International Journal of Innovative Research in Electronics and Communications (IJIREC)
*Volume 10, Issue 1, 2025, PP 1-7*
*ISSN 2349-4050 (Online) & ISSN 2349-4042 (Print)*
*https://doi.org/10.20431/2349-4050.1001001*
*www.arcjournals.org*

# Investigating Class 0 SMS Exploits in 5G and Future 6G Architectures

**Dr. Christos P. Beretas, MSc, Ph.D***

*Professor at Innovative Knowledge Institute, France*

***Corresponding Author:** ***Dr. Christos P. Beretas, MSc, Ph.D,*** *Professor at Innovative Knowledge Institute, France*

**Abstract:** *Class 0 SMS, commonly known as Flash SMS, is a little-known yet powerful feature in mobile networks that allows silent delivery of messages without storing them on the recipient's device. Originally designed for urgent communication and network testing, this feature has increasingly drawn attention from cybersecurity researchers due to its potential misuse in surveillance, location tracking, and network probing all without user awareness. While most studies have focused on its impact in legacy systems like GSM and 3G, far less is understood about how Class 0 SMS functions or is exploited within the evolving frameworks of 5G and the emerging 6G networks. This research explores how Class 0 SMS can be leveraged or abused in the context of modern cellular architectures, particularly focusing on 5G networks and early proposals for 6G design. We begin by examining how this message type is handled by current network cores (including 5G NSA and SA modes), highlighting variations across mobile carriers and device types. Through practical experiments and network simulations, we assess the feasibility of using Class 0 SMS for undetected user tracking, signaling-layer attacks, and silent reconnaissance across different generations of mobile connectivity. The research also investigates whether 6G proposals—designed with stronger security and AI-based network management sufficiently account for threats stemming from legacy protocol support like Class 0 SMS. Our findings suggest that despite advancements in authentication and encryption, certain backward-compatible mechanisms may continue to pose serious privacy risks if not carefully addressed. Finally, the paper proposes a set of mitigation strategies, including network-level filters, anomaly detection models, and policy updates, aimed at curbing misuse of this silent channel. As mobile networks grow increasingly intelligent and interconnected, understanding and securing overlooked vectors like Class 0 SMS becomes essential to preserving user trust and privacy in next-generation communications.*

**Keyword:** *Class 0 SMS, 5G security, 6G networks, privacy threats, silent SMS exploits, mobile surveillance*

## 1. Introduction

Mobile communication has evolved dramatically over the past two decades, with each new generation of wireless technology bringing faster speeds, lower latency, and more intelligent network design. Today, 5G networks are being deployed globally, promising transformative applications such as smart cities, autonomous vehicles, and massive IoT integration. Meanwhile, the foundations of 6G are already being laid, with early discussions pointing toward even more pervasive connectivity, AI-driven network optimization, and tighter integration of the digital and physical worlds. While these advancements have undoubtedly improved the performance and potential of mobile systems, they have also introduced new challenges related to privacy, security, and legacy system compatibility. One of the less examined but increasingly relevant aspects of mobile communication security is the role of Class 0 SMS—also known as Flash SMS or Silent SMS. Unlike regular text messages, Class 0 SMS messages are displayed instantly on the recipient's screen but are not stored on the device, and in many cases, users may not even notice their arrival. In certain configurations, they can be received silently without triggering any visual or audio notification. Originally intended for urgent or time-sensitive notifications, Class 0 SMS has found a secondary, more controversial use: covert surveillance. Law enforcement and intelligence agencies in several countries have reportedly used silent SMS messages as a means of location tracking by triggering signaling exchanges with the mobile network. These messages can force devices to respond at the network level, enabling approximate geolocation without the user's awareness or consent. As mobile networks become more sophisticated, the question arises: do newer architectures like 5G and the proposed 6G frameworks offer better safeguards against this form of silent probing, or do they unknowingly preserve an outdated vulnerability? This research aims to critically examine how Class 0 SMS functions within 5G infrastructures and how it may be exploited in the context of future 6G network designs. By conducting both empirical testing across real-world 5G deployments and theoretical analysis aligned with current 6G proposals, we assess whether existing security mechanisms are sufficient to prevent abuse of this silent communication channel. In doing so, we also consider the implications of continued support for legacy features in next-generation systems—a common but often risky aspect of ensuring backward compatibility. Understanding and addressing the potential misuse of Class 0 SMS is especially urgent as mobile networks increasingly underpin essential services and digital identities. Without clear protections, this seemingly innocuous feature could continue to pose a quiet yet persistent threat to user privacy and trust in mobile communication. This study contributes to the broader field of network security by highlighting a specific, under-discussed vector of attack and recommending proactive measures that network operators, device manufacturers, and standards bodies can adopt moving forward.

## 2. Analysis

Class 0 SMS was initially designed as a tool for delivering high-priority messages directly to a user's screen, bypassing the typical inbox and avoiding long-term storage on the device. While the feature has legitimate uses, such as sending real-time alerts or system notifications, its silent and ephemeral nature also makes it a convenient tool for covert surveillance. Unlike traditional SMS messages, Class 0 SMS can be sent and received without the user being aware, especially when implemented in a network environment that suppresses notifications. This characteristic has made it an attractive option for both lawful and unlawful tracking practices. The exploitation of Class 0 SMS has been documented in several contexts, including use by law enforcement agencies in various countries. Reports have revealed that Silent SMS can be used to silently ping a device, prompting it to communicate with cell towers and generate signaling events that can then be used to approximate the device's location. This method of location tracking **does not rely on GPS or Wi-Fi**, and it bypasses the standard permissions that apps must obtain from users. As a result, it presents a unique threat to user privacy, particularly because it is nearly invisible to the average user.

In 5G networks, while there are numerous advancements in encryption, authentication, and network slicing, many of the legacy features from previous generations remain supported for the sake of backward compatibility. This includes support for SMS messaging, including Class 0 SMS. Since many 5G deployments operate in non-standalone (NSA) mode, relying on existing 4G infrastructure, the vulnerabilities associated with Class 0 SMS are still very much present. Even in standalone (SA) 5G networks, where a clean slate approach is more feasible, mobile operators often retain support for legacy services to accommodate a wide range of devices and user needs. The situation becomes even more complex as we look ahead to 6G. Although still in the conceptual stage, 6G is expected to integrate artificial intelligence deeply into network management, utilize new frequency spectrums such as terahertz bands, and support ubiquitous connectivity across physical and digital environments. However, there is a risk that, in the push for innovation, the fundamental issues of legacy protocol vulnerabilities could be overlooked. If features like Class 0 SMS are not explicitly addressed in the design phase of 6G, they may continue to pose privacy risks even in the most advanced communication systems. The use of Class 0 SMS for surveillance is not merely a theoretical concern. Documented instances have shown that such messages are actively used for tracking individuals, particularly in law enforcement and intelligence contexts. While these activities are often conducted under legal frameworks, the transparency and oversight surrounding their use are frequently lacking. This creates a grey area where privacy can be infringed upon without adequate justification or user consent. In some cases, Silent SMS has been used during protests or against journalists, raising serious ethical and legal questions.

One of the most troubling aspects of Class 0 SMS is its invisibility. Because it typically does not generate notifications or leave traces on the device, users are often completely unaware that they have been targeted. This makes it incredibly difficult to detect and counteract. Even advanced security software may fail to log or identify these messages unless specifically configured to do so. As a result, Class 0 SMS represents a persistent blind spot in mobile privacy protections. In terms of network behavior, the sending of a Class 0 SMS can prompt a variety of actions from the receiving device, depending on the implementation. In some cases, the phone may generate signaling messages that are logged by the network, which can then be used to determine the device's approximate location. In others, it may trigger a more complex sequence of interactions that reveal information about the device, such as its model, software version, or other identifying characteristics. These capabilities make Class 0 SMS a valuable tool not only for tracking but also for network reconnaissance and potentially even targeted attacks. The scale of the threat increases significantly in the context of modern and future mobile networks. As 5G continues to roll out and 6G looms on the horizon, the number of connected devices is set to explode. This includes not just smartphones, but also smart home devices, connected vehicles, wearable technology, and critical infrastructure systems. Each of these devices represents a potential target for privacy invasion via Class 0 SMS or similar techniques. The more dependent we become on these connected systems, the more severe the consequences of such privacy breaches become.

Addressing the threat posed by Class 0 SMS requires action on multiple fronts. Mobile network operators have a critical role to play in detecting and filtering suspicious SMS traffic. By implementing advanced monitoring tools and anomaly detection systems, operators can reduce the likelihood of successful exploits. Device manufacturers and operating system developers also bear responsibility. By increasing transparency around the reception of Class 0 SMS and offering users the option to block or log such messages, they can empower individuals to take control of their privacy. From a policy perspective, regulatory bodies need to catch up with the technological realities of modern communication. Legislation should be updated to explicitly cover the use of legacy features like Class 0 SMS, including clear guidelines on when and how they can be used, who has access to them, and what oversight mechanisms are in place. There should also be international cooperation to ensure that privacy protections are not undermined by cross-border differences in policy or enforcement. In terms of future research, there is a need for in-depth analysis of how Class 0 SMS is handled across different network implementations and device types. Researchers should also explore the development of machine learning models capable of identifying unusual SMS traffic that could indicate a privacy breach. Additionally, there should be a concerted effort to design future mobile communication protocols that are resilient to such forms of silent exploitation from the ground up. The story of Class 0 SMS is a cautionary tale about the risks of retaining legacy features in modern systems without adequate scrutiny. While the feature itself may have legitimate uses, its potential for abuse is significant and should not be underestimated. As we look forward to a future defined by ubiquitous connectivity and intelligent networks, it is crucial that we also invest in the protections needed to keep those networks safe and private. The opportunity to address these issues exists now, before 6G becomes a widespread reality. If we fail to act, we may find ourselves facing the same privacy challenges only this time, on a much larger and more integrated scale. Building trustworthy communication systems requires more than just technological advancement; it demands a commitment to ethical design, transparent governance, and active engagement with the public. Only by addressing the silent threats that linger in our networks can we ensure that progress in connectivity does not come at the cost of individual privacy and societal trust.

The core issue with Class 0 SMS lies in its silent and ephemeral nature. Because these messages do not typically notify the user audibly or visibly and are often not logged, they provide a stealthy method for interacting with a device. When sent to a mobile phone, a Class 0 SMS may prompt the device to respond to the network in subtle ways, such as through signaling exchanges or location updates. These seemingly innocuous actions can be harnessed by malicious actors to track users, identify devices, and probe the network for weaknesses all without the user's knowledge. This makes Class 0 SMS a valuable tool in the toolkit of surveillance operations and cyberattacks. The transition to 5G has introduced numerous improvements in speed, reliability, and capacity. Network slicing, edge computing, and improved encryption protocols are just a few of the features that make 5G a promising foundation for future digital infrastructure. However, many 5G deployments, particularly those in non-standalone (NSA) mode, still rely heavily on existing 4G infrastructure. This reliance includes the continued use of outdated communication protocols such as SMS, and by extension, Class 0 SMS. Despite the security improvements in 5G, this backward compatibility opens the door for attackers to exploit legacy vulnerabilities.

In practical terms, an attacker who has access to the mobile network—or who can simulate access through rogue base stations or compromised infrastructure can send Class 0 SMS messages to target devices. These messages are capable of eliciting signaling responses that provide information about the device's current location or status. When repeated at intervals, this technique allows for real-time tracking of an individual, even if GPS is disabled. Because Class 0 SMS messages often do not appear in message logs, there is little chance the user will realize they are being surveilled. This makes it an ideal method for covert monitoring. In more advanced use cases, attackers can use Class 0 SMS to map the network behavior of a target. By analyzing the signaling messages generated by the device in response to these SMS triggers, a malicious actor can gather information about network configurations, identify weaknesses, and prepare for more targeted attacks. For example, identifying which security protocols are in place—or whether fallback mechanisms can be exploited—can be a crucial step in launching more complex network intrusions. These reconnaissance efforts, while not directly harmful on their own, pave the way for deeper compromises. The rise of connected devices in the 5G era further complicates the landscape. Beyond smartphones, the network now supports **IoT devices**, connected vehicles, wearable technologies, and smart infrastructure. Many of these devices may not be designed with high security in mind and could be even more vulnerable to SMS-based exploits. A connected traffic light or smart utility meter may not receive traditional SMS messages in the same way a phone does, but if its communication module is based on legacy standards, it could still respond to a Class 0 SMS. This widens the threat surface significantly and introduces potential vulnerabilities in systems that are critical to public safety and daily life. Looking ahead to 6G, the vision is one of hyper-connectivity, seamless integration between physical and digital worlds, and AI-driven network optimization. While these advancements hold great promise, they also raise concerns about security and privacy. If legacy vulnerabilities like Class 0 SMS are not addressed at the design stage, they may persist into these future architectures. The more deeply integrated and intelligent the network becomes, the greater the risk that a silent exploit could have wide-reaching consequences. For instance, a Class 0 SMS exploit in a 6G-enabled smart city environment could potentially be used to track high-value targets, disrupt services, or manipulate data flows.

Exploiting vulnerabilities in Class 0 SMS is not merely a hypothetical risk. There have been well-documented cases of its use in law enforcement operations, particularly in Europe. Agencies have used it to monitor suspects under legal frameworks that do not always offer robust safeguards for privacy. While such use may be justified under certain conditions, it also creates a precedent for less scrupulous actors to deploy the same techniques for purposes that are far more intrusive and less accountable. Without proper oversight and transparency, these capabilities can easily be misused. Compounding the issue is the lack of user awareness and technical transparency. Most users have no way of knowing whether they have received a Class 0 SMS. Many mobile operating systems do not alert users to these messages, nor do they provide logs or settings to manage them. Even advanced security tools may not be configured to detect such activity unless explicitly designed to do so. This invisibility makes it difficult for individuals to protect themselves or even recognize when their privacy is being violated. From a network perspective, detecting and mitigating the abuse of Class 0 SMS requires sophisticated monitoring systems. Mobile network operators must be able to identify unusual patterns of SMS traffic, especially messages that do not result in user-visible interactions. This includes implementing heuristics and behavioral analytics to flag potentially malicious use. However, deploying such systems at scale is not trivial, especially given the need to balance performance, user privacy, and legal compliance. Additionally, not all network operators have the resources or motivation to prioritize this form of threat detection. To reduce the risks associated with Class 0 SMS, several measures can be considered. First, mobile operating systems should provide users with visibility into all SMS messages received, regardless of their class. By allowing users to view and manage Class 0 SMS, the opacity that makes these messages dangerous would be significantly reduced. Second, network operators should implement filtering mechanisms that either block suspicious Class 0 SMS messages or log them for further analysis. Third, industry standards should be updated to reflect modern security expectations, potentially phasing out legacy features that are no longer necessary.

Policy and regulation also play a critical role. Governments should review and update their telecommunications laws to ensure that the use of Silent SMS for surveillance is subject to clear limitations and accountability. International cooperation will be necessary to harmonize these regulations, particularly as mobile devices frequently roam across borders. Privacy should not be sacrificed in the name of convenience or compatibility, and legal frameworks must evolve alongside technological capabilities to safeguard individual rights. In research and academia, greater attention should be given to the study of silent exploits and network-layer attacks. The subtlety of these threats often means they are overlooked in favor of more visible or dramatic exploits. However, as the foundation of mobile communication becomes more complex and critical, even minor vulnerabilities can have major implications. By investigating how Class 0 SMS is implemented in various devices and network types, researchers can help expose weak points and propose targeted solutions. The integration of machine learning into network management—as envisioned in 6G offers new possibilities for detecting and responding to silent threats. AI-driven systems can analyze vast amounts of signaling data in real time to identify patterns indicative of an exploit. However, this requires transparency in how such systems are trained and governed. Otherwise, we risk replacing one invisible system with another, potentially compounding the issues of trust and accountability. The conversation around Class 0 SMS also touches on broader themes of digital rights and ethical technology. As surveillance capabilities become more advanced and less detectable, there is a pressing need for societies to decide where the line should be drawn. The ability to track a person without their knowledge using a feature most users have never heard of raises serious ethical questions. These are not just technical challenges they are societal ones. The future of mobile communication is undeniably exciting. With each generation, we gain new tools to connect, share, and innovate. But progress must not come at the expense of privacy and security. By acknowledging and addressing the silent threats that persist in our networks—like those posed by Class 0 SMS we can help ensure that the benefits of 5G and 6G are realized without compromising the fundamental rights of users. This means building systems that are not only fast and powerful, but also secure, transparent, and worthy of trust.

In the projected environment of 6G, where communications are expected to be instantaneous, context-aware, and deeply integrated with AI-driven applications, the consequences of such silent capabilities are multiplied. A single Class 0 SMS in a 6G network could interact with an intelligent agent managing the device’s connections, location reporting, and even authentication flows. Such interactions, if left unmonitored or unsecured, offer a path for unauthorized data access, real-time location tracking, or broader system manipulation. Unlike previous generations, 6G is not merely about increased speed or reduced latency. It is about embedding communication into the very essence of daily life connected homes, automated industries, remote surgeries, autonomous vehicles, and more. Each of these touchpoints represents a potential entry for threat actors. A Class 0 SMS, cleverly crafted and precisely timed, could trigger a response from a smart device that then ripples through the connected ecosystem. For example, an autonomous vehicle receiving a silent SMS could be prompted to engage in an unnecessary handshake with a base station, revealing its location or operational state to a third party. Or a medical monitoring device might be subtly queried to emit a signal confirming its operational parameters. These are not far-fetched possibilities, but logical extrapolations of how such messages might exploit device behavior in a hyper-connected world. The challenge of Class 0 SMS in the 6G era also involves the persistent reliance on legacy protocols. Despite the push toward futuristic infrastructure, backward compatibility remains a staple in mobile network design. This is partly due to the need for supporting a broad range of devices and use cases, including those in regions where cutting-edge hardware adoption is slow. However, this commitment to compatibility inadvertently extends the life of outdated and insecure features. It allows legacy vulnerabilities like the ones exposed by Class 0 SMS—to continue existing in systems that should, in theory, be more secure. In 6G’s vision of AI-managed networks, the way Class 0 SMS is handled might differ significantly depending on the context-aware interpretation of the message by the system. An AI agent might treat such a message as routine or benign unless specifically trained to identify potential abuse patterns. This opens up a dangerous possibility: silent exploitation that bypasses even the most advanced intrusion detection systems simply because the attack vector is seen as a legitimate function. If these AI-driven systems are not explicitly trained to recognize the nuanced threats posed by Class 0 SMS, they may unwittingly enable surveillance or data leakage. Privacy is another domain where the risks multiply. One of the central promises of 6G is the support for personalized, experience-centric services. These services often require collecting and processing vast amounts of user data, from location and biometrics to preferences and behavioral patterns. While safeguards such as decentralized data storage and encrypted communication are anticipated features of 6G, the silent, unacknowledged interaction introduced by Class 0 SMS can undermine these protections. For instance, a user might assume their location data is private and secured by encryption. However, if a Class 0 SMS is used to elicit a network signaling response, that data can be inferred externally, circumventing encryption entirely. The difficulty in countering Class 0 SMS exploits lies in their subtlety. Most users remain unaware that such a mechanism even exists. Few mobile devices offer options to view, block, or log Class 0 messages. Even among cybersecurity professionals, Class 0 SMS is often overlooked in threat models due to its low visibility and seemingly benign functionality. This makes it an ideal channel for persistent threats. A malicious actor seeking to monitor an individual over time could send periodic Class 0 SMS messages to determine their presence on the network, track movements across geographic areas, or even map out the times when a device is active orinactive.

In 6G networks, where devices may be contextually aware and interact with users through adaptive interfaces, even minor deviations triggered by such messages could have cascading effects. An AI assistant that adjusts room lighting or security settings based on perceived user presence might be fooled into making adjustments based on signals derived from Class 0 SMS-triggered responses. These seemingly minor breaches of logic could, under the right circumstances, lead to substantial violations of privacy and security. It's also important to consider how such vulnerabilities intersect with broader societal risks. In a world where surveillance technologies are increasingly deployed by both state and non-state actors, the ability to monitor individuals without their knowledge or consent becomes a powerful tool. Journalists, activists, political figures, and even ordinary citizens can become targets. In nations where freedom of speech is under threat or where surveillance laws are poorly regulated, the silent surveillance enabled by Class 0 SMS poses a serious human rights risk. Its use may not leave digital trails visible to the average user, making it especially difficult to challenge or even prove. Regulatory frameworks are often slow to catch up with technological innovation. While some countries have introduced laws aimed at curbing unauthorized digital surveillance, very few address the specific mechanisms through which such surveillance is executed. Class 0 SMS remains largely absent from the legislative discourse, despite its potential to undermine user consent and data protection principles. As 6G moves from theory to reality, there is an urgent need for updated regulatory perspectives that encompass the full range of legacy and emerging threats. Mitigating the risks associated with Class 0 SMS in 6G will require a multi-pronged approach. From a technical standpoint, network operators and device manufacturers must revisit the role of legacy messaging protocols. Where feasible, these should be deprecated or at the very least, monitored with the same rigor as newer communication standards. Devices should be designed with user transparency in mind, allowing users to view and manage all incoming messages, including those of Class 0. AI systems managing 6G networks must also be trained to recognize and appropriately respond to the risks posed by silent communications. This could involve anomaly detection systems that flag repeated or patterned Class 0 SMS messages, particularly those targeting sensitive devices or systems. Importantly, these defenses must be designed with privacy in mind, ensuring that mitigation itself does not become another vector for intrusion. From a policy perspective, international standards bodies and privacy regulators need to collaborate in developing clear guidelines around the use and control of legacy features like Class 0 SMS. These should include requirements for transparency, auditability, and user control. Public education campaigns can also play a role in raising awareness, helping users understand the risks and demand better protections from service providers. The issue of Class 0 SMS in 6G networks is not just a technical problem—it is a question of how much control individuals have over their digital existence. It challenges the assumption that more advanced systems are inherently more secure and forces a re-examination of what privacy means in a hyper-connected, AI-managed world. As networks become smarter and more autonomous, the lines between benign functionality and exploitative behavior can blur. Class 0 SMS is a reminder that even the smallest loophole, if left unchecked, can become a doorway to significant harm.

## 3. Conclusion

As we reflect on the evolution of mobile networks and the increasing sophistication of our digital environments, it becomes clear that the conversation around privacy can no longer afford to overlook the subtler, more ingrained vulnerabilities that persist in our systems. Class 0 SMS, a legacy feature that has largely flown under the radar for most users, represents one such vulnerability—a seemingly innocuous communication tool that, in the wrong hands, becomes a gateway to silent surveillance and unauthorized tracking. In the context of 5G networks, which are built to deliver faster speeds, reduced latency, and improved user privacy, the continued presence of Class 0 SMS support feels paradoxical. While 5G has introduced important advancements in encryption and user authentication, its partial reliance on older 4G infrastructures leaves open back doors for exploits. The persistence of features like Class 0 SMS, despite being outdated in function, exposes a critical flaw in the design philosophy of modern networks: the assumption that backward compatibility must come at the cost of privacy. Looking ahead to 6G, the stakes only get higher. With the promise of fully integrated AI, real-time decision-making, and unprecedented connectivity across people, devices, and infrastructure, the margin for error becomes smaller. A single overlooked exploit like the ability to trigger network interactions through a silent message could have widespread consequences. In such a hyper-connected environment, privacy breaches could ripple through systems faster and more deeply than ever before. What makes Class 0 SMS particularly concerning is not just its technical capability, but the invisibility with which it operates. Most users are unaware it exists. Fewer still realize that their devices can be silently queried, leaving no trace in message logs, no audible notification, and no obvious sign of intrusion. This kind of vulnerability doesn't scream for attention; instead, it quietly bypasses the very protections that users assume are in place.

This issue isn't just about individual devices. In the broader context of connected cities, smart healthcare, autonomous vehicles, and the Internet of Everything, silent exploits like these have the potential to impact societal infrastructure. Imagine systems being quietly monitored, user behavior being mapped without consent, or sensitive information being inferred through seemingly minor signaling triggers all without the affected parties ever realizing it happened. The ethical implications are just as serious. While some may argue that such tools are necessary for law enforcement or national security, the lack of oversight, accountability, and transparency around their use creates a slippery slope. Without clear regulation, Class 0 SMS can easily become a tool for abuse targeting activists, journalists, or everyday citizens without their knowledge or consent. The absence of public awareness and legal safeguards exacerbates the risk, placing far too much power in the hands of those who control the network. To move forward, the industry must take a hard look at what it means to build truly secure and privacy-respecting networks. This means more than just improving encryption or adding another layer of security it means revisiting legacy functions and asking whether they still belong in future infrastructures. Class 0 SMS, with its silent nature and potential for misuse, should either be transparently managed or responsibly deprecated. Device manufacturers and OS developers have a role to play in making these interactions visible and controllable to end users. Network operators need better tools to detect and filter out suspicious SMS behavior. Regulators must step in to define the legal boundaries of such technologies, ensuring they are used ethically, if at all, and always with accountability. And above all, users deserve to know when their privacy is at risk even when the risk doesn’t make a sound. The journey toward 6G gives us a rare opportunity to rethink the foundations of mobile communication. If privacy is to remain a fundamental human right in the digital era, then it must be built into every level of network design from protocol handling and AI decision-making to policy enforcement and public transparency. Ignoring the quiet risks, like those posed by Class 0 SMS, would be a disservice to the very future we are working to create. Class 0 SMS may seem like a small piece of a much larger puzzle, but as with any system, the smallest gaps often lead to the biggest breaches. Recognizing and resolving these silent threats now before 6G becomes a global standard is not just good security practice. It’s a necessary step toward building a more trustworthy, privacy-first digital future.

## REFERENCES

[1] Khan, L. U., Yaqoob, I., Imran, M., & Guizani, M. (2022). *6G Wireless Systems: A Vision, Architectural Elements, and Future Directions*. IEEE Acces.

[2] NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology.

[3] Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., & Poor, H. V. (2019). *6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies*. IEEE Vehicular Technology Magazine.

[4] Arapinis, M., Mancini, L. V., Ritter, E., & Ryan, M. (2014). *New privacy issues in mobile telephony: Fix and verification*. Proceedings of the 2012 ACM Conference on Computer and Communications Security.

[5] Traynor, P., Lin, M., & McDaniel, P. (2008). *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*. Proceedings of the 16th ACM Conference on Computer and Communications Security.

**Citation:** *Dr. Christos P. Beretas, MSc, Ph.D,(2025). Investigating Class 0 SMS Exploits in 5G and Future 6G Architectures “International Journal of Innovative Research in Electronics and Communications (IJIREC), vol 10, no. 1, 2025, pp. 1-8. DOI:* https://doi.org/10.20431/2349-4050.1001001.