# (Gen)AI vs (Gen)AI in Industrial Control Cybersecurity

**GOAL: Study the impacts of (Gen)AI on industrial control systems (ICSs) for each step of the cyber kill chain (CKC) to better understand attacker strategies and build stronger defenses**

Cynthia Zhang, Ranjan Pal, Michael Siegel

## 1. ICSs are the backbone of critical infrastructure, but are left vulnerable

ICSs play a pivotal role in water treatment plants, the power grid, oil pipelines, telecommunications, etc. However, they are **vulnerable** because:

1. ICSs are littered with **legacy systems**
2. OT systems are **difficult to patch**
3. OT systems have **poor visibility**
4. IT/OT convergence leads to **attack spillover**
5. Lack of **security awareness**

## 2. (Gen)AI poses a new threat to an already threatened system of ICSs

(Gen)AI can exploit each of the vulnerabilities mentioned above as follows:

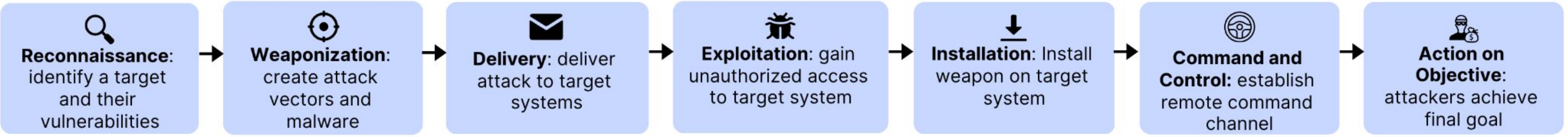
1. Legacy systems have **widely known vulnerabilities and exploits** which (Gen)AI can quickly discover and use
2. Unpatched systems and poor visibility lead to **easily exploitable vulnerabilities** such as default passwords
3. IT/OT convergence **increases the attack area** on which (Gen)AI can discover vulnerabilities
4. Undertrained employees are easy targets for **(Gen)AI-generated spear phishing attacks**.

## 3. A CKC guided analysis allows for insights into attack and defense sides

Analysis of (Gen)AI's impacts on ICSs on the Cyber Kill Chain allows for:

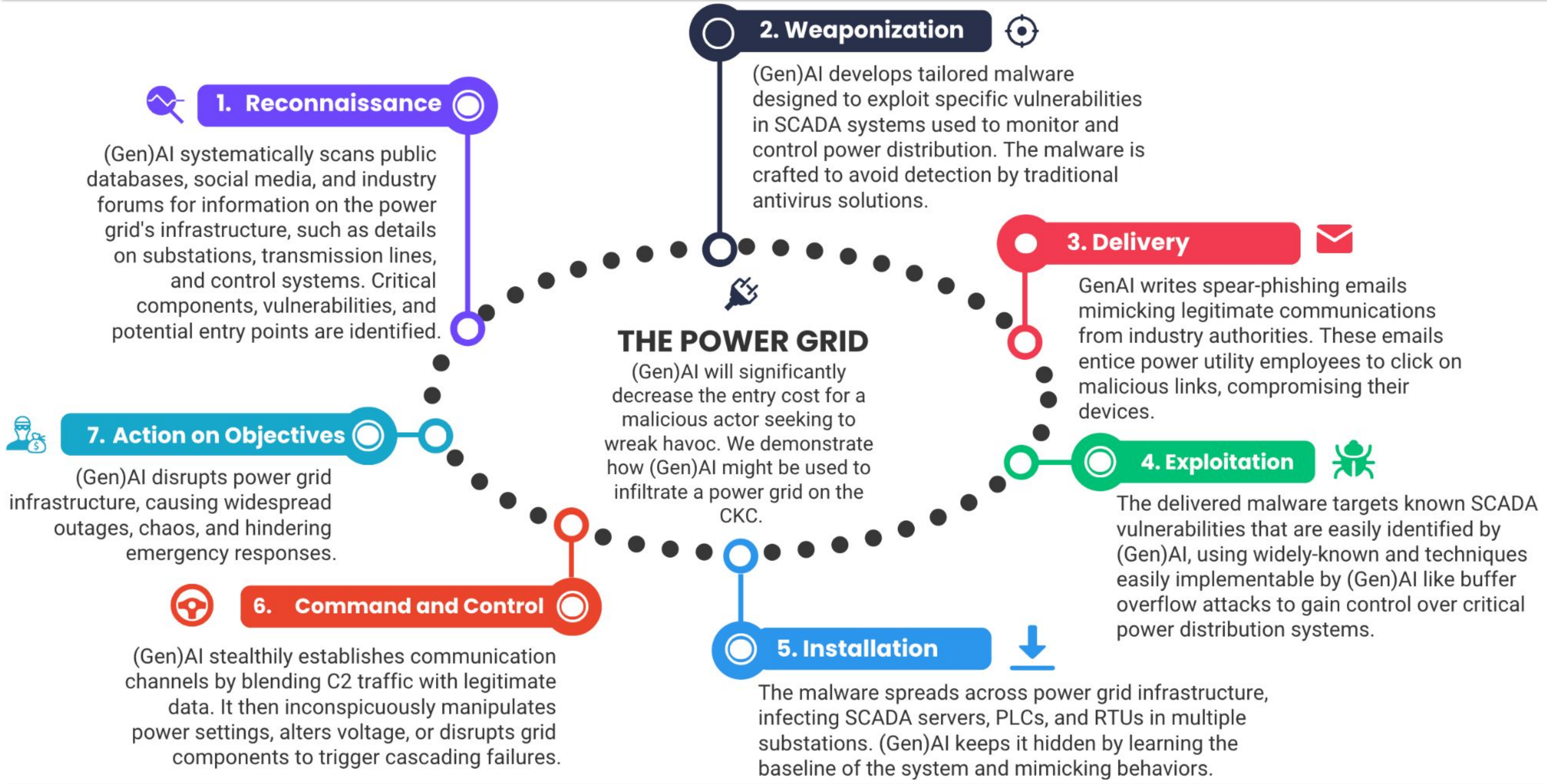
- enhanced comprehension of the threat landscape at every stage of a cyber attack
- a tool for devising proactive defense strategies to counter AI-driven cyberattacks on ICSs

## 4. What are the 7 steps of the Cyber Kill Chain (CKC) framework?



**Reconnaissance**: identify a target and their vulnerabilities →
**Weaponization**: create attack vectors and malware →
**Delivery**: deliver attack to target systems →
**Exploitation**: gain unauthorized access to target system →
**Installation**: Install weapon on target system →
**Command and Control**: establish remote command channel →
**Action on Objective**: attackers achieve final goal

## 5. Example of a (Gen)AI powered attack on a *power grid* on the CKC



**THE POWER GRID**

(Gen)AI will significantly decrease the entry cost for a malicious actor seeking to wreak havoc. We demonstrate how (Gen)AI might be used to infiltrate a power grid on the CKC.

**1. Reconnaissance**

(Gen)AI systematically scans public databases, social media, and industry forums for information on the power grid's infrastructure, such as details on substations, transmission lines, and control systems. Critical components, vulnerabilities, and potential entry points are identified.

**2. Weaponization**

(Gen)AI develops tailored malware designed to exploit specific vulnerabilities in SCADA systems used to monitor and control power distribution. The malware is crafted to avoid detection by traditional antivirus solutions.

**3. Delivery**

GenAI writes spear-phishing emails mimicking legitimate communications from industry authorities. These emails entice power utility employees to click on malicious links, compromising their devices.

**4. Exploitation**

The delivered malware targets known SCADA vulnerabilities that are easily identified by (Gen)AI, using widely-known and techniques easily implementable by (Gen)AI like buffer overflow attacks to gain control over critical power distribution systems.

**5. Installation**

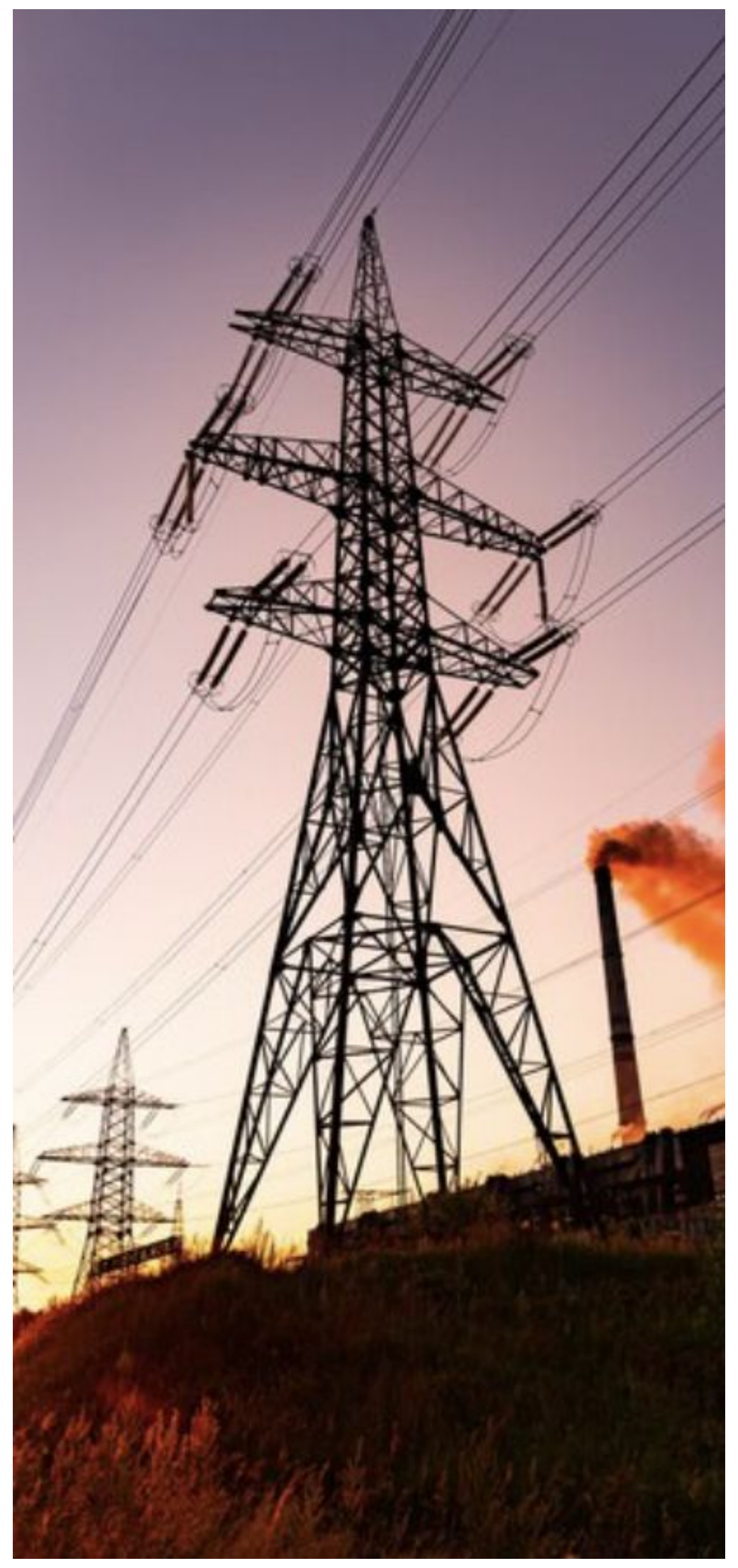
The malware spreads across power grid infrastructure, infecting SCADA servers, PLCs, and RTUs in multiple substations. (Gen)AI keeps it hidden by learning the baseline of the system and mimicking behaviors.

**6. Command and Control**

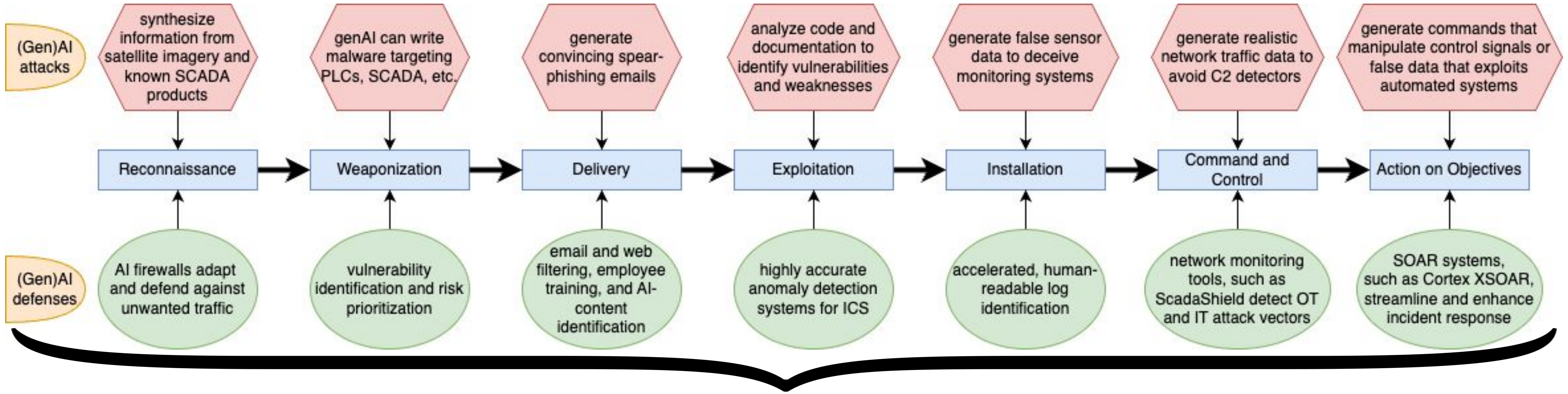
(Gen)AI stealthily establishes communication channels by blending C2 traffic with legitimate data. It then inconspicuously manipulates power settings, alters voltage, or disrupts grid components to trigger cascading failures.

**7. Action on Objectives**

(Gen)AI disrupts power grid infrastructure, causing widespread outages, chaos, and hindering emergency responses.



## 6. How does (Gen)AI affect attackers and defenders on the CKC?



| | Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command and Control | Action on Objectives |
|---|---|---|---|---|---|---|---|
| (Gen)AI attacks | synthesize information from satellite imagery and known SCADA products | genAI can write malware targeting PLCs, SCADA, etc. | generate convincing spear-phishing emails | analyze code and documentation to identify vulnerabilities and weaknesses | generate false sensor data to deceive monitoring systems | generate realistic network traffic data to avoid C2 detectors | generate commands that manipulate control signals or false data that exploits automated systems |
| (Gen)AI defenses | AI firewalls adapt and defend against unwanted traffic | vulnerability identification and risk prioritization | email and web filtering, employee training, and AI-content identification | highly accurate anomaly detection systems for ICS | accelerated, human-readable log identification | network monitoring tools, such as ScadaShield detect OT and IT attack vectors | SOAR systems, such as Cortex XSOAR, streamline and enhance incident response |

**(Gen)AI defense action items for industrial control system management**

**Read more about (Gen)AI's impact on ICSs on the CKC:**

**Answer a quick survey about your thoughts on (Gen)AI's impact on ICSs:**

*Contacts:* {zcynthia, ranjanp, msiegel}@mit.edu