# Forever Days, Silicon Immutability and the Crisis of Unpatchable BootROM Vulnerabilities in Cyberwarfare: Ethical and Anticipated Ethical Issues

**Richard L Wilson[1] and Noah Donnelly[2]**
[1]Department of Philosophy/Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA
[2]Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA

wilson@towson.edu
ndonnel1@students.towson.edu

**Abstract:** Modern mobile security architecture relies on a hardware Root of Trust, which is a set of capabilities in a device's hardware that functions as anchor for all security operations within that system. (Rambus Press) This is exemplified by components such as the Apple Secure Enclave (Touch ID or Face ID use a separate processor to handle your biometric information which is called Apple Secure Enclave) (Pot, 2018). However, the reliance on immutable Silicon, specifically BootROM code (Bootrom (or Boot ROM) is a small piece of mask ROM or write-protected flash embedded inside the processor chip (What is Bootrom). It contains the very first code which is executed by the processor on power-on or reset), introduces a very critical risk: the "Forever Day" vulnerability. Unlike software flaws, vulnerabilities within the BootROM cannot be patched once the chip leaves the manufacturing plant. BootROM code itself isn't *used* in cyber warfare; rather, vulnerabilities in BootROM become powerful footholds for: persistent espionage, secure-boot bypass, hardware-level compromise, supply-chain infiltration, cryptographic key extraction, attacks on critical infrastructure devices. Because of its immutable nature, a single BootROM vulnerability can become a strategic cyber weapon—especially for well-resourced nation-state adversaries. Ethical issues arise due to how malicious adversaries could exploit the immutable nature of BootROM vulnerabily. According to Furrow ethics is related to the intentions, actions and outcomes produced by agents involved in decision making. To intentionally manufacture technology with vulnerability built into immutable silicon is an ethical issue. This analysis, using case studies investigates the technical outcomes of such exploits, where a single compromised read-only sector renders millions of devices permanently vulnerable to compromise regardless of OS security updates. We further analyze the tension between the commercial imperative to rush new silicon models to market for profit and the rigorous security validation required for immutable code. Finally, the paper discusses the role of state actors, such as the NSA, in the disclosure versus hoarding of these hardware level exploits. We conclude that "Forever Days", (a Forever Day bug refers to security vulnerability in a software application or system that remains unpatched for an extended period of time ) (Forever Day Bug, 2023) represent a fundamental failure in the current hardware lifecycle, leaving a permanent window for exploitation that persists for the lifespan of the physical device. The analysis will conclude with an ethical and anticipated ethical analysis of BootROM code when it is used in support of cyberwarfare.

**Keywords:** BootROM vulnerabilities, Hardware Root of Trust (HRoT), Vulnerabilities Equities Process (VEP), Anticipatory technology ethics, Cyberwarfare, Supply chain security

## 1. Introduction

Modern computing security has been built upon an architectural concept called hardware root of trust (HRoT). As operating systems and application-layer software have been hardened against traditional cyber-attacks using mechanisms like application sandboxing and memory randomization, threat actors, especially well-resourced nation states, have moved their focus downward to attack the fundamental physical components of the devices themselves (Mishra & Sahay, 2025). The BootROM, or the first set of instructions executed by a processor when powered up, is at the heart of this hardware security paradigm (Fan et al., 2025). Since Boot ROM code is burned into silicon during the manufacturing process, it is immutable, this means it cannot be modified, updated or patched post manufacture (Schneier, 2012).

This immutability provides a cryptographic anchor that is tamper-proof and allows all programs added after boot to be mathematically verified against a reliable and immutable standard (Vasudevan et al., 2024). This architectural strength also presents a significant weakness. When a vulnerability is found in BootROM code, this immutability changes the status of that zero-day vulnerability to a "Forever Day" (Schneier, 2012). A Forever Day is a vulnerability in hardware that will remain in place for the life of the device, and therefore, software patches will have no effect on the device, and the hardware will be compromised forever (CISA, 2023).

The consequences of Forever Day vulnerabilities are significant not only for consumer privacy but also for global cyber warfare and national security (Kitchin, 2017). Ethical issues with forever day vulnerabilities are related to how Silicon Immutability and Unpatchable BootROM Vulnerabilities are intentionally designed and

manufactured. A variety of devices may be comprised of multiple hardware and software parts, and therefore are not structured as "all-one" Systems-On-a-Chip (SoCs); some examples include the modern mobile devices (the majority of which utilize SoCs), the controls for Industrial Control Systems (ICSs), and the routers associated with Critical National Infrastructure (Grassi, 2018). The most significant example of this type of architecture is the Baseband Processor (BP), which is a proprietary and opaque chip designed to control and provide cellular communications (Grassi, 2018). BP chips are located at a lower point in the OS and below the level of visibility and execution of the AP and are a "sovereign" computing environment. As such, the baseband processor has extensive privileges over all resources associated with the device, including the ability to use Direct Memory Access (DMA) to the main memory of the device (Weinmann, 2012).

The presence of an un-patchable vulnerability in the BootROM coupled with a highly privileged hardware component such as the baseband processor creates a persistent, un-auditable leveraging point for cyber-espionage (Weinmann, 2012). Manufacturers have allowed designers to intentionally introduce these vulnerabilities into their devices. The vulnerabilities introduced through these flaws give adversaries the ability to circumvent secure boot processes, conduct deep compromises at the hardware level, extract cryptographic keys, and create supply chain compromises that go undetected by traditional security software (Kataria et al., 2019). As a result, a single vulnerable read-only sector compromise has the potential to transform millions of devices into hidden assets for state-sponsored cyber warfare (Wilson & Donnelly, 2026).

The growing number of vulnerabilities that can't be fixed raises many major technical, strategic, and ethical issues. The commercial need for companies to produce new silicon quickly versus the need for thorough formal verification to create immutable code has created a vulnerability pipeline in the semiconductor ecosystem (PwC, 2024). Additionally, when an intelligence agency identifies a ‘Forever Day’, they face a significant moral dilemma; their country can either hold onto the exploit for possible future offensive cyber operations or disclose the vulnerability in order to protect civilians or critical infrastructure, as spelled out in the Vulnerabilities Equities Process (VEP), (Schwartz & Knake, 2016). Based on a careful and thorough analysis of the BootROMs' technology, the ethical implications of hardware sovereignty, a review of significant case studies, and Anticipatory Technology Ethics, this study helps to clarify the silicon immutability crisis and introduces several practical recommendations for mitigating those Forever Day threats.

## 2. Ethical Issues

In addition to a variety of technical issues related to Forever Days and silicon immutability there are a number of ethical issues that can be identified. Here we focus on ethical issues. The focus of ethical analysis involves a series of factors that expand upon the notion of an agent performing an action. As Furrow states, ethics is related to evaluating actions, and actions are performed by those capable of being moral agents. As Furrow says, “When we evaluate an action, we can focus on various dimensions of the action. We can evaluate the person who is acting, the intention or motive of the person acting, the nature of the act itself, or the consequences.” (Furrow, 2005) A moral agent can justify their intentions, actions and outcomes produced by actions by referring to ethical principles. When Forever Days, Silicon Immutability and the Crisis of Unpatchable BootROM Vulnerabilities occur related to modern mobile security architecture and cyberwarfare and when adversaries act, and these actions are based on intentions, these intentions and actions are aimed at producing outcomes. Identifying threats to Urban environments in urban warfare, has never been more evident. Each of these activities have ethical implications.

The fate of those at risk due to technological developments in and through urban warfare and cyber warfare are currently critical issues. Ethical analysis should identify ethical principles related to agents (friendly or adversarial) intentions, actions and projected outcomes that can be applied to developments in technology and issues such as Forever Days, Silicon Immutability and the Crisis of Unpatchable BootROM Vulnerabilities**.**

There are several ethical dilemmas caused by the technical reality of immutable vulnerabilities to silicon (i.e. the material that is foundational to computing). These challenges create systemic issues that fundamentally alter how we think about property rights, the sovereignty of states, the moral obligations of manufacturers of mobile devices, and the ethics of offensive cyberwarfare (Brey, 2012).

### 2.1 Device Ownership and Autonomy

Traditional ethical perspectives understand that the act of ownership of a mobile device allows the owner of the device to autonomously control, secure, alter, and audit their property (ScienceDirect, n.d.). The hardware architecture of today replaces actual ownership and autonomy with an illusory sense of control (Brey, 2012). The Baseband Processor and BootROM are both autonomous components that occupy an opaque layer

underneath the Application Processor of a mobile device (Weinmann, 2012), which means that users cannot perform an integrity check on the embedded firmware or patch any discovered vulnerabilities (Brey, 2012). The manufacturers' intentional design of user's devices provides users with the primary means of communication (the cell phone) an extensive amount of control over the primary means of communication (the network), but at the same time places that control in the hands of the network provider. This amounts to a violation of the fundamental negative rights of users which are recognized by all governments as the basic human rights to be free from unwarranted tracking and surveillance (Alabama Policy Institute, 2020).

### 2.2 The National Sovereignty Crisis

The scaling of ethical issues from consumer level to macroeconomic level highlights an extreme crisis in nation states' sovereignty (Wilson & Donnelly, 2026). This hardware sovereignty paradox creates conflict between a sovereign nation needing complete control over its telecommunications infrastructure while the nation is being forced to rely on corporate designed hardware chips that are opaque and cannot be audited by entities outside of corporate control (Kitchin, 2017). The structure of a compartmentalized/global semiconductor supply chain means that nations must build national security apparatuses on top of proprietary rights of corporately designed BootROMs that have been manufactured by corporations that may be susceptible to potentially hostile countries (PwC, 2024). If a nation has its foundational hardware routing/controlling and its sensitive data located/control owned by an external corporate entity, that entity will ensure that the outcome of this control of hardware architecture will potentially hide its internal operations within the foundational hardware from everyone. The ethical consequence is that a nation can't claim to have true digital sovereignty over its foundational hardware (PwC, 2024).

### 2.3 The Threshold of Cyber Warfare and the Gray Zone

The ethical landscape of Unpatchable BootROM Vulnerabilities, which is influenced by current interpretations of International Law surrounding internet-based technological infrastructures (or hardware) is further complicated by the ambiguity of defining hardware-based attacks as acts of war. We contend that the current framework for defining cyber-attacks utilizes an out dated "Effects-Based" methodology, which states that, for an act to be considered an example of cyberwarfare (or acts of war), it must include an action which results in some sort of violent physical outcome (e.g. buildings destroyed by a bomb) that would be equivalent to an event caused by a kinetic weapon. However, since BootROM exploits do not demonstrate any immediate physical destruction/kinetic energies and effects, this allows nation-states to take advantage of a legal "gray area" (Wilson & Donnelly, 2026). In other words, an ethical analysis that anticipates future technological developments suggests a shift should be made towards a "Norms-Based" categorization that instead judges the act related to an intrusion based on the intentions aimed at target being affected, as opposed to when a kinetic invasion occurs or when any physical catastrophic consequences are demonstrated (Wilson & Donnelly, 2026). This represents a shift focusing on a malicious actor's intentions rather than assessing consequences after an event has occurred.

### 2.4 Vulnerability Hoarding and the Vulnerabilities Equities Process (VEP)

State actors face an ethical dilemma when they find a vulnerability in commercial hardware that has not been previously disclosed (e.g. a "zero-day" or "Forever Day" vulnerability) as an outcome. This involves issues related to intentionally choosing to leave a potentially harmful vulnerability undisclosed. State actors must choose between either disclosing vulnerabilities, so they can be patched, fixed, or using them for offensive cyberwarfare against other nations (Schwartz & Knake, 2016). This is also an ethical issue related to the character traits of state actors. In the United States, the "Vulnerabilities Equities Process" (VEP) exists to help balance the need to protect critical infrastructure from cyberattack, against the need to collect intelligence on malicious cyber actors (White House, 2017). Some commentators have argued that hoarding vulnerabilities disproportionately favors military capabilities over concerns about the public good. This means that vulnerabilities within hardware will remain indefinitely unpatchable since an undisclosed vulnerability could be exploited by anyone who gains access to it. By choosing not to disclose the zero-day or Forever Day vulnerabilities to the public after they have been found, the state has breached its ethical obligation of truthfulness to the public while also failing to safeguard and protect its citizens against exploitation by foreign adversaries (Willcockson, 2019).

### 2.5 The Tension Between Time-to-Market and Security Verification

The principle of "security by design" requires commitment to acting so that all products be thoroughly and formally verified before they are manufactured (CISA, 2023). This means that manufacturers are required to

show that their products as designed to be secure. Nevertheless, the economic reality shows that the total time devoted to rigorous hardware verification on average takes more than 55% of the total time involved in designing a typical System-on-a-Chip (SoC) (McKinsey, 2014). Architectural defects discovered late in the production process are exponentially more expensive to remediate; thus, to meet strict release dates, many semiconductor manufacturers intentionally choose to trade off risk involving vulnerability versus efficiency (McKinsey, 2014). Manufacturers who release immutable silicon (the physical component of a microprocessor) without performing an exhaustive formal verification process for Unpatchable BootROM Vulnerabilities are primarily acting in a way that exploits users as a means for the end of generating immediate profits for their corporation rather than ensuring long-term consequence of providing safety of the worldwide digital ecosystem (McKinsey, 2014).

## 3. Case Studies

It is essential to provide context for the theoretical risks posed by immutable silicon and the potential ethical violations these risks create through the actual deployments of these vulnerabilities. The case studies that follow will illustrate how BootROM flaws, Baseband paradoxes, and secure boot bypasses related to immutable silicon are implemented in practice.

### 3.1 Case Study 1: Checkm8 and the iOS BootROM

In 2019, a security researcher known as axi0mX discovered a serious hardware vulnerability known as "Checkm8". This vulnerability is a 'use-after-free' vulnerability in the BootROM of Apple's A5 to A11 processors (axi0mX, 2019). This vulnerability is in the BootROM, which is part of the silicon/processor and is therefore 'masked', so the vulnerability cannot be patched. For this reason, Checkm8 is a type of Forever Day, and this vulnerability will impact hundreds of millions of devices (axi0mX, 2019). An attacker can exploit the use-after-free vulnerability from the BootROM via specially crafted USB commands to gain arbitrary code execution at the highest privilege level. Once this occurs, all integrity-related security guarantees offered by the BootROM are broken (Apple, 2021). Since BootROM is a read-only memory, this permanent exploit opens a unique opportunity for the forensic community to conduct a fundamental investigation of secured proprietary hardware (Wu et al., 2021). The intentional introduction of the BootROM in Apple's A5 to A11 processors is a violation of Apple's corporate duties to customers. Users inherit vulnerabilities from corporations they cannot control.

### 3.2 Case Study 2: Fusée Gelée and the Nvidia Tegra X1

The "Fusée Gelée" exploit highlights how a single BootROM fault can have far-reaching implications across multiple industries (Temkin, 2018). Researchers discovered the exploit while researching the Nintendo Switch. The exploit exists on the Nvidia Tegra X1 processor (Temkin, 2018). To exploit this vulnerability, the researchers successfully utilized a technique called "voltage glitching" where they bypassed hardware read locks to dump the proprietary BootROM code for analysis (Temkin, 2018). This BootROM vulnerability was intentionally located by the manufacturer within the USB Recovery Mode (RCM) protocol, allowing an attacker to control the size of the memory operation arbitrarily, creating a catastrophic buffer overflow vulnerability. This buffer overflow can allow adversaries to gain Return Oriented Programming (ROP) code execution based on the context of a high-security mode, effectively defeating the hardware's root of trust. Variants of the Tegra SoC are used in essential industrial control systems within the automotive industry, creating the potential for catastrophic hardware-level compromise to vehicle infrastructure (O'Flynn, 2016). This is an unacceptable outcome (consequence) with potentially large-scale bad outcomes and don't accept responsibility for long-term safety within the automobile industry.

### 3.3 Case Study 3: Cisco ROMMON and Secure Boot Bypass

Trust Anchor Module (TAM) is a Trust Anchor module (TAM) used in Cisco routers and firewalls that use Field Programmable Gate Arrays (FPGA) to implement the secure boot process (Kataria et al., 2019). The TAM is intended to act as a physical immovable anchor for the device, which means that only digitally signed software images will be allowed to load into the ROM Monitor (ROMMON) (Cisco PSIRT, 2018). Despite this, some researchers found logic errors in the firmware that allowed an attacker to act in such a way as to manipulate the FPGA bitstream directly (Cisco PSIRT, 2022). By manipulating the FPGA Bit Stream, an adversary can completely bypass all the Trust Anchor's functions and inject stealthy persistent malicious implants into both the TAM FPGA and the application processor (Kataria et al., 2019). Forever-day vulnerabilities give attackers indefinite exploitation windows which bypass the Trust Anchor using hardware, an attacker is then be able to intercept or drop a very large volume of network traffic without detection (Kataria et al., 2019).

### 3.4 Case Study 4: Pegasus and the Baseband Processor

Amnesty International (2021) describes how mobile devices have been utilized as weaponized devices, citing the intentional use of Pegasus spyware deployed by the NSO Group to accomplish the use of the spyware as an outcome. Pegasus can directly access a target smartphone baseband processor through cellular frequencies and communicate with the target phone (Amnesty International, 2021). The attacker intentionally acts to exploit memory corruption vulnerabilities in the proprietary real-time operating system that runs the baseband processor (Amnesty International, 2021), which produces the outcome of allowing for remote code execution without having the target phone receive any alerts (Amnesty International, 2021). Using the baseband processor's large Direct Memory Access (DMA) privileges, Pegasus will transition to the smartphone's main system random access memory (RAM) while completely bypassing the Application Processor (AP) operating system Kernel (Mishra & Sahay, 2025). This level of compromise allows Pegasus to extract messages from the smartphone's RAM before they have been encrypted, clearly demonstrating that a secure application layer is vulnerable if the hardware on the smart phone on which it resides has been compromised (Amnesty International, 2021). Involuntary risk exposure users cannot patch or replace systems. Corporations must act in such a way as to prevent disproportionate harm.

## 4. Anticipatory Ethics

A reactive approach to ethical analysis of technological development and deployment is inadequate for achieving a meaningful result when evaluating a product built from unalterable silicon (Brey, 2012). Anticipatory Ethics is a future oriented ethical framework that studies potential ethical issues that may arise from new and emerging technologies before they are fully integrated into manufacturing processes and then into society. According to Brey, Anticipatory Technology Ethics (ATE) requires that we move beyond reactive judgements about the effects of technologies after an event has occurred to a proactive attempt to make forecasts of the dangers that these technologies pose. Anticipatory ethics seeks to identify, evaluate, and mitigate moral hazards during the design and deployment phases of emerging technologies, rather than reacting retroactively after technologies have been implemented and catastrophic failures have happened (Johnson, 2010). There is a need for an industry-wide commitment to ATE (Anticipatory Technology Ethics), an ethical framework that emphasizes the identification of ethical risks and potential harm to stakeholders during the R&D phase of developing new technologies, and prior to casting the product in silicon (Brey, 2012). So, what can be said about Unpatchable BootROM Vulnerabilities from the perspective of anticipatory ethics? They need to be corrected when the technology is being designed and before manufacturing products such as smart phones are manufactured.

### 4.1 ATE Framework and the Problem of Uncertainty

The future social impacts of emerging technologies are inherently uncertain, and this is the largest challenge for ATE analysis. (Brey, 2012). According to Brey, ethical foresight involves undertaking a systematic future directed analysis at multiple levels of technological foresight: analysis needs to focus on 3 levels a technology, an artifact, and the application of the technology and artifact (Brey, 2012). In the case of BootROMs, ATE requires creating what Brey refers to as "dark scenarios" (Brey, 2012) for the hardware architect to imagine how an adversary state with sufficient resources could exploit a read-only memory (ROM) flash chip or an unmitigated direct memory access (DMA) channel. The failure to foresee the possibility of weaponizing the USB recovery mode on the Tegra X1 SoC or the iOS BootROM are illustrations of a lack of thorough ATE at the artifact level (Temkin, 2018).

### 4.2 The Sociotechnical Imperative and ACM Rules

Keeping in mind Furrows distinctions introduced above we can combine the Anticipatory Technology Ethics framework with the ACM Code of Ethics to help define the moral obligations of developers of technology. (Miller et al., 2011). According to Miller's first rule for computing artifacts state, developers and designers are morally responsible for the foreseeable consequences of their artifacts (Miller et al. 2011). Without any form of patch to the un-patchable hardware, providing a radio random access memory (RRAM) chip with unrestricted Direct Memory Access (DMA) may constitute a highly foreseeable possibility of massive exploitation of the equipment developed using this chip. As described by ACM Rule 2.9, it is the ethical responsibility of professionals to create systems that are designed to be secure. Therefore, manufacturers that rush the fabrication of stored read only memory (ROM) code without proper verification and security are in violation of this rule thereby violating the obligation they owe to society structurally prioritizing corporate profit and time to market ahead of reporting on legitimate safety issues (ACM, 2018).

Moreover, smartphones and routers are two civilian oriented objects (artifacts) that contribute to basic communication, business operations, democratic elections and free press (Amnesty International, 2021). From the perspective of anticipatory ethics, the negative rights of the user, the right not to be subject to covert surveillance in their day-to-day lives, are built into the silicon of a piece of technology itself (Alabama Policy Institute, 2020). Ethical frameworks must also actively protect independent security researchers, who have been called the "white blood cells of the Internet." Security researchers need to be protected when they identify and find vulnerabilities from being punished by state actors when they find the vulnerabilities before adversaries can use their discoveries for malicious purposes. When researchers are punished for finding Unpatchable BootROM Vulnerabilities their efforts when punished can create a chilling effect on similarly situated researchers and leave many critical vulnerabilities unpatched, which directly violates ACM Principles 1.2 and 1.5.

## 5. Recommendations

According to current practices alterations to what becomes immutable silicon and Unpatchable BootROM Vulnerabilities must occur while the hardware is being designed. We propose the following actionable practices that should be intentional actions for cyber security. Security can no longer be retrofitted via software updates into mobile devices; it must be included in the design of the hardware of mobile artifacts at the design and manufacturing levels of the development of technology.

### 5.1 Formal Verification of BootROM Logic

To eliminate Forever Day exploits (Vasudevan et al., 2024), traditional software engineering's "test-and-debug" paradigm is not sufficient for the semiconductor industry. All Secure Boot hardware designs must be formally verified prior to fabrication, utilizing formal mathematical proofs to confirm conformity with the specification of a devices defined security specifications. The formal verification process tests all possible states of a set of specified parameters using methodologies such as model checking and theorem proving, all of which can produce very good results at identifying hidden logical defects in mobile devices (Vasudevan et al., 2024). Through formal co-verification, manufacturers can use formal verification techniques to mathematically prevent memory corruption type bugs from being created when implementing their design into mask ROM for mobile devices (Vasudevan et al., 2024).

### 5.2 Hardware Isolation via IOMMU

According to Mishra and Sahay (2025), unrestricted direct memory access (DMA) should be banned through regulative actions for all consumer and industrial devices. System architects need to design and create a physical firewall as hardware with an input-output memory management unit (IOMMU) (Mishra & Sahay, 2025). The IOMMU enforces access control by translating an I/O virtual address to a physical address, and it verifies permissions during the I/O page walk (Evtyushkin et al., 2021). If there is an exploit of a baseband chip through an RTOS exploit, the IOMMU should intentionally limit the threat actor to a physical isolated memory buffer, thereby preventing them from using DMA to pivot and access cryptographic keys or manipulate the application processor of a mobile device (Mishra & Sahay, 2025).

### 5.3 Open-Source Firmware and Verifiable Hardware Kill Switches

Governments must encourage a shift toward the use of Open-Source Real-Time Operating Systems (RTOS) for cellular modems to address the problem of hardware vulnerability pipelines while also decreasing their reliance on un-auditable foreign manufactured hardware (Dodge & Kitchin, 2017). The code in OS RTOS is open to review and subject to global scrutiny. The outcome is that this wide-range review process is considered by the Cybersecurity and Infrastructure Security Agency (CISA, 2023) as the most effective form of defense against supply chain weaponization. In addition to this, it is imperative that high-security devices include hardware-based kill switch functionality. A hardware kill switch is an electronically enabled physical switch that interrupts the electrical circuit supplying power to the Baseband Processor, thereby providing the only mathematically definitive method of maintaining radio silence, and preventing location tracking when the device is off (Purism, n.d.).

### 5.4 Reforming the Vulnerabilities Equities Process (VEP)

Improvement needs to be made to the Vulnerabilities Equities Process (VEP) to better classify software zero-days and unpatchable hardware and Forever Days differently (Schwartz & Knake, 2016). The U.S. and its allies should make significant changes to the VEP. This is especially true since BootROM vulnerabilities cannot be patched and without these types of vulnerabilities, hoarding them will continue to pose an ongoing threat to critical domestic infrastructure that is much greater than any temporary gain in intelligence (Schneier, 2012).

The VEP's charter should have an assumed requirement for immediate disclosure of all hardware-level or unalterable silicon vulnerabilities (Willcockson, 2019). Additionally, moving the administration of the VEP from the intelligence community to civilian cyber-security entities will ensure that protecting domestic assets is more important than developing and maintaining offensive capabilities.

## 6. Future Work

Anticipatory Technology Ethics and formal verification models must continue to evolve as research becomes available in new areas of interest such as:

Heterogeneous Edge Computing and 6G Networks: As the evolution of architecture for 6G take over critical computing infrastructure by directing it toward heterogeneous edge nodes, the attack surface is also expanding (Yuan et al., 2024). Future research should focus on preventing the possibility of utilizing edge-based BootROMs and for exploiting them as attack vectors to initiate cascading failures in 6G Zero Trust Networks (Yuan et al., 2024).

Integrating AI Into Real-Time Operating Systems (RTOS) and Data Poisoning: The introduction of artificial intelligence models being integrated into Baseband Processors will continue to change the attack surface for RTOS (Yuan et al., 2024). Anticipatory Technology Ethics and formal verification models should investigate how state actors may intentionally leverage AI to automate fuzzing of BootROM code to discover new Forever Days and investigate the impacts of data poisoning on on-device AI training (ISA, 2024).

Low Earth Orbit (LEO) Satellite Attack Vectors: The rollout of Direct-to-Cell Low Earth Orbit (LEO) satellite networks eliminates the need for localized infrastructure and establishes a direct line of sight to the Baseband Processor from space (Yuan et al., 2024). Anticipatory Technology Ethics and formal verification models must analyze how compromised satellite infrastructure could facilitate global, zero-click RTOS exploits, which would render local network defenses ineffective and irrelevant (Yuan et al., 2024).

## 7. Conclusion

The unpatched BootROM vulnerabilities and the weaponization of the Baseband Processor are examples of systemic problems in the designs that make up today's digital world (McKinsey, 2014). The technology industry has focused more on getting products to market quickly rather than on performing a complete formal verification for mobile device security, (Schneier, 2012) This has resulted in the existence of "Forever Days," (i.e., permanent flaws that will last for the physical lifetime of the device, so they can make it impossible to patch a flaw with a software fix). At the same time, granting opaque hardware free Direct Memory Access has created a known vulnerability that is continually being exploited by nation-state actors to bypass a secured boot chain, to take encrypted data from a device, and to conduct undetectable cyberwarfare (axi0mX, 2019). The result of these exploits is a violation of universally accepted ethical principles such as autonomy, related to owning your own device, respecting national sovereignty, and protecting civilian users from systemic damage (Brey, 2012).

The security of global critical infrastructure is an ongoing cyber threat, and hoarding of vulnerabilities under so-called Vulnerabilities Equities Process (Schwartz & Knake, 2016) will only further exacerbate this crisis by placing the security of global infrastructure at risk to gain temporary offensive advantages. The technology sector must turn to Anticipatory Technology Ethics to anticipate possible threats during product design and to provide security assurance before product manufacturing occurs via a process of rigorous Formal Verification (Vasudevan et al., 2024). Hardware isolation through IOMMU implementation, open-source firmware, and verifiable hardware kill switches must be in place to contain any potential device compromise and restore user autonomy (Mishra and Sahay, 2025). Without the implementation of these architectural requirements, the foundational silicon of our digital infrastructure will continue to be vulnerable to the long-term consequences caused by such an event as a Forever Day exploit.

**Ethics Declaration**: No human participants or personally identifiable information were involved. All data sources were publicly available.

**AI Tools Declaration**: ChatGPT 5.1 for drafting and refinement. Human authors verified all content. Gemini 3.0 pro used for aiding in sourcing.

## References

Alabama Policy Institute. (2020). *Understanding the difference between positive and negative rights.* Alabama Policy Institute. https://alabamapolicy.org/wp-content/uploads/2020/11/GTI-Brief-Positive-Negative-Rights-1-1.pdf

Amnesty International. (2021). *Forensic methodology report: How to catch NSO Group's Pegasus*. Amnesty International Security Lab. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Association for Computing Machinery (ACM). (2018). *ACM code of ethics and professional conduct*. https://www.acm.org/code-of-ethics

axi0mX. (2019). *Checkm8: Permanent unpatchable bootrom exploit for hundreds of millions of iOS devices*.

Brey, P. A. E. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13. https://doi.org/10.1007/s11569-012-0141-7

Check Point Research. (2020). *Achilles: Small chip, big peril. Vulnerabilities in Qualcomm's DSP chip*. https://blog.checkpoint.com/security/achilles-small-chip-big-peril/

Cisco Product Security Incident Response Team (PSIRT). (2018). *Cisco IOS ROM Monitor (ROMMON) Software Secure Boot Bypass Vulnerability*. https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180926-catalyst6800.html

Cisco Product Security Incident Response Team (PSIRT). (2019). *Cisco Secure Boot Hardware Tampering Vulnerability*. https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20190513-secureboot.html

Cisco Product Security Incident Response Team (PSIRT). (2022). *Cisco Secure Firewalls 3100 Series Secure Boot Bypass Vulnerability*. https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-fw3100-secure-boot-5M8mUh26.html

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*. https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

Dodge, M., & Kitchin, R. (2017). The challenges of cybersecurity for smart cities. https://personalpages.manchester.ac.uk/staff/m.dodge/Dodge_Kitchin_Challenges_of_Cybersecurity_for_Smart_Cities.pdf

Evtyushkin, D., et al. (2021). *Hardware-rooted trust for secure key management and transient trust*. https://www.cs.wm.edu/~dmitry/assets/files/evtyushkin-TDSC-preprint.pdf

Fan, M., Wu, Q., Yu, K., Xu, G., Wang, X., & Shu, J. (2025). Write-Once, Prove-Once: A Reusable Framework for Secure Boot Verification in Rocq. *IEEE International Conference on Software Engineering*.

Forever Day Bug. https://www.devx.com/terms/forever-day-bug/ December 14, 2023.

Goodin, D. (2012). *Backdoor in computer controls opens critical infrastructure to hackers*. Ars Technica. https://www.thecre.com/fisma/?p=3597

Google Project Zero. (2023). *Multiple Internet to baseband remote code execution vulnerabilities in Exynos modems*. Google Project Zero Blog. https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html

Grassi, P. A. (2018). The baseband processor: A brief overview. *Information Security Journal: A Global Perspective*, 27(1), 35-42.

Healey, J. (2017). *The U.S. Government and Zero Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*. https://georgetownsecuritystudiesreview.org/2017/03/28/balancing-zero-day-vulnerabilities-between-operational-capability-and-public-disclosure/

Heinrich, A., Stute, M., Cucu, T., & Hollick, M. (2022). Evil Never Sleeps: When Wireless Malware Stays On After Turning Off iPhones. *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*, 114–124.

ISA. (2024). *Global OT and IoT Threat Landscape Report 2025*. https://raw.githubusercontent.com/jacobdjwilson/awesome-annual-security-reports/main/Annual%20Security%20Reports/2025/Shieldworkz-Global-OT-and-IoT-Threat-Landscape-Report-2025.pdf

Johnson, D. G. (2010). Anticipatory ethics and the sociology of technology. *Science and Engineering Ethics*, 16(4),743-745.

Kataria, J., Housley, R., & Cui, A. (2019). *Direct FPGA Bitstream Manipulation Techniques for Bypassing Cisco Trust Anchor Module*. USENIX Workshop on Offensive Technologies (WOOT). https://www.usenix.org/system/files/woot19-paper_kataria_0.pdf

Khandelwal, S. (2014). *10th anniversary of the world's first mobile malware 'Cabir'*. The Hacker News. https://thehackernews.com/2014/01/World-first-Mobile-Malware-Cabir-hacking-news.html

Kitchin, R. (2017). The InSecurity of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*. https://mural.maynoothuniversity.ie/id/eprint/11588/1/Kitchin_Insecurity_2017.pdf

McKinsey & Company. (2014). *Standing up to the semiconductor verification challenge*. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Semiconductors/Issue%204%20Autumn%202014/PDFs/MoSC2014_Standing_up_to_the_semiconductor_verification_challenge.ashx

Miller, K. W., Wolf, M. J., & Grodzinsky, F. S. (2011). Moral responsibility for computing artifacts: 'The Rules'. *IT Professional*, 13(3), 57–59. https://doi.org/10.1109/mitp.2011.46

Mishra, J., & Sahay, S. K. (2025). Modern Hardware Security: A Review of Attacks and Countermeasures. *arXiv preprint arXiv:2501.04394*. https://arxiv.org/abs/2501.04394

Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smart phones for security analysis. *Proceedings of the 18th USENIX Security Symposium*, 321-338.

O'Flynn, C. (2016). *Fault Injection using Crowbars on Embedded Systems*. https://eprint.iacr.org/2016/810

Perez, C., & Slay, J. (2013). Mobile device forensics: Airplane mode and live data extraction. *Journal of Digital Forensics, Security and Law*, 8(4), 23-45.

Pot, Justin. What Is Apple's "Secure Enclave", And How Does It Protect My iPhone or Mac? ttps://www.howtogeek.com/339705/what-is-apples-secure-enclave-and-how-does-it-protect-my-iphone-or-mac/ Jan 22, 2018

Rambus Press. Hardware Root of Trust: Everything you need to know. https://www.rambus.com/blogs/hardware-root-of-trust/

Purism. (n.d.). *Hardware Kill Switches*. https://puri.sm/learn/hardware-kill-switches/

PwC. (2024). *Semiconductor and beyond 2026 full report*. https://www.pwc.com/gx/en/industries/technology/pwc-semiconductor-and-beyond-2026-full-report.pdf

Schneier, B. (2012). *Forever Day Bugs*. Schneier on Security. https://www.schneier.com/blog/archives/2012/04/forever-day_bug.html

Schwartz, A., & Knake, R. (2016). *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/governments-role-vulnerability-disclosure-creating-permanent-and-accountable

Temkin, K. (2018). *Fusée Gelée: Methodically Defeating Nintendo Switch Security*. https://arxiv.org/pdf/1905.07643

Vasudevan, S., Ravi, P., Jati, A., Bhasin, S., & Chattopadhyay, A. (2024). Formal Verification of Secure Boot Process. *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. https://past.date-conference.com/proceedings-archive/2024/DATA/756_pdf_upload.pdf

Weinmann, R. P. (2012). Baseband attacks: Remote exploitation of memory corruptions in cellular protocol stacks. *12th USENIX Workshop on Offensive Technologies (WOOT 12)*. https://www.usenix.org/conference/woot12/workshop-program/presentation/weinmann

What is the difference between a Bootrom vs bootloader on ARM systems. https://stackoverflow.com/questions/15665052/what-is-the-difference-between-a-bootrom-vs-bootloader-on-arm-systems.

White House. (2017). *Vulnerabilities Equities Policy and Process for the United States Government*. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

Willcockson, M. (2019). *Revamping the Vulnerabilities Equities Process*. National Security Law Journal. https://www.nslj.org/wp-content/uploads/Willcockson.Revamping-the-Vulnerabilities-Equities-Process.pdf

https://www.researchgate.net/publication/400977840_Smart_Phones_and_Current_Developments_in_Cyberwarfare_An_Ethical_and_Anticipatory_Ethical_Analysis

Wu, J., et al. (2021). A research of digital forensic method based on the Checkm8 heap vulnerability. https://www.researchgate.net/publication/358342823_A_research_of_digital_forensic_method_based_on_the_Checkm8_heap_vulnerability

Yuan, Y., et al. (2024). 6G Security Challenges and Potential Solutions. https://www.researchgate.net/publication/350824205_6G_Security_Challenges_and_Potential_Solutions