrypt later" operations by adversaries. The OMB, coordinating with the Office of the National Cyber Director and the Department of Homeland Security (DHS), would later issue further guidance once NIST's standards were ready.

The National Institute of Standards and Technology (NIST) has been central to U.S. PQC efforts through its **PQC Standardization Project**. Launched in 2016, this project was a public competition inviting cryptographers worldwide to submit and vet candidate algorithms that could resist quantum attacks. After multiple evaluation rounds, NIST announced in July

2022 the first group of **“winner” algorithms** for standardization – notably **CRYSTALS-Kyber** (a key encapsulation mechanism for encryption) and **CRYSTALS-Dilithium**, **FALCON**, and **SPHINCS+** (digital signature schemes). These algorithms were selected based on security and performance, coming from families like lattice-based cryptography and hash-based signatures which are believed to be quantum-resistant.

In **August 2024, NIST officially released the first three PQC standards** as Federal Information Processing Standards (FIPS): **FIPS 203, 204, and 205**. FIPS 203 specifies a **Module-Lattice Key-Encapsulation Mechanism (ML-KEM)** for general encryption (derived from CRYSTALS-Kyber), FIPS 204 defines a **Module-Lattice Digital Signature Algorithm (ML-DSA)** for authentication (based on CRYSTALS-Dilithium), and FIPS 205 describes a **Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)** (related to the SPHINCS+ scheme)[39]. A fourth standard, FIPS 206: Falcon Digital Signature Algorithm (FN-DSA), based on the FALCON algorithm (another lattice-based scheme offering potentially smaller signatures but with greater implementation complexity), is expected to be used for digital signatures.

In **March 2025, NIST announced the selection of Hamming Quasi-Cyclic (HQC)** as the fifth algorithm to be standardized.[40] HQC is a Key Encapsulation Mechanism (KEM) based on error-correcting codes, providing a different mathematical foundation than the lattice-based ML-KEM. It is intended as a backup standard for general encryption, offering an alternative should vulnerabilities be discovered in ML-KEM. A draft standard for HQC is expected around March 2026, with finalization anticipated in 2027. This selection of a backup based on different mathematics underscores the inherent uncertainties in a new cryptographic era and reinforces the need for long-term crypto-agility, moving beyond a "set it and forget it" mindset even with the new PQC standards.

The finalization of these standards is a pivotal moment, kicking off a process of upgrading to post-quantum cryptography across the federal government and industry.

4.2.2. European Union PQC Policy Landscape

The European Union’s approach to post-quantum cryptography has been driven by a mix of strategic planning and coordination among the Member States. In April 2024, the **European Commission** issued a significant policy document: *“Commission Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.”* This Recommendation (C(2024) 2393 final) calls on all EU Member States to work together to transition Europe’s digital infrastructure to PQC[41]. While a Commission

Recommendation is a non-binding instrument, it carries political weight and sets expectations for action at the national level.

At the core of the Commission's Recommendation is the creation of a **"Post-Quantum Cryptography Coordinated Implementation Roadmap"** for the EU. Member States are asked to **develop comprehensive national strategies** for PQC adoption, which will feed into this EU roadmap[42]. The roadmap's goals include clear milestones and timelines for introducing PQC into public administrations and critical services across Europe. Importantly, the Recommendation suggests the use of **hybrid cryptographic schemes** during the migration which combine PQC algorithms with existing ones (or even with Quantum Key Distribution where available) to ensure security and interoperability in the interim.

To implement this, the Commission encourages Member States to leverage existing EU cybersecurity governance structures. Specifically, it proposes establishing a dedicated **PQC sub-group under the NIS Cooperation Group**. The NIS Cooperation Group (established under the NIS Directive, the EU's cybersecurity directive) brings together national cyber authorities. A PQC-focused sub-group would allow representatives from national agencies (e.g., Germany's BSI, France's ANSSI, etc.) and EU bodies like the EU Agency for Cybersecurity (ENISA) to coordinate technical evaluations of algorithms, standards selection, and share progress. In fact, even before the formal Recommendation, many European national cyber agencies were already collaborating: a **joint statement by 18 EU Member States' cybersecurity authorities in late 2024** underscored the urgent need for PQC and recommended protecting sensitive systems *"as soon as possible, and no later than 2030,"* against store-now-decrypt-later attacks[43]. It also noted the establishment of a PQC work stream co-chaired by multiple countries under the NIS Cooperation Group– reflecting exactly the structure which the Commission recommended.

Internationally, the EU aims to **coordinate with allies** such as the United States, NATO partners, and others on PQC standards. This interoperability is crucial given global communication networks: the Commission text explicitly mentions engaging in discussions with bodies like **EuroPol, NATO**, etc., to avoid divergent approaches and to address "emerging challenges" collectively. The EU's stance is that by acting in unison internally and speaking with a single voice externally on PQC, it can better influence the development of resilient standards worldwide.

Several EU Member States have launched national programs for PQC: for instance, France's ANSSI and Germany's BSI have published guidance on using PQC in certain settings (often recommending a hybrid approach initially). The Netherlands in early 2022 issued a strategic agenda highlighting the need for quantum-safe encryption to protect

government data. The proactive approach taken by these key European nations, particularly France, Germany, and the Netherlands, which have also signed a trilateral collaboration on quantum technologies, in developing national guidance and fostering research demonstrates their strategic commitment to PQC readiness. Below is a brief overview on the status quo in these countries:

4.2.2.1 France

Driven by its National Quantum Strategy, France has taken a strong stance on PQC. The national cybersecurity agency, ANSSI (Agence nationale de la sécurité des systèmes d'information), has published detailed position papers and guidance. ANSSI strongly recommends a progressive transition, emphasizing hybrid PQC solutions (combining classical and post-quantum algorithms) in the short to medium term due to the perceived immaturity of stand alone PQC implementations. They advocate crypto-agility and provide specific recommendations for using NIST-standardized algorithms (Kyber, Dilithium, Falcon, SPHINCS+) and their secure implementation, including preferred security levels (Level 5, equivalent to AES-256 where possible) and the use of ephemeral keys.ANSSI outlines a three-phase transition plan for its security certifications. The Banque de France has also conducted PQC experiments, notably in securing email communications.

4.2.2.2 Germany

The Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik) provides key guidance, including its regularly updated "Cryptographic Mechanisms: Recommendations and Key Lengths" and specific papers on quantum-safe cryptography. Like ANSSI, BSI recommends crypto-agility and the use of hybrid solutions during the transition. They also advise upgrading symmetric key lengths (e.g., to AES-256) and using Perfect Forward Secrecy. BSI highlights different mathematical bases for PQC (code, lattice, hash). A significant initiative is QUANTITY which is a BSI and German Aerospace Center (DLR) joint project running until June 2026 aimed at evaluating the practical impact of quantum algorithms on cryptanalysis and developing defensive measures, going beyond known threats like Shor's algorithm.

4.2.2.3 The Netherlands

The Netherlands has taken a collaborative approach involving AIVD (General Intelligence and Security Service), CWI (National Research Institute for Mathematics and Computer Science), and TNO (Netherlands Organisation for Applied Scientific Research) which jointly published "The PQC Migration Handbook” in December 2023. This handbook provides concrete guidelines and actionable steps for organizations to develop a migration strategy. The National Cyber Security Centre (NCSC-NL) also advises organizations on how to create PQC action plans.

Furthermore, there is a notable convergence among these leading agencies (ANSSI, BSI, NCSC-NL) on core principles such as the need for immediate planning, crypto-agility, the utility of hybrid modes, and alignment with NIST algorithms, suggesting a shared understanding of the technical and strategic landscape.

These national efforts converged in the aforementioned **joint statement by 18 countries** (issued at a European Cybersecurity Conference in Athens in December 2024) which effectively pre-empted and supported the European Commission's call for a unified roadmap. That joint statement, entitled *"Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography,"* called for immediate action in the 2020s, detailed migration plans by 2030, and heavy promotion of research and cross-sector collaboration. It also **welcomed NIST's announcement** to stop using vulnerable algorithms by 2035 , underscoring transatlantic alignment on end-goals.

4.2.3. US and EU Analysis

Unlike the U.S., where an Act was passed specifically for quantum preparedness, the EU's actions so far are at the level of recommendations and integrating PQC into existing frameworks. However, some EU laws indirectly relate to PQC. For example, the **NIS2 Directive** (Directive (EU) 2022/2555), which EU Member States are transposing into national law by 2024, requires operators of essential services and critical infrastructure to follow state-of-the-art cybersecurity practices. While NIS2 does not specifically name PQC, its mandate for risk management could be interpreted to include assessing quantum threats and planning mitigations. Similarly, the **EU Cyber Resilience Act (CRA)** imposes cybersecurity requirements on manufacturers of digital products including "secure by design" cryptography. In time, "secure by design" will likely mean using quantum-resistant cryptographic components once standards mature. The **eIDAS Regulation** (for electronic identification and trust services) will also need updating: today's digital signature and encryption mechanisms currently regulated under eIDAS must eventually be replaced or complemented with PQC algorithms to remain trustworthy once large quantum computers exist.

The EU also explicitly ties PQC to **digital sovereignty and strategic autonomy**, ensuring Europe can secure itself with minimal dependence on external technologies, which is a key theme in EU digital policy. Awareness is high in both the US and EU jurisdictions: and PQC has been firmly on the policy agenda. The US and EU also influence each other. For instance, the EU's Recommendation references working with international partners and notes NIST's actions. Meanwhile U.S. officials often discuss aligning with allies on cryptography so that, for example, NATO's communications remain secure on all sides. This transatlantic cooperation is likely to deepen as standards roll out, for example if the EU tests and possibly endorses the NIST-chosen algorithms, and if both participate in ISO standardization of those algorithms).

Finally, both regions stress **the importance of public-private collaboration**. Governments can mandate for their own systems but the majority of the Internet's infrastructure and IoT is in private hands. U.S. efforts like CISA's initiative and the DHS's roadmap, and EU efforts such as engaging industry through ENISA reports or public consultations, all aim to foster the support and collaboration of industry.

4.3. Societal, Legal, Economic and Environmental Implications of PQC Transition

Transitioning to post-quantum cryptography is a technological imperative but it also carries wide-ranging implications beyond the technical realm. This section analyzes how the move to PQC will affect the legal and regulatory environments, industry, the environment, as well as the economy and society in general. Each subsection examines one specific area of impact, noting both the positive outcomes and potential challenges and costs. All impact assessments and predicted outcomes are supported by evidence from research and official sources.

4.3.1.Societal Implications

4.3.1.1 Trust in Digital Infrastructure

In modern society, daily life is deeply intertwined with digital systems which are rendered secure by cryptography, from online banking and e-commerce to personal messaging and critical public services. Society's trust in the **privacy and integrity** of digital communications is underpinned by the assumption that the encryption cannot be easily broken. If advances in quantum computing render current cryptosystems (such as RSA/ECC) vulnerable, there is a risk of **erosion of public trust**. People might fear that confidential information (medical data, financial records, personal chats) could be exposed and misused. By proactively adopting PQC, governments and private organizations signal to the public that they are safeguarding this trust for the future. In essence, PQC is a **public good**: it helps ensure that the digital backbone of society remains reliable and secure even in the face of new technological threats.

4.3.1.2. Privacy [and Surveillance] Concerns

There is a societal dimension in terms of privacy rights. Many forms of data, from personal communications to national ID databases, have long retention periods. Encrypted information that needs to remain confidential for decades such as : personal health records, census data and sensitive research is at risk from adversaries wanting to capture this kind of valuable data now with the intention to decrypt it later once a quantum computer becomes available.

This "**harvest now, decrypt later**" threat is not theoretical: intelligence agencies and cybercriminals are suspected of stockpiling encrypted traffic already. If society does not transition to PQC in time, individuals could see privacy violations in the future without knowing that their personal data had already been stolen. For instance, someone's genetic or medical information encrypted today could be decrypted in 15 years' time, potentially impacting that person's privacy or data being used in discriminatory ways. From a societal perspective, therefore, PQC is tightly linked to **preserving privacy and civil liberties** in the long term. Data protection regulators acknowledge this, For example, the UK Information Commissioner's Office highlighted[44] in 2024 that quantum computers, though possibly years away, require action now to protect personal data and fundamental rights in the future.

On the flip side, PQC might also spur new debates regarding surveillance. Law enforcement and national security agencies currently rely on techniques such as encrypted traffic analysis or on occasion breaking weaker crypto (and using quantum computing themselves when it becomes available). As encryption overall becomes stronger with PQC, agencies might push for new legal powers or backdoors, reigniting the encryption policy debate (privacy vs. security). Society will have to navigate maintaining strong quantum-proof encryption for privacy, while handling government requests for access in investigations, a tension that already exists but could be heightened when even current encryption vulnerabilities are closed.

4.3.1.3. Securing Critical Services for Society

Society is also directly impacted by how essential services weather the PQC transition. Consider sectors like healthcare, transportation and energy which use cryptography for everything from securing patient records to controlling traffic lights and power grids. A failure to properly transition these to PQC could result in future incidents that have tangible societal harm (e.g. a breach of a hospital's data or a major disruption in utilities). Conversely, a well-managed PQC upgrade in these areas means that citizens continue to enjoy uninterrupted and **safe services**. For instance, the confidentiality of e-government services

(like digital tax filing or electronic voting in some countries) must be preserved against quantum attacks in order to maintain civic trust and participation. Ensuring that **democracy and public safety** are protected from quantum threats is a societal imperative; policies relating to PQC, inherently prioritize these societal pillars by focusing on critical infrastructure first.

In sum, the societal implications of transitioning to PQC revolve around **maintaining trust, privacy, and equal access** in the digital age. Society stands to benefit greatly from timely PQC migration because it is essentially future-proofing the protections that people have come to rely on. However, care must be taken to manage the transition inclusively and transparently, so that the benefits of continued security and privacy are realized by all, and the risks associated with new issues such as exacerbating the digital divide or sparking policy conflicts, are mitigated.

4.3.2. Legal and Regulatory Implications

4.3.2.1 Data Protection and Compliance

Legal frameworks for data protection, such as the EU's General Data Protection Regulation (GDPR) and various national privacy laws, generally require organizations to protect personal data using "appropriate technical and organizational measures," often explicitly mentioning encryption as an example of a security control. As the threat landscape evolves, what is considered "appropriate" can change, and GDPR's notion of state-of-the-art security (Article 32) could arguably compel the use of quantum-resistant encryption once it becomes the industry standard or at least when quantum threats become imminent. Regulators have started acknowledging this; the UK ICO noted that organizations processing personal data should start preparing for PQC now, even if quantum computers capable of breaking encryption are years away. This implies that failing to plan for PQC could, in the future, be seen as a form of negligence or non-compliance with data protection obligations. Companies might face legal liabilities if they knowingly continue using outdated and vulnerable cryptography and a breach occurs due to that weakness.

4.3.2.2. Economic and Industry Implications

Cost of Transition: Adopting PQC will incur significant costs for both the public and private sectors. Organizations will need to inventory and upgrade potentially thousands of applications and devices. This involves **software development costs** (to implement new

algorithms in applications, protocols, and systems), **hardware costs** (some older hardware modules or smart cards might not support larger key sizes or may need replacement), and **operational costs** (managing a migration project, compatibility testing, etc.).

The transition is often compared to the Y2K effort or the migration from 32-bit to 128-bit encryption, though arguably larger in scope. While exact numbers are hard to predict, one can gauge magnitude by analogies: a major bank or tech company could spend tens of millions of dollars and several years to fully transition their cryptographic infrastructure. At a macro level, the **global market for cybersecurity solutions** will see a surge in demand for PQC-related products – from new VPNs and secure messaging systems to quantum-safe IoT chips. This is a cost, but also an economic stimulus in the cybersecurity sector.

However, delaying the transition would likely lead to **much higher costs** later. A breach enabled by quantum cryptanalysis in the future could cost an organization hugely in terms of fines (for regulatory breaches), lawsuits, and reputational damage, not to mention the national security and human safety implications. Therefore, spending on PQC now is often justified as a cost-avoidance measure, essentially *invest now to save later*. The U.S. government's approach implicitly recognizes this, aiming to "mitigate as much of the quantum risk as possible by 2035"[45], thereby reducing future breach costs.

4.3.3. Environmental Implications

Many PQC algorithms demand more computational resources than their classical predecessors therefore posing a risk on **Energy Consumption of Algorithms**. For example, lattice-based schemes like CRYSTALS-Kyber and Dilithium involve heavy matrix and polynomial arithmetic that can strain central processing units (CPUs) and memory. As a result, operations (key generation, encryption, signing, verification) may take more time or power. A general observation, as noted in the literature, is that *"post-quantum cryptography algorithms… require larger key sizes… [with] tradeoffs in computational efficiency"*. If not optimized, widespread use of PQC could mean **increased energy use for cryptographic operations**. In data centers, if every transport layer security (TLS) connection uses a PQC key exchange and signature, the CPU overhead for each connection would increase which multiplied by billions of connections would increase the power consumption of servers globally. Research has started to quantify this. A study by the Institute of Electrical and Electronics Engineers (IEEE) found that certain PQC algorithms can consume significantly more energy for each operation on embedded devices than on classical ones (depending on implementation). In particular, the type of post-quantum cryptography known as hash-based schemes which have large signatures and slow performance, can be energy-intensive to verify. (Roma & Hasan 2021).

However, it is not all negative. Some PQC algorithms are surprisingly efficient. Lattice-based cryptographic systems for example can be quite fast and in some cases the **Dilithium signature scheme can be faster than the RSA (Rivest Shamir Adelman) one** because RSA with very large key sizes is also slow. Furthermore, symmetric cryptography such as the Advanced Encryption Standard (AES) remains unchanged; it is mainly the public-key operations that change. So, the net energy impact will vary according to each use-case.

There is ongoing work to optimize PQC implementations for performance and energy. For example, hardware accelerators for lattice math and using vector instructions to speed up calculations with the aim of reducing the energy and carbon footprint.

Another major environmental concern is that if many existing devices (routers, smart cards, IoT sensors, etc.) cannot be upgraded to PQC, they might have to be replaced. This can contribute to **electronic waste (e-waste)** if done rapidly and on a large scale. Ideally, devices will be retired at end-of-life as usual but with billions of IoT devices in use globally (estimated to be approximately 25-40 billion by 2030), even a fraction needing early replacement due to cryptography transition could be a large absolute number.

Perhaps surprisingly, there can also be **positive environmental aspects**. Secure and trusted networks enable digitalization which replaces more carbon-intensive activities such as travel for meetings being replaced by secure video calls, or paper-based processes being replaced by digital formats.

Furthermore, if users' fear of quantum breaches undermines digital adoption, they might well revert to less efficient means. By securing the future deployment of digital technologies, PQC indirectly supports the continuation of **digital transformations that often have environmental benefits** such as smart grids and telecommuting. A report on the **sustainability context** noted that without PQC, quantum attacks could undermine critical systems, which in turn could impact sustainability efforts.

4.4. Policy Recommendations for National Governments and Regulators

1. **Develop National PQC Roadmaps with Timelines:** Countries should create or adopt clear roadmaps for migrating government and critical infrastructure systems to PQC. Define clear goals, timelines, milestones, and agency responsibilities for PQC migration within government and critical infrastructure sectors, drawing inspiration from existing models (e.g., US OMB M-23-02) but tailored to national context. Ensure alignment with international standardization efforts (NIST).
2. **Foster Robust Public-Private Partnerships**: Create formal mechanisms for ongoing collaboration between government agencies, industry (technology providers, critical infrastructure operators, end-users), and academic researchers. Focus on joint R&D, threat intelligence sharing, development of best practices, and addressing implementation challenges.
3. **Fund Research, Development, and Talent:** Allocate funding for R&D in post-quantum cryptography and related fields. Invest strategically in R&D for PQC, focusing not only on algorithm security but also on implementation efficiency (especially for constrained environments like IoT), side-channel resistance, formal verification methods, and crypto-agility tools. Support basic research and programs to nurture startups and specific application use cases.
4. **Mandate or Incentivize Crypto-Agility:** Implement policies that require or strongly encourage the design and deployment of crypto-agile systems within government and critical sectors. This ensures flexibility to adopt new PQC standards and respond to future cryptographic breaks.
5. **Leverage Public Procurement:** Utilize government purchasing power to accelerate PQC adoption. Update procurement regulations (such as the US Federal Acquisition Regulation (FAR) or EU public procurement directives) to require NIST-standardized (or equivalent) PQC support in new IT systems and services, especially those handling sensitive data or supporting critical functions.
6. **Raise National Awareness and Provide Guidance**: Launch national awareness campaigns targeting businesses (especially SMEs), critical infrastructure operators, and the public about the quantum threat, in particular from HNDL ("harvest now, decrypt later") attacks and the need for PQC migration. Develop and disseminate practical guidance, tools, and resources (e.g., migration handbooks, inventory tools).
7. **Address the Cybersecurity Workforce Skills Gap**: Partner with educational institutions and industry to develop curricula and training programs focused on PQC, quantum computing fundamentals, and crypto-agility. Implement initiatives to attract, train, and retain a skilled and diverse quantum-ready cybersecurity workforce
8. **Update Legal and Policy Frameworks:** Review and update laws and regulations to incorporate quantum-safe requirements. Data protection authorities should issue guidance making it clear that "state of the art" encryption includes PQC as soon as relevant standards are mature.
9. **Promote International Collaboration and Harmonization**: Actively participate in international standards bodies (ISO) and intergovernmental forums (such as

the OECD, G7 and NATO which published its Quantum Technologies Strategy in January 2024) to promote global harmonization of PQC standards, share best practices, coordinate threat responses, and address cross-border legal and policy issues. Work towards common approaches on technology transfer and export controls for PQC.

4.5. Best Practice Recommendations for Industry and Service Providers

1. **Create a Comprehensive Cryptographic Inventory:** Conduct a comprehensive inventory of all applications, systems, hardware, and data flows that rely on public-key cryptography. Document algorithms used, key lengths, data sensitivity, system owners, and vendor dependencies. Consider using automated discovery tools supplemented by manual verification. Maintain this inventory as an ongoing process.
2. **Develop a Quantum-Readiness Plan:** Based on the inventory, plan the key stages of transition with target dates and sequencing. Assign clear responsibility for PQC migration (e.g., a dedicated team or lead). Secure executive buy-in and necessary resources. Do not delay planning until mandates are imminent.
3. **Perform Risk Assessment and Prioritization:** Analyze the systems in the inventory to identify those most vulnerable or critical. Prioritize migration based on:
    1. Data Sensitivity and Shelf-Life: Systems handling data requiring confidentiality beyond the potential arrival of CRQCs (addressing HNDL risk).
    2. System Criticality: High Value Assets, systems supporting essential business functions or critical infrastructure.
    3. External Dependencies: Systems interfacing with partners or customers who may have different PQC timelines.
    4. Ease of Migration: Consider tackling less complex systems first ("quick wins") to build experience.
4. **Develop a Phased PQC Migration Roadmap:** Based on the inventory and risk assessment, create a detailed, multi-year roadmap outlining:
    1. Scope of systems to be migrated.
    2. Chosen PQC algorithms (aligned with standards) and migration approach (e.g., hybrid vs. full replacement).
    3. Timelines and milestones for each phase (discovery, testing, pilot, rollout).
    4. Budget and resource allocation.
    5. Dependencies (internal teams, vendors).
    6. Testing and validation strategy.
5. **Adopt Hybrid Solutions in the Interim:** During the transition period, consider deploying **hybrid cryptography**, use combinations of classical and post-quantum algorithms, such that even if one is broken the other still provides security. For example, some TLS implementations allow doing two key exchanges (one ECDH, one Kyber) and using both keys to derive the session secret; an attacker would need to break both.

6. **Pilot and Test PQC Implementations:** Discuss PQC roadmaps and support timelines with all critical hardware, software, and cloud service providers. Include PQC compliance clauses in new contracts and renewals. Prioritize vendors demonstrating a clear commitment to PQC transition. Start with pilot projects in non-production or less critical environments. Experiment with PQC libraries (NIST has reference implementations and many open-source libraries exist for algorithms like Kyber, Dilithium, etc.).

Part 3

5.IoT and PQC

The Internet of Things (IoT) has rapidly transformed numerous aspects of modern life, permeating sectors ranging from smart homes and wearable devices to industrial automation and healthcare monitoring. This proliferation of interconnected devices has brought unprecedented convenience and efficiency, fostering a growing reliance on their diverse functionalities. However, the increasing dependence on these connected ecosystems has simultaneously amplified concerns regarding their security[46] also in light of their ubiquitous access to personal data.[47] Given that vulnerabilities in even a single IoT device can potentially compromise entire networks and critical infrastructures, robust security measures are paramount.[48] Therefore, IoT devices have historically been seen as a weak link in cybersecurity as many devices operate with minimal processing power and memory, and some use outdated or weak cryptographic methods (if any at all) due to cost and power constraints.

A significant and emerging threat to the security of IoT devices lies in the advancements of quantum computing.[49] Quantum computers possess the theoretical capability to break many of the current cryptographic methods that underpin the security of IoT systems. While the precise timeline for the development of quantum computers powerful enough to render current encryption obsolete remains uncertain, estimates generally place this within the next 5 to 15 years.[50] This impending threat necessitates a proactive approach to security, urging the adoption of quantum-resistant solutions. Post-Quantum Cryptography (PQC) policies are therefore crucial for ensuring the long-term security and resilience of IoT ecosystems against these future quantum threats.

This vulnerability extends beyond the confidentiality of data; it also undermines the integrity and authenticity of IoT systems by compromising the digital signatures used for authentication.[51] Attackers could potentially forge signatures, leading to unauthorized access and control over IoT devices, mimicking legitimate devices, and creating extensive

IoT botnet attacks.[52] With quantum threats on the horizon, IoT security faces a paradox: these devices need quantum-resistant protection but may struggle to implement it.

5.1. Policies and Challenges

IoT policy, such as the EU's Cyber Resilience Act or various national IoT security frameworks (like the UK's Code of Practice for Consumer IoT Security), emphasizes "security by design". Going forward, **quantum-resistance should be part of "security by design" for IoT**. New devices being designed should include hardware support (if possible) for PQC or at least be made crypto-agile (i.e. able to change algorithms) through firmware updates. Regulatory standards should explicitly state that connected devices should not rely solely on cryptography that will become insufficient in the devices' expected lifetime. In view of the likelihood that many IoT devices might be deployed for 10 or more years in fields like smart infrastructure, it is prudent to require that devices in certain categories (e.g., vehicles, medical devices) are permanently quantum-safe if they use public-key cryptography.

Many IoT use cases deploy asymmetric cryptography for actions such as authentication when a device proves its identity to a network server by signing a challenge, or sets up keys via a handshake. If these schemes are broken by quantum computing, large-scale impersonation or MitM (man-in-the-middle) attacks could happen. The consequences of such breaches could be catastrophic damage if for example an attacker were able to spoof thousands of healthcare IoT monitors by forging their signatures, or to decrypt previously captured traffic from industrial sensors in order to learn how to send false control commands. PQC will mitigate such threats by restoring the barriers that prevent the breaking authentication and encryption. PQC can thus ensure the **continuity of secure IoT operations** well into the future. This is especially crucial for systems like smart grids and autonomous vehicles where security failures can endanger lives or property.

PQC algorithms typically use larger keys and more complex calculations than classical algorithms. For a minute IoT sensor such as a temperature sensor on a battery, performing a lattice-based key exchange or generating a hash-based signature is technically very demanding. ,**power consumption** is a significant concern because quantum encryption algorithms are generally more power-intensive than classical algorithms, which is a critical factor for battery-operated IoT network nodes for Internet connectivity. Policymakers and industry standards bodies need to encourage the development of **lightweight PQC algorithms or variants** optimized for constrained devices, and possibly allow a slower transition for the most constrained environments, perhaps by segmenting networks or using gateways that can handle heavier-to-operate cryptography on behalf of devices with limited capabilities.

The successful integration of post-quantum cryptography into the Internet of Things presents a unique set of challenges, primarily stemming from the inherent resource constraints of many IoT devices. These limitations in processing power, memory (both volatile and non-volatile), and energy availability significantly impact the direct implementation of many PQC algorithms. Compared to the traditional cryptographic algorithms currently employed in IoT, many PQC algorithms require larger key sizes and involve more complex computational operations.

This increased demand for resources can lead to several practical issues for IoT devices, including higher energy consumption, potentially draining batteries more quickly and reducing operational lifespan; slower performance of security operations, which can impact the responsiveness and overall user experience of IoT applications; and the risk of exceeding the available memory capacity on the device, preventing the deployment of certain PQC algorithms altogether.

The fundamental challenge, therefore, lies in reconciling the resource-intensive nature of many promising PQC algorithms with the stringent limitations imposed by the design and operational requirements of a vast number of IoT devices.

Finally, to further optimize the performance of PQC algorithms on the often resource-constrained IoT devices, the utilization of hardware acceleration can play a significant role. This involves employing dedicated hardware components, such as specialized cryptographic coprocessors or secure elements integrated into the IoT device, to offload the computationally intensive PQC operations from the device's main processor.[53] These custom hardware solutions can be optimized for the specific mathematical operations inherent in certain PQC algorithms, leading to substantial gains in both processing speed and energy efficiency compared to running the same algorithms purely in software on a general-purpose processor. For instance, various research projects have focused on implementing quantum-safe security solutions on resource-constrained embedded systems by leveraging the capabilities of dedicated cryptographic coprocessors to achieve the necessary levels of performance and security required for practical deployment.[54]

The impact of existing policies and standards on promoting the adoption of quantum-resistant security measures in the IoT ecosystem is currently limited due to the nascent stage of PQC standardization and the lack of specific regulations mandating its use in most sectors. However, proactive government initiatives, such as the US government's push for federal agencies to adopt PQC in their acquisitions[55], and collaborative efforts within the industry, such as the GSMA's work on PQC for IoT[56], are expected to play a crucial role in accelerating the transition. Ultimately, policy will be a key driver in ensuring the widespread adoption of PQC in the IoT ecosystem, compelling organizations to prioritize the migration to quantum-resistant security measures.[57]

5.2. Privacy Impacts and Concerns

The quantum threat poses significant privacy implications for the vast ecosystem of IoT devices. These devices routinely collect and transmit a wide array of sensitive personal data, including health information from wearables, location data from trackers, and usage patterns from smart home devices. If the current encryption methods used to protect this data are broken by quantum computers, it could lead to severe privacy violations, including identity theft, financial fraud, and the exposure of highly personal details.[58] The sheer volume and sensitivity of data handled by IoT devices amplify these privacy risks.

The threat of "harvest now, decrypt later" attacks is particularly concerning for the long-term privacy of IoT users. Malicious actors might already be intercepting and storing encrypted data transmitted by IoT devices with the anticipation that they will be able to decrypt it in the future using quantum computers. Given the potentially long lifespan of many IoT devices and the enduring value of the data they collect (such as medical records or historical location data), this poses a significant and long-term privacy risk. This scenario underscores the urgent need for organizations to transition to PQC to safeguard data that has long-term value and sensitivity.[59]

Beyond data decryption, quantum attacks could also potentially compromise the functionality of IoT devices. This could lead to privacy violations through the manipulation of device settings, unauthorized access to device features, or even the repurposing of devices for malicious activities.[60]

5.3. Policy Recommendations

To effectively address the quantum threat to IoT security and ensure the protection of user privacy in the quantum era, the following specific and actionable policy recommendations are proposed at both national and organizational levels:

5.3.1. National Level Recommendations

Government Initiatives for Awareness and R&D: Implement national-level programs to raise awareness among stakeholders (including consumers, industry, and researchers) about the quantum threat to IoT security and the importance of PQC. Significantly fund research and development efforts focused on creating lightweight and efficient PQC algorithms and hardware acceleration techniques that are specifically tailored for the resource-constrained nature of IoT devices.

Standardization Collaboration for IoT: Actively engage with international standardization bodies (such as ISO/IEC) to collaborate on the development and adoption of standardized PQC algorithms and protocols that are specifically designed to meet the unique security and resource requirements of IoT devices.

Mandatory PQC Compliance: Mandate the adoption of PQC for all government-funded IoT projects and within critical infrastructure sectors (such as energy, healthcare, and transportation) by setting clear and achievable timelines. This will drive early adoption and ensure the security of sensitive public services.

National Guidelines for PQC in IoT with Privacy Focus: Develop comprehensive national guidelines and frameworks that provide clear instructions and best practices for organizations on how to effectively implement PQC in their IoT systems while prioritizing the protection of user privacy. These guidelines should address aspects like algorithm selection, key management, data governance, and transparency requirements.

Educational and Training Programs: Establish national-level educational programs and training initiatives aimed at equipping cybersecurity professionals, IoT developers, and system integrators with the necessary knowledge and skills to understand, implement, and manage PQC in IoT environments.

5.3.2. Best Practice Recommendations for Industry

Cryptographic Asset Inventory for IoT: Conduct a thorough and comprehensive inventory of all cryptographic assets currently deployed within their IoT products and services. This inventory should identify the specific IoT devices in use and the cryptographic algorithms they rely on to assess their current vulnerability to potential quantum attacks.

PQC Transition Roadmap for IoT: Develop a clear and well-defined roadmap outlining the organization's strategy for transitioning to PQC in their IoT product lines and service offerings. This roadmap should consider the lifecycle of their devices, the feasibility of firmware updates, and the prioritization of systems based on the sensitivity of the data they handle.

Prioritized PQC Implementation: Prioritize the implementation of PQC for IoT devices and systems that handle highly sensitive user data or perform critical functions. This risk-based approach will ensure that the most vulnerable and high-impact areas of their IoT ecosystem are secured against quantum threats first.

Establishing clear data governance policies for IoT data in the context of PQC: Organizations need to define clear rules and responsibilities regarding the collection,

processing, storage, and retention of data generated by IoT devices, taking into account the long-term implications of quantum computing and the need for quantum-resistant security.

Adoption of Crypto-Agility and Robust Security Testing for PQC in IoT: Embrace a "crypto-agile" design philosophy for all new IoT device development. This involves ensuring that devices are designed with the flexibility to be updated with new cryptographic algorithms in the future as the field of PQC evolves and new standards emerge. Implement rigorous security testing and validation processes specifically for PQC implementations within their IoT devices. This should include vulnerability assessments and penetration testing to ensure that the new quantum-resistant cryptographic methods are secure and perform effectively in the IoT environment.

Data Privacy Policies for PQC in IoT: Establish clear and comprehensive policies and procedures that specifically address data privacy in the context of PQC for their IoT products and services. These policies should define how user data will be protected using quantum-resistant cryptography and ensure ongoing compliance with all relevant privacy regulations.

Supply Chain Engagement for PQC Readiness: Actively engage with their supply chain partners, including vendors and manufacturers of IoT components, to ensure that they are also preparing for the transition to PQC. Collaboration and communication throughout the supply chain are crucial for the successful and timely adoption of quantum-resistant security measures across the entire IoT ecosystem.

Notes

---

[1] The ethical implications of the Internet of Things (IoT): study adopted in September 2021

[2] Margolis, J., Oh, T. T., Jadhav, S., Kim, Y. H., & Kim, J. N. (2017, July). An in-depth analysis of the mirai botnet. In *2017 International Conference on Software Security and Assurance (ICSSA)* (pp. 6-12). IEEE.

[3] Elsaraf, R. (2021). 'Chrysler UConnect hack and automotive computer and cyber security.

[4] Tech Targer, (2017), How Serious are the flaws in the St. JudeMedical's IoT medical devices? https://www.techtarget.com/searchsecurity/answer/How-serious-are-the-flaws-in-St-Jude-Medicals-IoT-medical-devices

[5] Diagnostic and Interventional Cardiology, (2027), FDA Cinfirms Cyversecurity Vulnerabilities of St. Jude's Implantable Cardiac Devices, Merlin Transmitter, https://www.dicardiology.com/article/fda-confirms-cybersecurity-vulnerabilities-st-judes-implantable-cardiac-devices-merlin

[6] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, 44, 100

[7] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[8] https://social.cyware.com/news/the-mirai-mania-a-brief-look-into-the-notorious-mirai-botnet-and-its-variants-37c443f8

[9] https://www.infosecinstitute.com/resources/malware-analysis/mirai-botnet-evolution-since-its-source-code-is-available-online/

[10] https://www.infosecurity-magazine.com/news/unpatched-cctv-cameras-exploited/

[11] CVE-2024-6047 & CVE-2024-11120

[12] https://www.akamai.com/blog/security-research/active-exploitation-mirai-geovision-iot-botnet

[13] For example: CVE-2017-18368 in ZTE routers and CVE-2021-20090 in Arcadyan-derived firmware

[14] https://www.aquasec.com/blog/matrix-unleashes-a-new-widespread-ddos-campaign/

[15] https://blog.lumen.com/derailing-the-raptor-train/

[16]https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

[17] https://blog.talosintelligence.com/vpnfilter/

[18] https://blog.talosintelligence.com/vpnfilter-update/

[19] https://www.sciencedirect.com/science/article/abs/pii/S1353485819300376

[20] https://www.csk.gov.in/alerts/MoziIoTBotnet.html

[21] Federal Trade Commission, (2024) FTC Takes Action Against Security Camera Firm Verdaka over Cgarges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act, https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other

[22] CVE-2023-6321, CVE-2023-6322, CVE-2023-6323, and CVE-2023-6324

[23]https://www.bitdefender.com/en-us/blog/labs/notes-on-throughtek-kalay-vulnerabilities-and-their-impact

[24] National Cybersecurity Centre, (2025), Timelines for Migration to Post-Quantum Computing Cryptograpgy, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[25] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[26] https://datatracker.ietf.org/wg/lake/about/

[27] https://datatracker.ietf.org/doc/draft-reddy-uta-pqc-app/

[28]

https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern

[29] Alvin Moon and Michael Vermeer, 'Supporting the Future Effectiveness of Post-Quantum Cryptography' (RAND Corporation 2023) <https://www.rand.org/pubs/perspectives/PEA2690-1.html> accessed 9 May 2025.

[30] ibid.

[31] David Joseph and others, 'Transitioning Organizations to Post-Quantum Cryptography' (2022) 605 Nature 237.

[32] Victor Lovic, 'Quantum Key Distribution: Advantages, Challenges and Policy' (2020) 1 Cambridge Journal of Science & Policy.

[33] ibid.

[34] U.S. Government Accountability Office, 'Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy' (2024) GAO-25-107703.

[35] The White House, 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (*The White House*, 4 May 2022) <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/> accessed 20 March 2025.

[36] Ro [D-CA-17 Rep. Khanna, 'H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act' (21 December 2022) <https://www.congress.gov/bill/117th-congress/house-bill/7535> accessed 20 March 2025.

[37] ibid.

[38] William Newhouse and others, 'Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery' NIST SPECIAL PUBLICATION 1800-38B.

[39] Gorjan Alagic and others, 'Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process' (National Institute of Standards and Technology 2025) NIST Internal or Interagency Report (NISTIR) 8545 <https://csrc.nist.gov/pubs/ir/8545/final> accessed 20 March 2025.

[40] 'NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption' [2025] NIST <https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption> accessed 9 May 2025.

[41] ‘New EU Recommendation on Post-Quantum Cryptography’ (*Digital Government*, 23 April 2024) <https://www.nldigitalgovernment.nl/news/new-eu-recommendation-on-post-quantum-cryptography/> accessed 20 March 2025.

[42] ‘COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography’ (Council of the European Union 2024) 9212/2.

[43] ‘Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography’ [2024] A joint statement from partners from 18 EU member states:

[44] Information Commissioner’s Office, ‘Tech Horizons Report’ (2024) <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-report-2024/quantum-computing/> accessed 24 March 2025.

[45] The White House, ‘National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems’ (*The White House*, 4 May 2022) <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/> accessed 20 March 2025.

[46] Kazi Masum Sadique, Rahim Rahmani and Paul Johannesson, ‘Towards Security on Internet of Things: Applications and Challenges in Technology’ (2018) 141 Procedia Computer Science 199.

[47] Mark Mbock Ogonji, George Okeyo and Joseph Muliaro Wafula, ‘A Survey on Privacy and Security of Internet of Things’ (2020) 38 Computer Science Review 100312.

[48] ‘A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures | IEEE Journals & Magazine | IEEE Xplore’ <https://ieeexplore.ieee.org/document/8742551> accessed 16 May 2025.

[49] Diksha Chawla and Pawan Singh Mehra, ‘A Survey on Quantum Computing for Internet of Things Security’ (2023) 218 Procedia Computer Science 2191.

[50] Charles Kinyua Gitonga, ‘The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography’ (2025) 5 European Journal of Information Technologies and Computer Science 1.

[51] Yaser Baseri, Vikas Chouhan and Ali Ghorbani, ‘Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure’ (arXiv, 16 April 2024) <http://arxiv.org/abs/2404.10659> accessed 16 May 2025.

[52] Skip Sanzeri, ‘The Quantum Threat To IoT’ (*Forbes*) <https://www.forbes.com/councils/forbestechcouncil/2023/09/25/the-quantum-threat-to-iot/> accessed 16 May 2025.

[53] Tao Liu, Gowri Ramachandran and Raja Jurdak, ‘Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization’ (arXiv, 31 January 2024) <http://arxiv.org/abs/2401.17538> accessed 24 March 2025.

[54] Gregory Fitzgibbon and Carlo Ottaviani, ‘Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography’ (2024) 8 Cryptography 21.

[55] Justin Doubleday, ‘Agencies Explore Post-Quantum Cryptography in Acquisitions’ (14 May 2025) <https://federalnewsnetwork.com/cybersecurity/2025/05/agencies-explore-post-quantum-cryptography-in-acquisitions/> accessed 16 May 2025.

[56] Yolanda Sanz, ‘Post Quantum Cryptography in IoT Use Case’ (*GSMA*, 24 February 2025) <https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/post-quantum-cryptography-in-iot/> accessed 16 May 2025.

[57] Chawla and Mehra (n 4).

[58] Liu, Ramachandran and Jurdak (n 8).

[59] Sachin Kumar, Prayag Tiwari and Mikhail Zymbler, ‘Internet of Things Is a Revolutionary Approach for Future Technology Enhancement: A Review’ (2019) 6 Journal of Big Data 111.

[60] For safety-critical IoT applications, such as medical devices like pacemakers or insulin pumps, or industrial control systems, the compromise of device functionality due to quantum attacks could have severe consequences, potentially endangering lives.