

Security Brief / Year 2024 / Scene 1

Attack 1

AI Disinformation Campaign Targeting the U.S. Election and its Aftermath

An AI-driven campaign spread hyper-targeted deepfakes and fake news, shaking voter confidence ahead of the U.S. election. Orchestrated from abroad, the operation caused post-election unrest and delayed results certification. Investigations revealed systemic vulnerabilities in platform moderation. In response, the U.S. launched emergency digital trust initiatives and accelerated legislation regulating political AI content and algorithmic transparency.

Key Factors: Generative AI (C1), Workflow / Logistics / Supply Chain (C3), Virtual Assistants / AI Bots (C5)

Attack 2

China Drones in South China Sea

China deployed stealth drones from artificial islands in the South China Sea, conducting close flyovers near Vietnamese and Filipino naval vessels. The drones gathered surveillance data while testing regional responses. ASEAN members filed diplomatic protests, while the U.S. increased naval patrols. China dismissed concerns, claiming lawful sovereignty. The incident escalated tensions and triggered regional drone defense upgrades.

Key Factors: Traceability / Attribution / Analytics (C2), All-Domain Autonomous Defense (C4)

Attack 3

North Korea Cyberhack of U.S. Bank through Sophisticated Catfishing

North Korean operatives used AI-generated personas to catfish U.S. cybersecurity contractors, gaining access to sensitive bank infrastructure. Millions of dollars were siphoned off before detection. The hackers laundered funds via crypto mixers. The breach exposed social engineering risks and prompted an overhaul in employee digital hygiene training across financial institutions and new sanctions targeting North Korean cyber divisions.

Key Factors: Generative AI (C1), Traceability / Attribution / Analytics (C2), All-Domain Autonomous Defense (C4)

Security Brief / Year 2025 / Scene 2

Attack 4

Russian-Backed Hacking Group Disrupts Global GPS Systems

A Russian-linked group launched a cyberattack disabling segments of global GPS networks, affecting aviation, maritime shipping, and emergency services. Spoofed signals caused cargo misroutes and grounded flights. Attribution pointed to GRU affiliates. NATO condemned the act as a hybrid warfare escalation. Emergency summits followed, and nations fast-tracked adoption of backup navigation systems resistant to spoofing.

Key Factors: Workflow / Logistics / Supply Chain (C3), Foreign Language Processing (C7), Advanced Cybersecurity (C8)

Attack 5

Drug Cartels Employ Coordinated Drone Operations to Smuggle Narcotics Across US-Mexico Border

Mexican cartels began using synchronized drone swarms to bypass traditional border enforcement, dropping narcotics with GPS precision. The tactic overwhelmed Border Patrol radar and response systems. U.S. officials called the method “militarized smuggling.” Seizures dropped by 30% as drones became harder to intercept. Congress initiated bipartisan talks on autonomous threat detection and counter-drone technology deployment.

Key Factors: Traceability / Attribution / Analytics (C2), Workflow / Logistics / Supply Chain (C3), All-Domain Autonomous Defense (C4)

Attack 6

Teenagers Exploit AI Voice Synthesizers in Elaborate Fraud Scheme

A group of teens used AI voice cloning tools to impersonate parents and CEOs in phone scams, extracting thousands from unsuspecting victims. The fraud spread rapidly on social media, triggering nationwide alarm. Law enforcement arrested six involved, sparking debate over access to open-source AI tools.

Key Factors: Generative AI (C1), Virtual Assistants / AI Bots (C5), Advanced Cybersecurity (C8)

Security Brief / Year 2026 / Scene 3

Attack 7

Chinese Cyberattack Knocks Out Power in North Dakota After U.S. Aircraft Carrier Move

Following a U.S. carrier deployment to the Taiwan Strait, a cyberattack originating in China shut down power grids in North Dakota. The blackout lasted 18 hours, disrupting hospitals and communications. Beijing denied involvement. U.S. intelligence confirmed industrial control systems were breached via a zero-day exploit.

Key Factors: Traceability / Attribution / Analytics (C2), Foreign Language Processing (C7), Advanced Cybersecurity (C8)

Attack 8

Russia Deploys Offensive Drones Across European Borders in Response to Ukraine War Settlement Proposal

After rejecting a Western-brokered Ukraine peace framework, Russia launched drone incursions into Poland, Latvia, and Romania. The drones didn't fire but jammed radar and surveillance feeds. NATO forces scrambled jets in response. Moscow framed the move as "strategic signaling." The EU accelerated its joint drone defense network, while member states debated invoking Article 5 protections.

Key Factors: Traceability / Attribution / Analytics (C2), All-Domain Autonomous Defense (C4), Foreign Language Processing (C7)

Attack 9

Iranian Cyberattack Targets U.S. Banks, Exfiltrating Sanctioned Funds Through Blockchain

Iranian hackers breached two U.S. banks, using smart contracts and crypto bridges to move sanctioned funds into anonymized wallets. The operation bypassed traditional sanctions enforcement. Treasury froze affected accounts and flagged Ethereum mixers. Iran claimed the operation was retaliation for frozen assets.

Key Factors: Traceability / Attribution / Analytics (C2), Workflow / Logistics / Supply Chain (C3), Advanced Cybersecurity (C8)

Security Brief / Year 2027 / Scene 4

Attack 10

Extremist Group Steals Identity, Diverts CDC Viral Samples; Samples Still Missing

A bio-hacktivist cell stole CDC credentials via dark web forums and redirected a shipment of viral research samples. The breach went undetected for 72 hours. The missing samples sparked fears of weaponization. Intelligence agencies suspect the group intended to expose “bio-surveillance tyranny.”

Key Factors: Traceability / Attribution / Analytics (C2), Biological Models (C7)

Attack 11

Anti-5G Group Uses Drones, Cyber Hacks to Disable Cell Antennas; Economic Damage Mounts

An anti-5G group coordinated drone attacks and malware to disable over 300 cell towers across three states. Downtime crippled logistics and financial transactions. Social media platforms failed to contain viral conspiracies boosting the attackers. Telecom giants demanded stronger federal protections.

Key Factors: Traceability / Attribution / Analytics (C2), All-Domain Autonomous Defense (C4), Advanced Cybersecurity (C8)

Attack 12

Former Columnist Louis the Luddite Leads Attack on Data Centers, Disrupts AI Services

Louis the Luddite, a radical ex-journalist, led coordinated raids on data centers hosting AI models, causing widespread outages in voice assistants, medical diagnostics, and autonomous systems. His manifesto accused AI of eroding truth and agency. Authorities captured Louis after a standoff in Nevada.

Key Factors: Traceability / Attribution / Analytics (C2), Virtual Assistants / AI Bots (C5), Advanced Cybersecurity (C8)