The Baseband Sovereignty Paradox: Anticipated Ethical and Technical Issues of Baseband Processors

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: Users and administrators of mobile devices focus on hardening the defenses of the devices to the application processors and Operating Systems (OS) of these devices. Meanwhile an unrestricted, parallel computing environment operates unchecked beneath the surface of these systems: the Baseband Processor (BP). This paper examines the "Baseband Sovereignty Paradox," where the chip responsible for cellular communication possesses Direct Memory Access (DMA) to the entire device while remaining completely opaque to the user, the main OS, and security software (Weinmann, 2012). The Baseband Sovereignty Paradox refers to the following items: A nation state wants full control over its mobile communications infrastructure, but must often rely on foreign, opaque, un-auditable baseband chips and firmware. This paradox creates a strategic dependency that directly undermines state centered technological and national sovereignty (Brey, 2012). The relevance of these items to cyberwarfare can be described as follows: Baseband compromises allow within mobile devices deep, persistent access invisible to OS defenses. Nation-states can weaponize baseband vulnerabilities for the purposes of disruption of communications, espionage, and supply-chain cyber-attacks and interference. The reliance on foreign basebands by nation states becomes a potential geopolitical attack vector, while putting future cyber network generations potentially at strategic risk. In this analysis we follow a standard conceptual analysis where define concepts and terminology related to the baseband paradox which are then applied to case studies. examine historical precedents, such as the Pegasus spyware, to demonstrate how the BP in mobile devices can be exploited to gain SYSTEM privileges, bypass encryption, and exfiltrate data (Amnesty International, 2021). This research highlights the persistent nature of baseband communications in mobile devices, which maintain contact with cell towers even when the device is in "Airplane Mode" or powered down, which allows them to act as an unmitigable tracking beacons. We argue that the Baseband Processor constitutes a "Fifth Column" for cyber warfare. Baseband processors are a ubiquitous, privileged, and unmanageable hardware component within mobile devices that fundamentally undermine the concept of user privacy and device ownership and control (Johnson, 2010). Our analysis will conclude with an ethical and anticipated ethical analysis of The Baseband Sovereignty Paradox which when exploited by adversaries can used in support of cyberwarfare.

Keywords: Baseband processor, Sovereignty paradox, Direct Memory Access (DMA), Fifth column cyberwarfare, Anticipatory ethics, Pegasus spyware

1. Introduction

Within the modern digital landscape, the smartphone has been transformed into an object that is at the center of the lives of those who own them. They are no longer merely devices for sending calls and text messages. Smartphones now serve a variety of purposes including being a financial ledger, a biometric database, a location tracker, and a primary means for professional and personal communication. Since these devices are central to so many lives, countless resources are invested in the security of smartphones. iOS and Android are constantly audited by companies like Apple, google, and independent contractors are hired to patch and strengthen the security of the smartphone mobile Operating System (OS). These actions are focused on application sandboxing which is the process of isolating an application from the rest of the system (Apiiro, n.d.), e. g. isolating end-to-end encryption for secure communications, and from user permissions. This focus on the user-oriented goals neglects a vulnerability that is present in smartphones. This vulnerability is beneath the Application Processor (AP) end of operations, where there is a parallel computing environment that is the Baseband Processor (BP).

Baseband Processors are responsible for cellular network communications, they manage complicated radio frequences that are necessary for connecting to 3G, 4G LTE, and 5G networks. The Baseband Processor is not designed to interact with the user; it is designed to operate independently, which separates its vulnerabilities from the user end Application Processor within smartphones. Baseband Processors run their own proprietary Real-Time Operating System (RTOS) environments where closed source firmware is executed in separation from the user and from the Operating System of the main device.

The separated parts of a smartphone's technical architecture are what this paper defines as the "Baseband Sovereignty Paradox." This paradox affects both macroeconomics and geopolitics. Sovereign nations and their intelligence agencies attempt to secure their military communications infrastructure, but to participate in the

modern world they are required to rely upon foreign and unsuitable baseband chips that are manufactured by a few select entities like Qualcomm, MediaTek, Samsung, and Huawei. This reliance upon foreign manufacturers for advanced products like baseband chips that are then used in military devices, creates a strategic dependency that threatens to undermine national sovereignty and national security. Can a state establish true sovereignty over its digital infrastructure if the hardware that it runs on is manufactured by foreign entities that intentionally obscure their manufacturing processes?

This paper argues that Baseband Processors are the Achilles heel of smartphones in the context of cyber warfare. The Baseband Processor acts as an embedded, highly privileged, and unmanageable hardware component that lays dormant in the smartphones of every citizen, politician, and military leader in the developed world. It undermines the concept of user privacy and device ownership by serving as a silent back door that can be activated without the user ever knowing it has been activated. By examining the technology behind baseband processors, case studies where baseband exploitation is involved, and an application of traditional and anticipatory ethics, this analysis can explore the ethical violations and strategic implications of the Baseband Sovereignty Paradox. Recommendations can then be developed about how to confront the Baseband Sovereignty Paradox in cyberwarfare in the twenty first century. Therefore, this paper seeks to answer the following research question: How does the lack of clarity and privileged access of the Baseband Processor threaten national sovereignty and user autonomy, and what ethical frameworks should guide the mitigation of these vulnerabilities? Ethical issues will be related to the conceptual distinctions involving according to Furrow, 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)

2. Technical Issues

A true understanding of the ethical and strategic threats from smartphones can only be gained by first understanding the technical architecture behind the Baseband Processor and the immense power it exercises over the mobile device. Modern mobile devices are in effect two different computers that share a chassis and power source. The first computer is the Application Processor (AP), which is a chip that runs the main Operating System like Android or IOS and handles user interfaces as well as high-level computations. In essence, the Application Processor is the one the user interacts with when they open their phone, play a game, watch a video, or make a call. The second computer is the Baseband Processor (BP), which is a chip dedicated to managing complicated, time-sensitive radio protocols that enable cellular communication. The user cannot make a call on the Application level without the Baseband Processor first connecting them to the network. The technical vulnerabilities of Baseband Processors can be divided into four unique domains: Real-Time Operating Systems (RTOS), the implementation of Direct Memory Access (DMA), the extreme opacity of the firmware, and the persistence of the component's operational state (Weinmann, 2012).

2.1 Real Time Operating System (RTOS)

When cellular networks operate, they require strict timing. A mobile device communicates with the network by sending and receiving packets, which are just bundles of information that allow for inter-device communication. Transferring packets is simple and would not require its own processor, except that mobile devices pose unique challenges: they need packet transfer to occur in the order of microseconds to maintain a connection. They need to be able to manage the switching of connection from tower to tower while the user moves and manages signal degradation as the user gets farther from the tower to which they are connected. The Application Processor is incapable of doing this because it gets bogged down by user apps and graphics rendering which eats up CPU cycles, meaning it cannot meet the strict timing requirements that a cellular connection requires (Mulliner & Miller, 2009). To address this need, developers made the Baseband Processor run on a Real Time Operating System (RTOS), which is designed to process data as it arrives without buffering as is common in normal Operating Systems. RTOS is a highly efficient solution for radio signaling. The problem lies in their design being crafted in the 1990’s and early 2000's. The first mobile malware named ‘Cabir’ was discovered in 2004 (Khandelwal, 2014), which means when RTOS were being invented, security had not yet become an important concern. RTOS environments are dependent on codebases that were developed during the lax security era and are still in use today. Various patches have been developed to attempt to secure them, such as Qualcomm’s REX or different implementations of ThreadX (Weinmann, 2012). These are legacy systems which masquerade as modern software and are inherently fragile and susceptible to memory corruption vulnerabilities (Weinmann, 2012). These legacy RTOS environments frequently lack modern software mitigations, such as Address Space

Layout Randomization (ASLR) and stack cookies, making over-the-air memory corruption attacks from fake base stations significantly easier to execute (Grassi, 2018).

2.2 Direct Memory Access (DMA) and Privilege Escalation

Baseband Processors need to rapidly transmit large amounts of data (video streams, voice calls) to the main processor so the user may interact with the content, which creates a logistical problem because piping massive amounts of data through the central CPU would bottleneck the device. The solution developers found was Direct Memory Access (DMA) for the Baseband Processor. To accomplish this the Baseband Processor requires system privileges, the most powerful set of permissions one can have. Direct Memory Access is important, it allows the baseband chip to read from and write to the device's main Random Access Memory (RAM), bypassing the CPU, the main OS, and any security protocols. DMA is extremely efficient, but the cause for alarm from the perspective of cybersecurity. This is not malicious or negligent on the part of the developers, it was a genuine solution to an engineering problem, but a solution that must be re-examined in the modern cyber threat landscape. If the Baseband Processor was not privileged, malicious radio signals or SMS attacks would not be cause for worry, but with DMA the attacker can take control of every aspect of the mobile device. This would allow attackers to manipulate the OS kernel, extract cryptographic keys, bypass screen locks, and access encrypted messages before they are encrypted or after they are decrypted. The main memory is a trusted hardware component, meaning OS-level security is blind to it, thus completely blind to the intrusion (Check Point Research, 2020).

2.3 Obscurity and Proprietary Components

The systems mobile devices run on are highly proprietary and guarded by the few corporations that manufacture them. This means that baseband firmware is proprietary, and that independent researchers and academic institutions are unable to legally audit the code that runs on the Baseband Processor to locate vulnerabilities. This is the security through obscurity model, when the vulnerabilities exist, and given that they run on millions of lines of C/C++ code, which they likely do, they are only going to be discovered by well-funded nation-state intelligence agencies, or private cyber arms dealers who stockpile "Zero-Day" exploits. The end user, the device manufacturer, and even the national government relying on these devices have no means of independently verifying that the baseband firmware on their devices is free of backdoors or critical flaws (Check Point Research, 2020).

2.4 Persistence and Unmitigated Tracking

The final technical issue regarding Baseband Processors is persistence. Baseband Processors are designed to prioritize network connectivity, which means they are always looking to communicate with cell towers. When a user selects the option "Airplane Mode" on their mobile device the assumption is that communications to and from the mobile device are severed. The main Operating System updates their user interface to display an icon of an airplane, that creates what amounts to an illusion of being disconnected. In many mobile device architectures, airplane mode is just a software instruction from the Application Processor to the Baseband Processor asking it to stop transmitting user data. The Baseband Processor does not shut off, it continues to connect to and passively listen to cellular towers, and in some cases, it will still perform low level handshakes with the network to ensure the user reconnects quickly once airplane mode is disabled (Perez & Slay, 2013). When a user powers their device "off: it does not physically sever the connection to the Baseband Processor. When the off button is pressed the mobile device enters a deep sleep state where the Application Processor is powered down, but this is not strictly true for the Baseband Processor, notably in iOS 15+, the "Find My" functionality remains in a low power state and can be tracked by iOS devices on the same network. While it does not ping towers, it can still be used as an unmitigable tracking beacon. If the device has battery power, the baseband processor can still periodically wake up, allowing an attacker to potentially triangulate in on the position of a target that has a compromised phone in the off state (Heinrich et al., 2022).

3. Ethical Issues

The technical realities of the Baseband Processor generate ethical issues that fundamentally change the relationship between humans, their personal technology in the form of smartphones, and the state. We assume Furrow's ethical distinctions involving an agent's intentions, actions and outcomes apply to the Baseband Sovereignty Paradox and to the designers of baseband processors. The designers of baseband processors have intentions, perform actions and produce outcomes. Through an examination of the hardware architecture and traditional ethical frameworks from the intentions of different types of agents, we can identify

three main ethical issues with Baseband Processors: the degradation of agency over an individual's mobile device, the undercutting of national sovereignty, and the exploitation of a digital Achilles heel.

3.1 Device Ownership and Autonomy

At the most fundamental ethical level, the Baseband Processors architecture creates a pervasive illusion of device ownership. Within traditional property and privacy ethics ownership implies the inherent right to control, secure, and modify one's property (ScienceDirect, n.d.). Because the BP operates autonomously beneath the Application Processor and remains completely opaque to the user, the main OS, and security software, this control over the device is a facade. The designers of baseband processors ignore the outcomes related to the actions of the users of the devices.

Users cannot audit the firmware, patch new vulnerabilities or monitor the Baseband Processors background processes. Since the Baseband Processor has DMA to the entire device, the user is essentially a tenant in their own device. The device serves the cellular network provider and the manufacturers digital imperatives long before it serves the users security needs. Using the framework of anticipatory ethics and the philosophy of technology, Philip Brey (2012) argues that technology is not morally neutral, there are inherent power dynamics that control the technology without the user's explicit consent. When manufacturers design a device where the user's control over the primary communication node is tenuous at best, manufacturers of the technology are removing the individual's digital autonomy. The result of this lack of control is a ubiquitous and unmanageable hardware component that undermines the ethical issues related to user privacy and device ownership.

3.2 The National Sovereignty Crisis

The ethical issues arising from the Baseband Sovereignty Paradox created by the designers of the technology scales past the individual level to a macroeconomic level revealing a national sovereignty crisis. This paradox posits a set of conflicting features with mobile devices. On the one hand, a state has the intention of wanting full control over its mobile communication infrastructure, while on the other hand it relies on opaque foreign baseband chips and firmware. In the digital age sovereignty only exists if communications can be secured that are free from foreign interference for sensitive information, is a nation sovereign if hackers can listen in on conversations pertaining to national security? The realities of the compartmentalized global supply chain are that governments must build their military and national security communications on top of a proprietary baseband chip often produced by a foreign entity. This creates a strategic dependency upon companies whose host nations might be adversaries, which directly undermines national sovereignty. The ethical issue lays in the complicity of the state, where the government produces an outcome that includes knowingly subjecting their citizens and military personnel to hardware that cannot be audited and that can possibly be covertly weaponized. A nation cannot claim true sovereignty if the foundational hardware routing its data in mobile devices is controlled by a foreign corporate or state entity capable of obscuring its internal operations. Supply chain reliance on foreign basebands becomes a potential geopolitical attack vector, while future network developments and new generations deepen the strategic risk.

3.3 The Digital Achilles Heel Concept

This dynamic for Baseband Processors establishes what we identify as a digital Achilles heel. Historically an Achilles heel is a colloquial phrase meaning a surprising weakness in an otherwise strong individual (Gill, 2019). With the Application Processor and mobile Operating Systems are constantly being patched and hardened against attacks, as they are the obvious target, we argue that this otherwise strong/secure device having a more vulnerable Baseband Processor constitutes an outcome that is an Achilles heel. Baseband processors are embedded, privileged entities that is carried into secure military bases, government offices, and private homes. Since any baseband compromise would allow deep and persistent access to devices invisible to mobile device security, this makes it possible for malicious agents to act so that such devices become the perfect target for anyone who wishes to conduct cyber warfare or espionage. Nation states that force populations to rely on this architecture means that a society implicitly accepts a baseline of vulnerability that violates fundamental ethical norms of security and autonomy, transforming every smartphone into a dormant cybersecurity vulnerability.

4. Case Studies

To support these technical and ethical claims, there must be real-world examples that provide an insight into the vulnerabilities related to the Baseband Sovereignty Paradox. These cases demonstrate how the theoretical vulnerabilities of the Baseband Processor can translate into breaches in device security, privacy and international telecommunications infrastructure. This paper uses a qualitative case-study methodology. The four case studies

were selected to represent a diverse spectrum of the Baseband Sovereignty Paradox: targeted nation-state spyware (Pegasus), mass supply-chain hardware flaws (Qualcomm DSP), localized rogue infrastructure (Washington D.C. Stingrays), and zero-click remote execution (Samsung Exynos).

4.1 Pegasus Spyware

The NSO Group's Pegasus spyware represents the pinnacle of modern mobile espionage. The reality of this threat was established in 2021 when a consortium of media outlets and Amnesty International released the "Project Pegasus" report, forensically confirming the successful, covert infection of devices belonging to human rights activists, journalists, and politicians globally (Amnesty International, 2021). This was an intentional action on the part of the designers of the Pegasus spyware While early iterations of Pegasus required users to click malicious links, the 2021 forensic analysis revealed a shift toward zero-click network injections. NSO Group was documented selling tactical network injection equipment, hardware acting as rogue cell towers, that interacts directly with the baseband to push malicious payloads. Once the spyware successfully compromises the baseband or leverages its Direct Memory Access (DMA) capabilities, it operates entirely beneath the level of jurisdiction of the OS kernel. This low-level compromise allowed Pegasus to silently extract the contents of messages directly from the device's RAM before they were encrypted for transmission, activating microphones and harvesting location data without leaving standard forensic traces on the Application Processor.

4.2 Supply Chain Reality

A geopolitical threat that involved supply chain consolidation was demonstrated in august 2020 when over 400 vulnerabilities were discovered in Qualcomm's Digital Signal Processors (DSPs). The DSP interacts with the baseband to process audio, video, and telecommunication data. Security researchers at Check Point showed that these vulnerable Qualcomm chips were in approximately 40% of the world's smartphones at the time of discovery. 40% includes models from companies like Google, Samsung, LG, and Xiaomi (Check Point Research, 2020). These flaws were not merely theoretical, researchers proved that they could use these exploits to record calls, steal data, embed malware that could survive a factory reset, and do it all without the user interacting with the device or knowing about the exploits. The moral character of the manufacturers and designers of Qualcomm chips with their many vulnerabilities is morally problematic. The scale of this discovery demonstrated the reality that a single manufacturer's obscured legacy firmware could instantly destabilize the communications infrastructure of almost the devices for nearly half the world.

4.3 Washington D.C. Rogue ISMI Catchers

The exploitation of the baseband's processor's intention to connect to the strongest cell signal can be executed via International Mobile Subscriber Identity (IMSI) catchers, colloquially known as Stingrays. This was proven to be an active cyberwarfare tactic used on U.S. soil in 2018. In a letter to congress the Department of Homeland Security (DHS) officially acknowledged the discovery of several unauthorized rogue ISMI catchers that were operating in Washington D.C., including near the White House and the Pentagon (Department of Homeland Security, 2018). Foreign intelligence operatives utilized these rogue cell towers to force the basebands of nearby smartphones to connect to them instead of legitimate carrier networks. By doing so, the attackers forced the targeted basebands to downgrade their encryption to legacy, broken protocols such as 2G GSM. This documented event allowed foreign actors to intercept calls, read unencrypted texts, and precisely triangulate in on the physical locations of government personnel. This action produced an outcome that is morally suspect. Crucially, this event highlighted the deceptive nature of smartphone UI (user interface). Even if personnel utilized "Airplane Mode," the baseband's persistent listening state meant the device could still be pinged and tracked by these rogue towers.

4.4 Exynos Internet-to-Baseband Exploits

In March 2023, the reality of automated, mass-scale baseband exploitation was confirmed when security researchers at Google's Project Zero publicly disclosed 18 severe zero-day vulnerabilities in Samsung's Exynos baseband chipsets. These chips were actively embedded in millions of global devices, including Google's own Pixel 6 and 7 series, various Samsung Galaxy models, and wearable devices (Google Project Zero, 2023). Most alarmingly, Project Zero confirmed that four of these vulnerabilities (including CVE-2023-24033) allowed for Internet-to-baseband Remote Code Execution (RCE) with absolutely zero user interaction (Google Project Zero, 2023). To execute the attack and compromise the device, the threat actor only needed to know the victim's phone number. By sending specially crafted data over the cellular network, the attacker exploited a memory corruption flaw in the baseband's firmware. Because the baseband automatically parsed the incoming cellular data before notifying the main OS, the malicious code executed silently. This historical disclosure proved that

basebands could grant attackers a persistent, high-level foothold on the device without the user ever receiving a notification, touching their screen, or realizing they were under attack. In effect the user of a device is being used as a means for an attacker's intended goal.

5. Anticipatory Ethics

Anticipatory Ethics is a future oriented ethical framework that attempts to identify potential ethical issues that arise from new and emerging technologies before they are fully integrated into society. As defined by Phillip 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 forecasting 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 catastrophic failures happen (Johnson, 2010). Because the Baseband Processor determines the fundamental communication capabilities of global society, hardware engineers and software developers must be held to strict anticipatory and professional standards (Ciulla, Martin, & Solomon, 2013). Applying the "Moral Responsibility for Computing Artifacts" framework by Miller et al. (2011), alongside the Association for Computing Machinery (ACM) Code of Ethics, clarifies the moral obligations breached by the current baseband architecture. These concepts are applied to the dimensions that Furrow states as related to the intentions, actions and outcomes produced by agents.

5.1 The Foreseeability of Effect (Rule 1) and Robust Security

Rule 1 of Miller's framework states that "The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact" (Miller et al., 2011). In the context of baseband architecture, granting an opaque, internet-facing radio chip unrestricted Direct Memory Access (DMA) to the main system memory by developers makes mass exploitation entirely foreseeable. The zero-click vulnerabilities observed in the Samsung Exynos chips (Case 4) and the supply chain flaws in the Achilles discovery (Case 2) were not anomalies; they were the predictable result of fragile, legacy code executing with maximum privileges.

Under the ACM Code of Ethics Rule 2.9 ("Design and implement systems that are robustly and usably secure"), developers are mandated to implement structural safeguards against such foreseeable breaches (Association for Computing Machinery, 2018). Hardware manufacturers who knowingly design basebands with unchecked DMA violate this rule, so they bear direct moral responsibility for the cyberwarfare vulnerabilities facilitated by this reckless architectural choice.

5.2 The Sociotechnical Imperative (Rule 4) and Avoiding Harm

Rule 4 states that "People who design... can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded" (Miller et al., 2011). Smartphones are fundamentally civilian artifacts embedded within the sociotechnical systems of journalism, healthcare, banking, and democratic elections. By designing a device that prioritizes network connectivity and intelligence-gathering capabilities over verifiable user security, manufacturers actively ignore this civilian context. This disregard directly conflicts with ACM Rule 1.2 Avoid harm. When nation-states hoard baseband vulnerabilities to deploy tools like Pegasus (Case 1) rather than reporting them to be patched, they cause systemic harm to global smart device infrastructure.

5.3 Negative Rights, Deception, and Privacy

Furthermore, the deceptive user interface design of "Airplane Mode" (Case 3) constitutes a severe ethical breach. Users possess a fundamental "negative right" a right to be free from unwarranted tracking, interference, or surveillance by external actors (Alabama Policy Institute, 2020). By designing an interface that creates a false sense of security while BP continues to act as an unmitigable tracking beacon, engineers designing baseband processors eliminate the informed consent of users. This violates ACM Rule 1.6 Respect privacy by engineering interfaces that explicitly mislead users about the transmitting state of their hardware.

6. Recommendations

To resolve the Baseband Sovereignty Paradox and dismantle the "Fifth Column" nature of modern mobile devices, which creates an attack vector for cyber-attacks and cyber warfare, a paradigm shift from software-level security to hardware-level enforcement is required. We propose three actionable technical mandates to reestablish device sovereignty:

6.1 Hardware Isolation via IOMMU

The most critical vulnerability of BP is its unrestricted Direct Memory Access. An outcome that should be expected of manufacturers is that they must implement strict Input-Output Memory Management Units (IOMMU) at the hardware level. An IOMMU acts as a physical firewall between the baseband and the main system memory. Instead of the BP having free rein over the entire RAM, the IOMMU restricts the BP to reading and writing within a tightly controlled, isolated memory buffer. If the baseband is compromised by a zero-click radio exploit, the threat actor is trapped within this restricted buffer and cannot pivot to access the OS kernel, extract cryptographic keys, or manipulate user data.

6.2 Open-source Baseband Firmware

The paradigm of "security through obscurity" has demonstrably failed, leaving national infrastructure dependent on opaque, foreign supply chains while making this infrastructure vulnerable to cyber-attacks. Telecommunication standards bodies and governments have the ethical responsibility of mandating a transition toward open-source Real-Time Operating Systems (RTOS) for cellular modems. Just as open-source operating systems like Linux benefit from rigorous global scrutiny, baseband firmware must be auditable by independent academic and security researchers. Transparency removes the strategic dependency on foreign black-box chips and serves as the only sustainable defense against supply-chain weaponization.

6.3 Verifiable Hardware Kill Switches

Software toggles cannot be trusted to secure a device from remote exploitation or persistent tracking via IMSI catchers. Smartphones designed for government, military, or privacy-conscious civilian use must be manufactured with physical, hardware-level kill switches. These switches must physically break the electrical circuit providing power to the Baseband Processor and its associated antennas. Only a physical severing of power can provide a verifiable guarantee of radio silence, neutralizing the unmitigable tracking beacon effect and restoring absolute control of a device such as a smartphone to the device owner.

7. Limitations

Since Baseband firmware is proprietary and legally protected, this analysis relies entirely on publicly disclosed vulnerabilities and third-party forensic reports such as from Amnesty International or Google Project Zero. There are likely undiscovered or undisclosed vulnerabilities that could not be considered for this paper. There may also be undisclosed patches to what we believe are current existing vulnerabilities to which we simply do not have no access. Relying on public data creates an inherent selection bias, since we can only produce analysis based upon what is publicly available.

8. Future Work

As the global telecommunications infrastructure transitions to 5G Advanced and anticipates the rollout of 6G, the complexity of baseband firmware will grow exponentially. Future research must analyze the security implications of integrating Artificial Intelligence (AI) directly into the Baseband Processor's RTOS to manage complex radio spectrum allocations. Furthermore, the advent of Direct-to-Cell Low Earth Orbit (LEO) satellite internet (such as Starlink and AST SpaceMobile) introduces a novel attack vector. Future work should investigate how baseband vulnerabilities might be exploited from space-based infrastructure, completely bypassing terrestrial cell towers and rendering localized geographic defenses obsolete.

9. Conclusion

The Baseband Sovereignty Paradox exposes a catastrophic flaw in the architecture of the modern digital ecosystem. While users and administrators focus on hardening the Application Processor, a sovereign, parallel computing environment operates unchecked beneath the surface of operating systems. By granting the Baseband Processor Direct Memory Access and wrapping its operations in proprietary opacity, manufacturers have created an embedded, unmanageable "Fifth Column" in devices owned by nearly every citizen.

This architecture systematically undermines device ownership, violates fundamental negative rights to privacy, and makes problems the technological sovereignty of nation states. As demonstrated by zero-click exploits, supply chain vulnerabilities, and persistent tracking mechanisms, the baseband is not merely a communication node; it is the primary vector that can be exploited for modern cyberwarfare. Reclaiming control requires an urgent abandonment of "security through obscurity" in favor of hardware-level isolation, open-source auditing,

and verifiable physical kill switches. Until these architectural mandates are enforced, the smartphone will remain an unmitigated threat to both personal privacy and national security.

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, July 18). *Forensic methodology report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Apiiro. (n.d.). What is application sandboxing? Challenges & best practices. https://apiiro.com/glossary/application-sandboxing/

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

Brey, P. A. E. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13.

Check Point Research. (2020, August 6). *Achilles: Small chip, big peril. Vulnerabilities in Qualcomm's DSP chip*. https://research.checkpoint.com/2020/achilles-small-chip-big-peril/

Ciulla, J. B., Martin, C. W., & Solomon, R. C. (2013). *Honest work: A business ethics reader* (3rd ed.). Oxford University Press.

Department of Homeland Security (DHS). (2018, March 26). *Letter to Senator Ron Wyden regarding unauthorized IMSI catchers in the National Capital Region*. National Protection and Programs Directorate.

Furrow, Dwight. Ethics Key concepts in Philosophy, Continuum Press, 2005.

Gill, N. S, (2019, November 19) *What is an Achilles' Heel? Definition and Mythology.* Thoughtco. https://www.thoughtco.com/what-is-an-achilles-heel-116702

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

Google Project Zero. (2023, March 16). *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

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

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

Khandelwal, S. (2014, January 27). *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

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

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

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

ScienceDirect. (n.d.). *Right of ownership*. https://www.sciencedirect.com/topics/social-sciences/right-of-ownership

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