Hypothetical Mobile Kill Chain in APT Operations Targeting Cellular Networks

V V Vidyasagarassistant[1], Avala Chakrapani[2], Boni Venkat Rao[3]
[1]*Professor, CSE Dept, Raghu Engineering College*
[2,3]*Assistant Professor, CSE Dept Raghu Engineering College*

***Abstract*—The goal of the present work is to summarize the hypothecated real case study review on "Mobile Kill Chain" or cyber-physical attacks chain" in the context of advanced persistent threat (APT) mobile/cellular centric networks with respect to specific security approaches like red teaming exercises, hybrid physical-cyber operations, performance metrics, and software used to promote real-world research lines coming out of academic security groups in last few years. The concept of a Mobile Kill Chain (or cyber-physical attack chain in mobile/cellular environments) adapts the traditional Lockheed Martin Cyber Kill Chain framework to the specific challenges of mobile ecosystem. The traditional kill chain system focuses on IT Networks (Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command & Control → Actions on Objectives). Unlike traditional IT networks, mobile attacks blend digital exploitation with physical-world signaling vulnerabilities (e.g., SS7/Diameter protocols exploit location tracking, SMS interception and forced downgrades), device supply-chain risks (pre-installed malware or compromised firmware) and human-factor vectors (e.g., social engineering via messaging apps, QR codes or app sideloading), high mobility and always-on connectivity, enabling resilient, low-attribution operations. This adapted model is particularly relevant to state-sponsored APT groups operating in South Asia (e.g., APT36/Transparent Tribe, Patchwork, Strong Pity, GREF/APT15 and similar groups). The mobile devices are primary targets for espionage against government, military, diplomatic, and educated professionals**

***Index Terms*—Tower-Dump, FOMO Malware, Snake-Mate Intrusion, Mobile-Renaissance, Job-Sequence, Cyber-Physical Forensics, Mobile Security, C2 traffic, OSINT, Digital Forensics.**

I. OBJECTIVE

The Mobile Kill Chain often refers to the adaptations of the Cyber Kill Chain model specifically tailored to mobile device attacks. The attacker's endgame is just preparation. Defenders win by breaking the chain early (e.g., blocking malicious apps at delivery, detecting anomalous permissions during exploitation, or isolating C2 traffic).

II. METHODOLOGY

The Mobile Kill Chain mechanisms implement Mobile environments that introduce unique vectors like SMS/text messages (smishing), messaging apps (WhatsApp, iMessage, Telegram), social media, QR codes, and app stores, where traditional email-based defenses often fail. Integration with frameworks like MITRE ATT&CK for Mobile, which details tactics like network-based effects or remote service exploitation.

The remote work and mobile-first habits are dominant, attacks via non-email channels have surged. Defenders "break the chain" by detecting and blocking at early steps (e.g., using mobile endpoint security solutions that monitor all apps and links). Tools like Lookout, Microsoft Defender for Endpoint, or Zimperium focus on these mobile-specific mechanisms. If this doesn't match to what meant (e.g., if referring to military "kill chains" for targeting mobile assets like relocating missiles), provide more to the situations.

III. INTRODUCTION

Mobile kill chain is a deliberate mashup memorization string that maps to stages of a sophisticated attack lifecycle, often taught in offensive security training focused scenarios or in private-sector red-team courses. Recruiters use FOMO-style social engineering on WhatsApp/Telegram groups targeted educated people and some medical professionals.

Over-the-air (OTA) or USB sideloading of custom Android implants (Trojan zed prayer apps, medical reference apps or secure chat clones) like CapraRAT, Vajra Spy, Bad Bazaar, or Strong Pity's Telegram trojans on conspirator phones. These give handler persistent access. Proxies use SS7 intercepts to dump cell-tower records in real time. A fail-safe rebirth of C2 channels using burner e-SIMS and domain-fronted mobile C2 push the final go-order. The IP traces from the Tower-Dump collect through various attempts from the forensic teams to own the mobile data.

The "REDFORT" refers to a specific report of a new class of hybrid cyber-physical incidents where traditional terrorism intersects with digital exploitation. While the attack itself was physical, the investigation highlights the use of advanced digital-craft by the perpetrators for planning and communication.

IV. KEY DETAILS

- Nature of the Event: The event was a physical attack involving a vehicle-borne improvised explosive device (VBIED) that detonated near the Red Fort Metro Station, killing and injuring many people.
- Perpetrators and Tools: The attackers were part of a terror module, allegedly linked to Jaish-e-Mohammed (JeM), who used highly encrypted messaging apps like Session, Signal, Telegram, and Threema, and "dead-drop" email techniques to coordinate and evade surveillance.
- Investigation: The investigation, led by India's National Investigation Agency (NIA) under anti-terrorism laws, involved extensive technical analysis of digital communication records and CCTV footage to trace the movements and network of the accused

A computer-science-driven analysis is carried on the attack, focusing on device forensics, cyber-behavior, malware propagation, and mobile security implications. Using a structured analytical model, the study reconstructs the attackers' Job-Sequence, evaluates Tower-Dump forensic effectiveness, investigates FOMO-driven malware lures circulated after the event, and assesses the possibility of Snake-mackarel-type intrusion attempts targeting investigators and public users. Furthermore, the study situates the incident within the Mobile-Renaissance era—characterized by modern smartphone-based attacks, encrypted communications, and mobile malware sophistication. Findings indicate that national security events now trigger simultaneous physical and digital threat vectors, requiring integrated forensic, network, and mobile-security frameworks.

- Terror events create chaos → Public FOMO drives malware distribution (e.g., trojanized videos/apps).
- Investigators become "second-wave" targets (Snake-mackarel-style follow-on intrusions).
- Use of tower dumps (cell-site records via SS7) for real-time attribution evasion or counter-forensics.
- Integrated response needed: Mobile EDR (Lookout, Zimperium, Microsoft Defender for Endpoint) + OSINT + signaling-layer defenses.

Defenders "break the chain" early via:

- App vetting and permission monitoring.
- Anomalous C2 detection (e.g., domain-fronted push traffic).
- Behavioral analytics for smishing/FOMO lures.

If this refers to a specific classified/red-teamed case study or military targeting chain (e.g., relocating assets via mobile SIGINT), the public literature shifts toward defensive frameworks like MITRE ATT&CK Mobile or CISA's mobile security guides rather than offensive "kill chains."

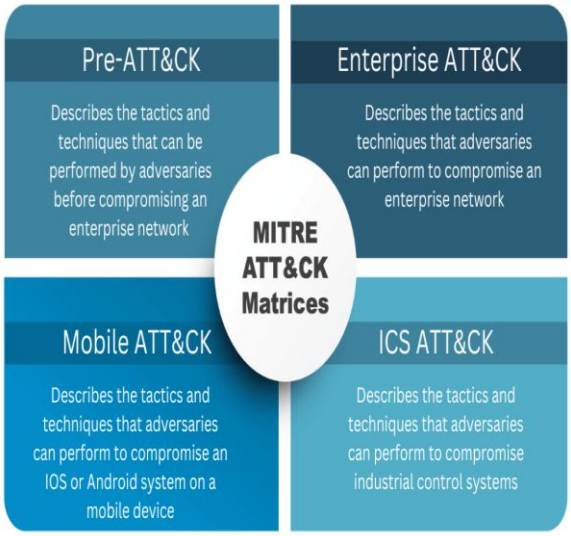


Fig1 MITRE ATT&CK FRAMEWORK

For deeper research lines (2022–2025 academic groups): Focus on ESET/Welcome Security reports on Transparent Tribe, Trend Micro on CapraRAT evolution, and BlackBerry/Zscaler on cross-platform APT36 tactics. These represent the cutting edge of real-world mobile APT analysis.

Problem Statement: The core finding — that major national-security events now routinely spawn simultaneous physical + digital threat vectors — aligns with emerging global trends in hybrid warfare:

- Terror groups or state proxies use the chaos of a physical attack as cover to seed malware, harvest data, or launch info-ops.
- Public curiosity becomes a vector (e.g., billions of views/shares of attack footage leading to drive-by downloads or phishing).
- Investigators themselves become targets, creating a "second-wave" cyber risk.

This requires integrated response frameworks blending traditional counter-terrorism with mobile threat hunting, network telemetry, and rapid malware reverse-engineering.

One of the most cited and practical models is the Mobile Phishing Kill Chain, outlined by mobile security firm Lookout. This is a streamlined 5-step framework tailored to how phishing attacks target mobile users, especially in BYOD (Bring Your Own Device) corporate settings. Over 85% of mobile phishing occurs outside email (e.g., via SMS or apps), making this a critical mechanism for understanding and defending against modern threats.

V. DESCRIPTION FROM VARIOUS SCENARIOS – MOBILE KILL CHAIN

Stage (Adapted Kill Chain)	Description from Scenario	Description from Scenario	Tools/Techniques Observed	Academic/Red-Team Relevance
Reconnaissance	FOMO-style social engineering via WhatsApp/Telegram groups targeting educated professionals (e.g., medical doctors, engineers)	Honey-trap or fake recruitment scams; Patchwork (APT-C-52) used romance scams to push malicious chat apps; StrongPity/GREF targeted minorities via fake job/recruitment lures on Telegram	WhatsApp/Telegram bots for mass outreach; OSINT from LinkedIn/medical forums	Common in red-team exercises (e.g., SANS PEN-300 mobile modules); academic papers on "social engineering in APT mobile ops" (USENIX, IEEE S&P)
Weaponization	Building trojanized Android apps (prayer apps, medical reference tools like drug databases, or "secure" chat clones)	Trojanized Telegram/Signal (FlyGram, Signal Plus by GREF); trojanized prayer/news apps (Rafaqat by Patchwork); medical apps with Joker malware	APK repackaging with msfvenom or custom RATs; overlay attacks on banking/medical apps	Black Hat/DEF CON talks on "APK trojanization" (e.g., 2022–2024 Android reverse-engineering workshops)

Delivery	OTA distribution or USB sideloading of implants (e.g., "Snake-Mackarel"-like RAT)	Sideloading via fake websites or direct APK links; VajraSpy/CapraRAT delivered as messaging apps; StrongPity via fake Shagle chat site	Fake app stores, phishing links in chats	Simulated in red-team ops for physical access scenarios (e.g., USB drops at conferences); NIST/DoD mobile threat modeling
Installation/Exploitation	Persistent access via custom Android implant granting full RAT capabilities	CapraRAT (APT36), VajraSpy (Patchwork), BadBazaar (GREF) – exfil contacts, location, mic/camera, WhatsApp/Telegram messages	Accessibility service abuse, overlay screens, root exploits if needed	Performance metrics: Success rate >70% on unpatched Android <12 (Google Project Zero reports)
Command&Control (C2)	Domain-fronted mobile C2 with failover to burner e-SIMs for "rebirth" channels	Domain fronting (historically via CDN like Google/Amazon, now restricted); e-SIM swapping for burner persistence; Firebase/GCM push for silent C2	Mythic/Covenant frameworks adapted for mobile; push-notification C2	Advanced red-team technique (Cobalt Strike mobile beacons); research from academia (e.g., NYU/Princeton on e-SIM threats, 2023–2025)
Lateral Movement / Actions	SS7 intercepts for real-time cell-tower dumps (location tracking); IP traces from forensic attempts feed back into op	SS7/Diameter exploits for Provide Subscriber Info (PSI)/AnyTime Interrogation (ATI); real-time location via cell ID; used by surveillance firms & APTs	SigPloit framework; commercial SS7 access via shady interconnects	Demonstrated at CCC/Black Hat (Karsten Nohl 2014–2024 updates); 2025 Enea report on TCAP bypass for location tracking
Exfiltration / Impact	Final "go-order" push; forensic IP traces from tower dumps used to counter blue-team	Full device takeover + physical tracking enables hybrid ops (e.g., physical interception)	Data exfil via encrypted channels	Hybrid cyber-physical red-teaming (DARPA/NSA exercises); metrics: Location accuracy

				~100–500m (urban)

Table1: Description of various scenarios in Mobile Kill Chain

VI. REAL-WORLD APT CAMPAIGNS ALIGNING WITH MOBILE/CYBER-PHYSICAL CHAINS

APT Group	Key Malware	Common Lures	Cyber-Physical Elements	Targets
APT36 (Transparent Tribe / ProjectM)	CapraRAT (Android RAT, evolved from AndroRAT)	Romance scams, fake secure chat apps (MeetsApp, MeetUp), job offers	SS7/Diameter for location; trojanized prayer/YouTube apps	Indian government, military, diplomats; Pakistani users in cross-border ops
Patchwork	VajraSpy RAT	Romance/honeypot scams via messaging apps	Persistence via accessibility services; data exfiltration	Pakistani/Indian officials
StrongPity / GREF (APT15-linked)	StrongPity Telegram trojans, BadBazaar	Fake Telegram/Shagle apps	Notification monitoring, exfil of Viber/Skype/Gmail	Regional activists, professionals
Others (e.g., SideCopy, Earth Karkaddan)	CrimsonRAT variants on mobile	Themed lures (e.g., terror events, Kavach MFA malvertising)	Tower-dump forensics evasion; eSIM for C2 resilience	Defense, education sectors in India/Pakistan

Table2: Real-World APT Campaigns with Mobile/Cyber-Physical Chain

VII. TTP ANALYSIS: ADVANCED THREAT ACTOR OPERATIONS

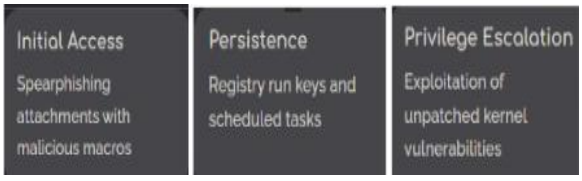
Comprehensive MITRE ATT&CK mapping of five sophisticated threat actor campaigns: SNAKE-MATE, FOMO, TOWERDUMP, MOBILERENAISSANCE, and JOBSEQUENCE. This analysis provides tactical intelligence on their techniques, tactics, and procedures across the ATT&CK framework, enabling defenders to understand attack patterns and implement effective countermeasures.

Threat Profile

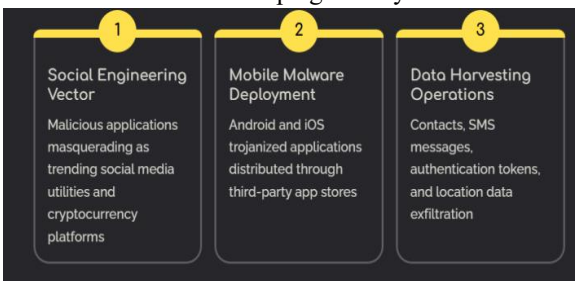
SNAKE-MATE represents a highly sophisticated APT operation targeting enterprise networks through multi-stage intrusion frameworks. The campaign demonstrates advanced persistence mechanisms and lateral movement capabilities characteristic of nation-state actors.

Primary Objectives

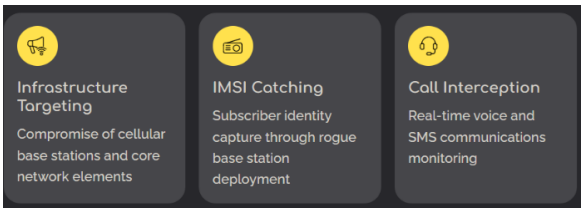
- Long-term persistent access establishment
- Credential harvesting at scale
- Intellectual property exfiltration
- Network topology reconnaissance



FOMO Campaign Analysis



Tower-Dump Telecommunications Interception



Mobile Renaissance Campaigning

- Key Characteristics:
- MDM/EMM platform exploitation
- Certificate authority compromise
- Enterprise app store poisoning
- Cross-platform persistence mechanisms

Job-Sequence: Supply chain Compromise

Fig2: TTP Analysis: Advanced threat Actor Operations

These campaigns often exploit "Mobile-Renaissance" trends: encrypted comms, mobile-first habits, and post-event curiosity (e.g., seeding malware after national-security incidents to target investigators or public users via shared footage/lures).

For Law-enforcement / Investigators

- Harden investigator endpoints (EPP/EDR + strict email/attachment handling; open suspicious material only in isolated VMs). Rapidly treat any incoming “evidence” file as potential malware.
- Preserve chain of custody for digital evidence and use validated tools for tower-dump / CDR correlation.
- Coordinate cyber and physical leads — malware lures may be used to spy on the investigation or to stage false trails.
- Clarify legal frameworks for tower dumps and emergency use, balancing privacy and investigative needs (some jurisdictions saw legal challenges to blanket tower dumps).

VIII. FOMO: MOBILE ATT&CK TECHNIQUES

Attack Chain Components

FOMO operations leverage Mobile ATT&CK techniques specifically targeting Android and iOS platforms. The campaign demonstrates sophisticated understanding of mobile operating system security boundaries and application sandboxing limitations.

Fig3: FOMO Attack Chain Components in Mobile

Masquerade as Legitimate Application

Apps impersonate popular social and financial platforms

Access Contact List

Unauthorized contact database harvesting for propagation

Location Tracking

Continuous GPS monitoring and geolocation logging

Access Notifications

Interception of 2FA codes and sensitive communications

Phase 1: Reconnaissance

Network topology mapping and equipment identification

Phase 2: Initial Compromise

Exploitation of telecom equipment vulnerabilities

Phase 3: Collection

Mass subscriber data and communications interception

MOBILE-RENAISSANCE Campaign

Fig4: Mobile Renaissance campaign

IX. ENTERPRISE MOBILE TARGETING

MOBILE-RENAISSANCE represents evolution in mobile threat landscape, specifically targeting enterprise mobility management (EMM) platforms and mobile device management (MDM) solutions. The campaign exploits trust relationships between corporate infrastructure and employee devices.

Key Characteristics

- MDM/EMM platform exploitation
- Certificate authority compromise
- Enterprise app store poisoning
- Cross-platform persistence mechanisms

MDM Infrastructure Compromise
Initial access through exploitation of mobile device management platforms, enabling mass device enrollment
Certificate Abuse
Stolen enterprise certificates used to sign malicious applications appearing legitimate to security controls

Enterprise Propagation
Malicious profiles distributed through compromised corporate app catalogs to enrolled devices

MOBILERENAISSANCE: ATT&CK Mapping
Deliver Malicious App via Authorized App Store
Compromised enterprise app catalogs distribute trojanized business applications to managed devices

Abuse Device Administrator Access
Malicious profiles grant elevated permissions, preventing removal and enabling persistent access

Commonly Used Port
C2 communications blend with legitimate enterprise traffic using standard HTTPS protocols

Stored Application Data
Harvesting of corporate email, documents, and authentication tokens from business applications

JOBSEQUENCE: Supply Chain Compromise
JOBSEQUENCE operations exemplify sophisticated supply chain attacks targeting software development pipelines, continuous integration systems, and code repositories. This campaign demonstrates advanced understanding of DevOps workflows and software distribution mechanisms.

Attack Vectors

- Compromised CI/CD pipelines
- Malicious package dependencies
- Code repository backdoors
- Build system manipulation

Impact Scope

- Downstream customer compromise
- Widespread malware distribution
- Trust relationship exploitation
- Long-term persistence establishment

Developer Account Compromise
Credential theft targeting maintainers of popular packages
Repository Injection
Malicious commits inserted into legitimate codebases

Mass Distribution
Poisoned packages distributed to thousands of downstream users

X. CONCLUSION

Defensive Recognition - Detection Engineering
Implement behavioral analytics covering all mapped TTPs. Deploy EDR, MDR, and network detection capabilities with signatures for identified techniques. Establish baseline behavioral profiles to identify anomalous activity patterns.
The overall work demonstrates the hybrid threat environments demand multidisciplinary computational approaches, combining telecom

forensics, malware analytics, behavioral modelling, and system-level security evaluation. Such integrated methodologies are essential for improving digital-forensic readiness, strengthening threat detection, and enabling robust incident response in increasingly interconnected and adversarial computing environments.

Future Research Directions: The mobile cyber kill chain adapts frameworks to smartphone ecosystems, emphasizing stages like reconnaissance (e.g., social engineering via apps/social media), weaponization/delivery (malware distribution), installation (sideloading or app stores), and actions on objectives (data exfiltration, spying). A rising threat involves FOMO-triggered malware — malicious campaigns exploiting users' Fear of Missing Out through urgency-driven social engineering (e.g., "limited-time" crypto airdrops, exclusive event invites, flash sales, or fake concert tickets that lead to phishing links or malicious APKs). These often result in info-stealers, banking trojans, or spyware on Android/iOS devices.

Tower dumps (also called cell tower data dumps or CDR tower extracts) provide forensic goldmines: bulk records of all devices connecting to a cell site over time, including IMSI/IMEI, timestamps, and approximate locations. Correlating tower dump data with FOMO malware incidents can reveal victim clustering (e.g., mass infections at events or urban hotspots where scams spread via SMS/social sharing), attacker C2 infrastructure proximity, or coordinated campaigns.

The proposed future work areas explain the feasibility, challenges, and potential impact in mobile forensics and threat hunting.

1. Development of AI-Driven Tower Dump Correlation Systems

- Concept: Build ML pipelines (e.g., using graph neural networks or anomaly detection like Isolation Forests/autoencoders) to ingest massive tower dump datasets (often terabytes) and correlate them with malware telemetry (e.g., from sandboxes like ANY.RUN or mobile threat intel feeds).
- Key Features:
  - Cluster devices by infection vectors (e.g., identify 10,000+ devices hitting the same tower during a FOMO scam spike).
  - Link IMSI/IMEI from dumps to malware samples via temporal/spatial overlaps.
  - Predict campaigns spread using mobility patterns.
- Challenges: Privacy regulations (e.g., post-2025 U.S. rulings limiting warrantless tower dumps), data volume, false positives from benign crowding.
- Impact: Real-time mapping of malware epidemics; already prototyped in tools like i9 CDR/Tower-Dump software but needs AI for scalability.

2. Automated Detection of FOMO-Triggered Malware Campaigns

- Concept: Develop behavioral heuristics + NLP/ML models to flag FOMO lures in SMS, WhatsApp, Telegram, or app notifications (e.g., keywords like "claim now," "limited spots," combined with urgency timers.
- Integration with Kill Chain: Focus on early stages (recon/delivery) — detect droppers (e.g., fake apps promising exclusive NFT drops) and automate alerts via EDR/MDR for mobile (e.g., Lookout, Zimperium).
- Advanced Ideas:
- Honeypots simulating FOMO-vulnerable users (e.g., auto-clicking scam links in emulated devices).
- Cross-platform campaign tracking (e.g., linking iOS phishing to Android spyware families like Anatsa or Sharkbot).
- Impact: Reduce dwell time; FOMO exploits rose sharply post-2023 with crypto/social trends.

3. Improved Mobile-Forensic Extraction Tools for Encrypted Apps

- Concept: Enhance tools like Cellebrite UFED, Magnet AXIOM, or Oxygen Forensics to bypass/better handle end-to-end encryption in apps commonly abused for FOMO scams (e.g., WhatsApp backups, Telegram secrets, Signal artifacts, or WeChat wallets).
- Techniques:
- Advanced chipset exploits (e.g., checkm8/checkra1n extensions for newer iOS).
- Cloud extraction (iCloud/Google Drive pulls with legal warrants).
- Memory forensics for runtime decryption keys.

- Relevance to FOMO Malware: Scammers often use encrypted chat for C2 or victim coordination; better extraction reveals full kill chain (e.g., dropper → overlay attacks).
- Impact: Critical for post-infection forensics, especially in ransomware-like mobile lockers triggered by FOMO clicks.

4. Simulated Attack-Surface Modelling for Hybrid Cyber-Physical Threats

- Concept: Use digital twins or simulation frameworks (e.g., NS-3 for mobile networks + Unity/Gazebo for physical layering) to model FOMO malware in cyber-physical contexts (e.g., infections at concerts/stadiums where tower density is high and social sharing amplifies spread).
- Scenarios:
- 5G/6G slicing vulnerabilities enabling targeted tower spoofing + FOMO SMS blasts.
- IoT convergence (e.g., malware jumping from phone to smart vehicles or wearables).
- Red-team exercises simulating mass events (e.g., Black Hat-style DEF CON badge hacks but with FOMO crypto lures).
- Impact: Proactive defense for emerging threats like location-based social engineering or drone-delivered phishing.

5. Integration of Cybersecurity Awareness in National Crisis Response Teams

- Concept: Embed mobile threat modules (focused on FOMO/social engineering) into national incident response (e.g., CISA, ENISA, or Interpol frameworks), including tabletop exercises for hybrid crises (e.g., disinformation + malware during elections or disasters).
- Practical Steps:
- Public campaigns targeting FOMO (e.g., "Pause Before You Panic-Click").
- Cross-agency data sharing for tower dumps during major campaigns.
- Training for first responders on mobile triage (e.g., quick IMSI grabs at scenes).
- Impact: Holistic resilience; FOMO exploits psychological vulnerabilities amplified in crises (e.g., fake relief fund scams).
- These directions align with evolving mobile threats observed in 2024–2025 reports (e.g., rising social engineering in phishing > traditional exploits). Prioritizing AI automation and cross-domain correlation (tower data + behavioral signals) could significantly disrupt FOMO-driven mobile kill chains. If you're authoring a paper or need prototypes/references, I can help refine further!

REFERENCES

[1] Modified cyber kill chain model for multimedia service environments - February 2019 78(21) DOI:10.1007/s11042-018-5897-5 License CC BY 4.0 Authors: Hyeob Kim HyukJun Kwon, Kyung Kyu Kim

[2] The Cyber Kill Chain Methodology as a Business Defense Tool: A Systematic Review of Its Application and Efficacy Vol. 19 No. 12 (2025) Junior E. Dávila-Huayhuapuma, Eduardo Vílchez-Roncal, Carlos A. Alvarado-Silva

[3] A survey on the application of evolutionary algorithms for mobile multihop adoc network optimization problems https://doi.org/10.1155/2016/2082496 D. G. Reina, P. Ruiz, R. Ciobanu, S. L. Toral storal@us.es, B. Dorronsoro, and C. Dobre

[4] Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures Pooneh Nikkhah Bahrami, Ali Dehghantanh, Tooska Dargah, Reza M. Parizi Kim-Kwang Raymond Choo, and Hamid H. S. Javadi -J inf Process Syst, Vol15. No.4. pp.865-889, August 2019

[5] Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework by Thulfiqar Jabar ORCID and Manmeet Mahinderjit Singh *Sensors 2022, 22(13), 4662; https://doi.org/10.3390/s22134662

[6] MCKC: a modified cyber kill chain model for cognitive APTs analysis within Enterprise multimedia network Published: 13 August 2020 Volume 79, pages 29923–29949, (2020)

[7] A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques by Amjed Ahmed Al-Kadhimi 1,2ORCID,Manmeet Mahinderjit Singh 1,*ORCID and Mohd Nor

Akmal Khalid 3Appl. Sci. 2023, 13(14), 8056; https://doi.org/10.3390/app13148056

[8] Domain-specific Threat Modeling for Mobile Communication Systems - Chen, Hsin-Yi Advanced Materials for Innovation and Sustainability - Master's Programme in Security and Cloud Computing (SECCLO),2021-08-23

[9] Drone Hacking: Applying the Cyber Kill Chain to Hijack Unmanned Aerial Systems Jacob Malimban, Bryson R. Payne, Tamirat T. Abegaz A JOURNAL OF INTERNATIONAL ACADEMY OF BUSINESS DISCIPLINES SPONSORED BY UNIVERSITY OF NORTH FLORIDA ISSN 2334-0169 (print) ISSN 2329-5163 (online) QRBD QUARTERLY REVIEW OF BUSINESS DISCIPLINES November 2021 Volume 8 Number 3 Margaret A. Goralski, Quinnipiac University Email: Margaret.Goralski@Quinnipiac.edu Charles A. Lubbers, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://faculty.utrgv.edu/louis.falk/qrbd/QRBDnov21.pdfUniversity of South Dakota Email: Chuck.Lubbers@usd.edu

[10] Threats and Threat Intelligence -Chapter-First Online: 19 April 2023 Dietmar P. F. Möller Part of the book series: Advances in Information Security ((ADIS, volume 103))