Xiaosong ZHANG, Yukun ZHU, Xiong LI, Yongzhao ZHANG, Weina NIU, Fenghua XU, Junpeng HE, Ran YAN, Shiping HUANG, 2025. Active cybersecurity: vision, model, and key technologies. *Frontiers of Information Technology & Electronic Engineering*, 26(8):1243-1278. https://doi.org/10.1631/FITEE.2500053

Active cybersecurity: vision, model, and key technologies

Key words: Active cybersecurity; Intelligent threat sensing; In-depth behavior analysis; Comprehensive path profiling; Dynamic countermeasures

Xiaosong ZHANG
E-mail: johnsonzxs@uestc.edu.cn
ORCID: https://orcid.org/0000-0001-9886-1412

Existing cybersecurity model

- Despite advancements in dynamic defense, real-time response, and attacker behavior analysis, current cybersecurity models continue to exhibit significant limitations.
- Existing defense enhancement model and attack confrontation cannot balance proactivity, flexibility, comprehensiveness, and lightness.

Table 1 Summary of each cybersecurity model

Category	Model	Advantage	Disadvantage	P	F	C	L
Defense enhancement	PDR (Schwartau, 1998)	Structured defense	Lack of dynamic adjustment	○	○	○	●
	P2DR (Li DP et al., 2014)	Security strategy for dynamic optimization	Slow response in distributed environments	○	○	○	●
	PDRR (Yang Y et al., 2024)	Recovery phase for full restoration	Weak pre-attack threat identification	○	○	○	●
	PDR2A (Gao, 2012)	Auditing vulnerability	Limited real-time threat management	○	◐	◐	●
	IPDRR (Zhang X et al., 2023)	Lifecycle framework	High complexity and cost	○	◐	◐	◐
	APPDRR (Xu XZ et al., 2024)	Closed-loop protection	Limited dynamic adaptability	○	◐	●	◐
	Intrinsic security (Sabnis et al., 2012)	Active threat awareness	High resource consumption	◐	●	●	○
	Mimicry security (Wu, 2016)	Increased attack difficulty	Focusing on internal defense	○	●	◐	◐
	LMSaniator (Wei et al., 2024)	Runtime behavior verifaction	Insufficient adversarial perspective and contextual inflexibility	◐	◐	◐	●
Attack confrontation	F2T2EA (Tirpak, 2000)	Structured attack process	Lack of dynamic adaptability	◐	○	◐	●
	Kill chain (Sun S et al., 2023)	Modeling attack	Limited adaptability	◐	◐	◐	◐
	ATT&CK (Strom et al., 2020)	Matrix attacker behavior	Struggling with unknown threats	●	◐	●	◐
	WPDRRC (Yao, 2010)	Active warning and counterattack	Risk of greater retaliation	●	◐	●	○
	CARTA (Jiang X, 2020)	Real-time response	High resource consumption	●	●	◐	○
	Shield (Fowler et al., 2020)	Deception attacker	Limited proactive feature	◐	◐	◐	◐
	MTD (Cai et al., 2016)	Dynamic network and system	High resource consumption and low coordination	●	◐	●	○
	SARPPR (Fang et al., 2024)	Full lifecycle protection	High resource consumption	●	●	●	○
	Space Odyssey framework (Willbold et al., 2023)	Adaptive attack surface modeling	Cross-domain coordination and real-time reponse	●	●	◐	◐
Proposed model	SAPC	Full-stage dynamic game	–	●	●	●	●

P represents proactivity, F represents flexibility, C represents comprehensiveness, and L represents lightness. ○ represents low, ◐ represents medium, and ● represents high

Active cybersecurity model (SAPC model)

- We introduce an active cybersecurity model grounded in game theory to tackle evolving network security threats.

- This model abstracts attack–defense interaction as a dynamic game, predicting attacker behavior in information asymmetry environments. It also adapts defense strategies dynamically, optimizing outcomes within resource constraints.

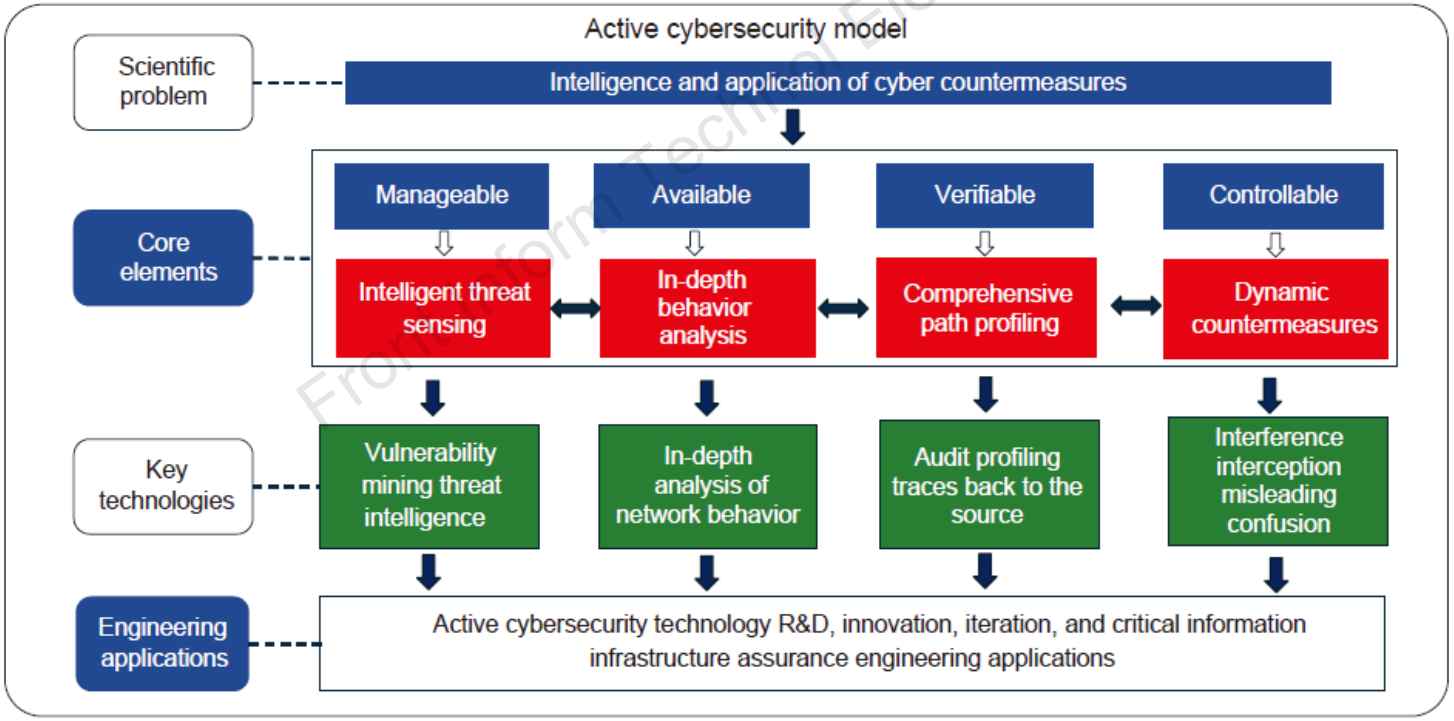

Fig. 1 Proposed sensing, analysis, profiling, and countermeasures (SAPC) model

Technical framework of the SAPC model

- The active network security model is built on an extensive technical framework, designed to form a closed-loop defense system via proactive and intelligent technological methodologies

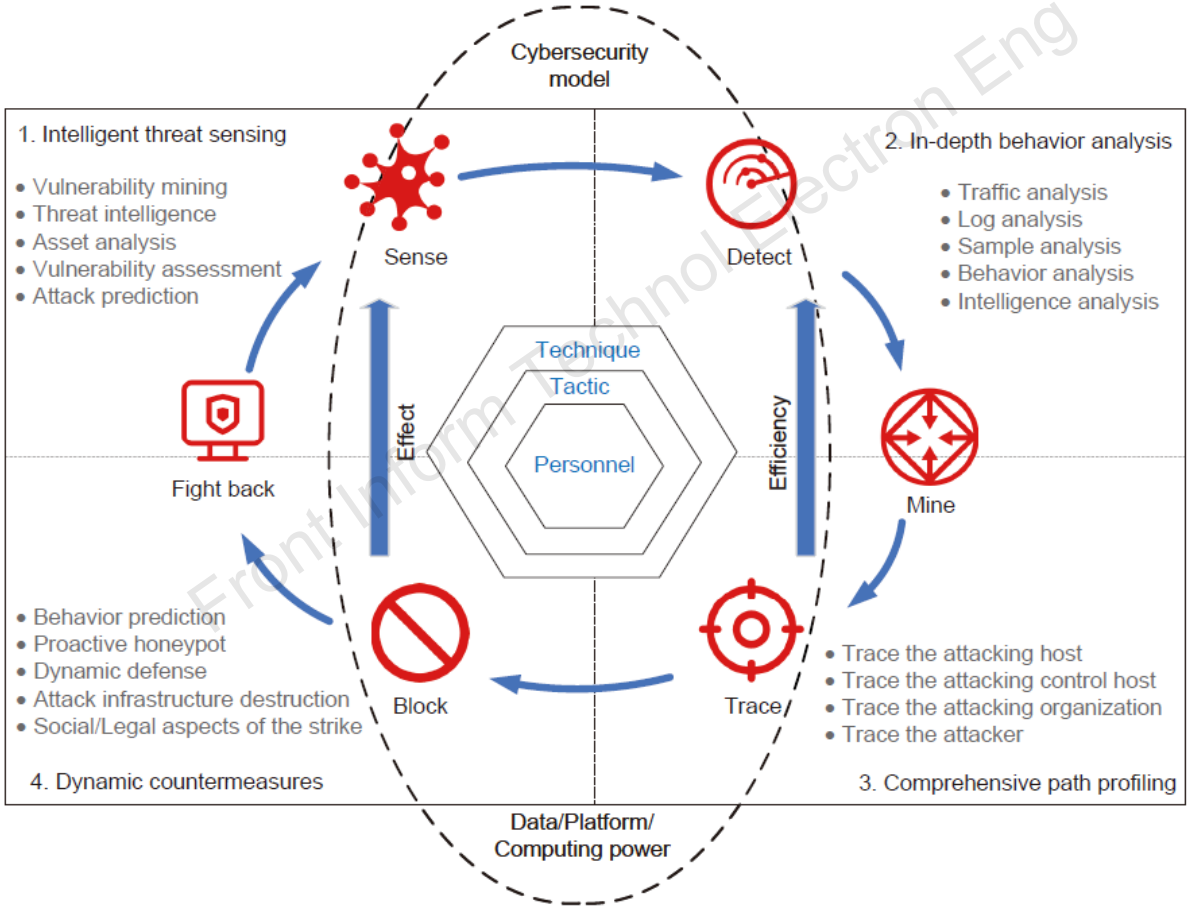

Fig. 2 Technical framework of the sensing, analysis, profiling, and countermeasures (SAPC) model

1) Intelligent threat sensing

- “Intelligent threat sensing” focuses on leveraging dynamic games to uncover unknown vulnerabilities. The technical framework includes target identification, model training, vulnerability generation, and vulnerability combination, covering the entire lifecycle of vulnerability mining to enable active perception and dynamic response.

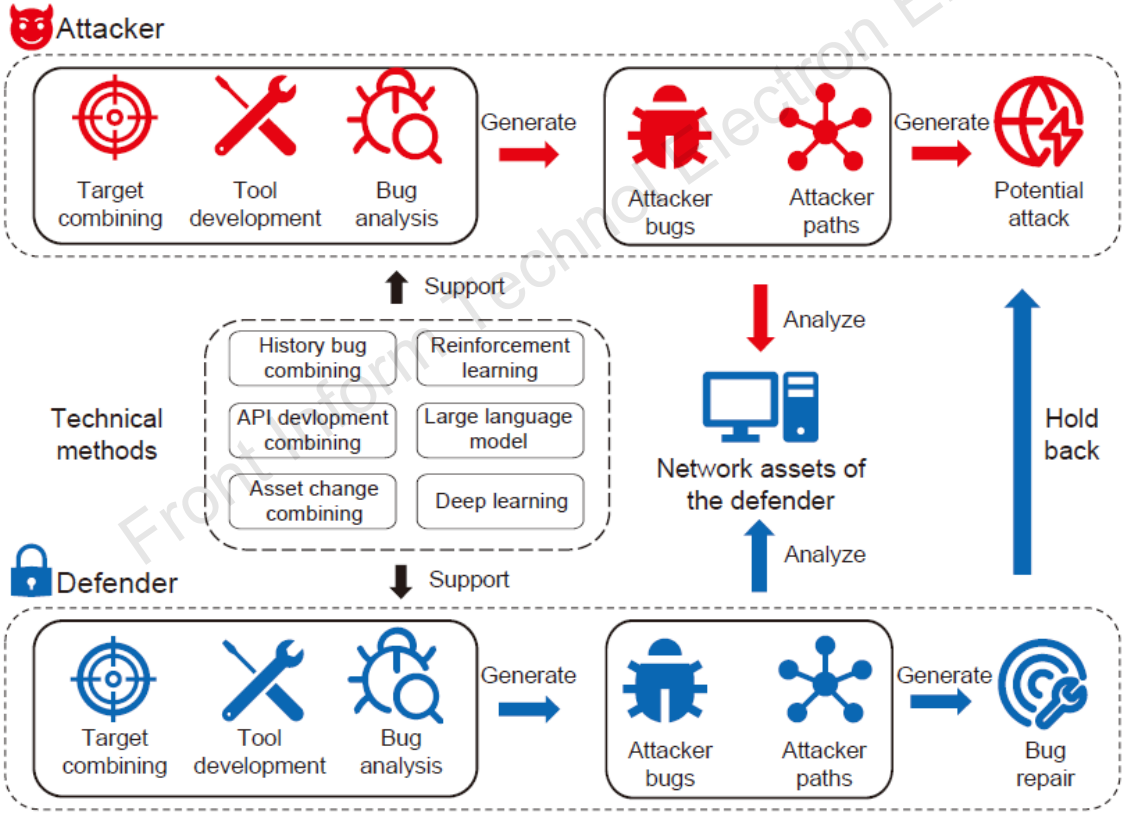

Fig. 3 Vulnerability mining technology based on active cybersecurity with game theory

2) In-depth behavior analysis

- “In-depth behavior analysis” focuses on leveraging active traffic detection technologies, combining historical attribute analysis of attack traffic with real-time updated feature intelligence and thereafter dynamically adjusting defense strategies in response to evolving attacker behaviors.

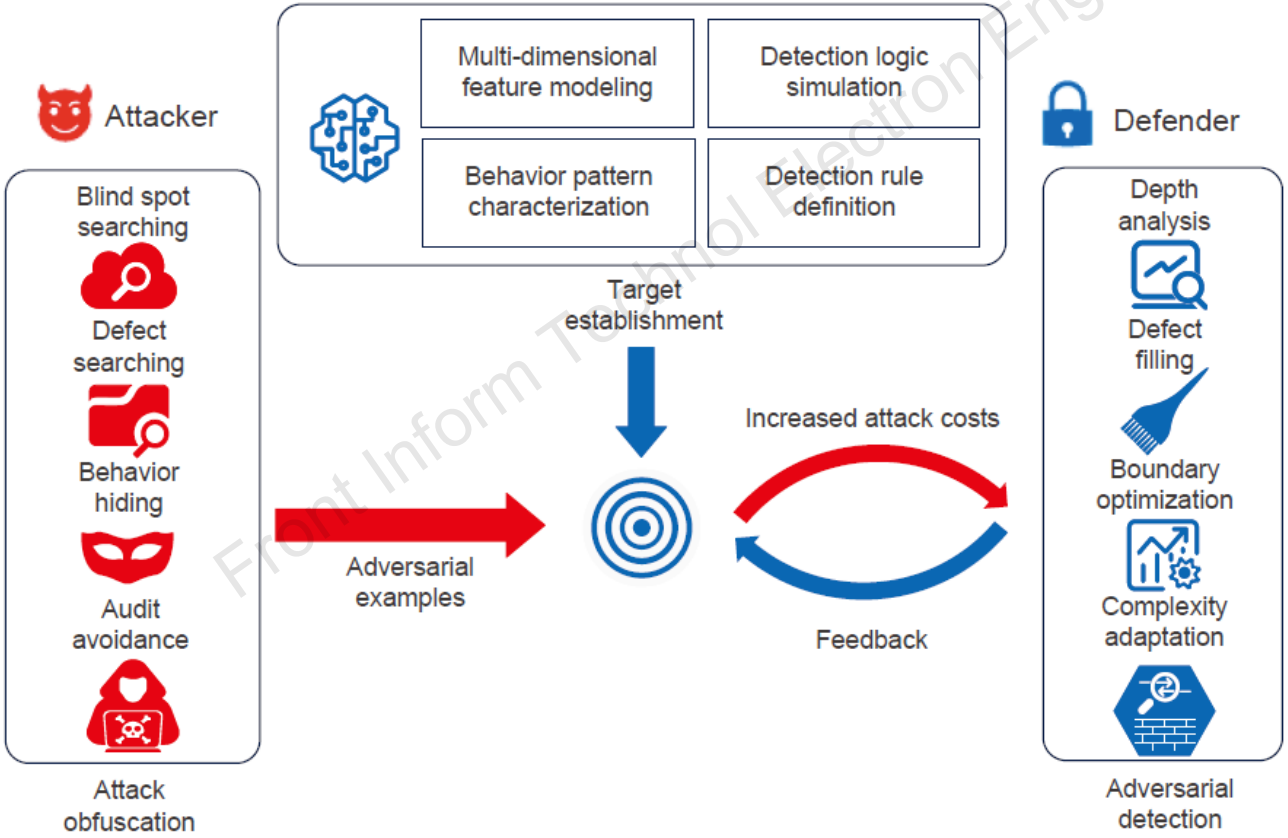

Fig. 4 Traffic detection technology based on active cybersecurity with game theory

3) Comprehensive path profiling

- “Comprehensive path profiling” tracks attack paths, reconstructs attack chains, and analyzes attacker behaviors. This enables defenders to implement precise countermeasures, particularly against APTs.

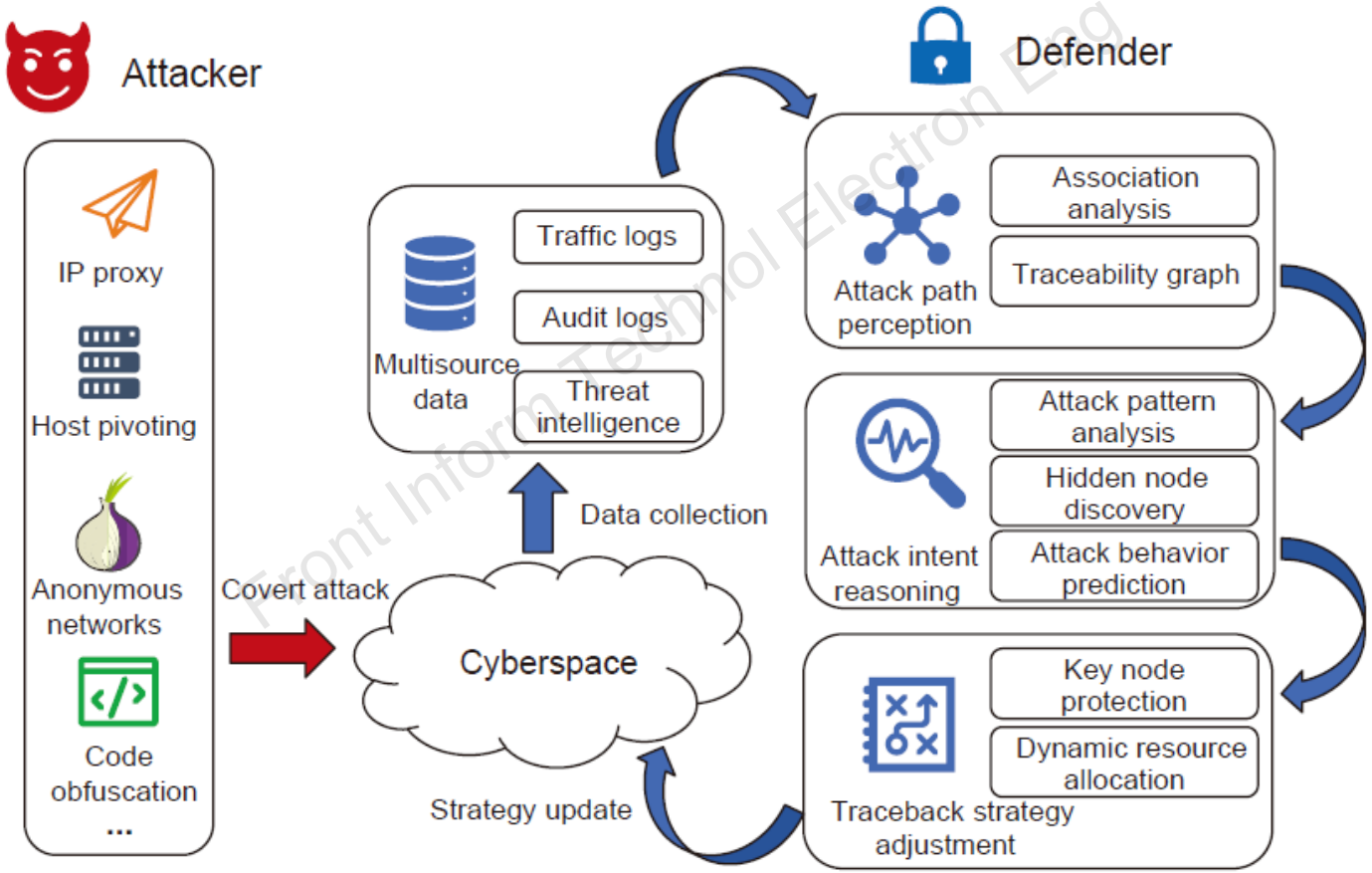

Fig. 5 Attack traceback technology based on active cybersecurity with game theory

4) Dynamic countermeasures

- "Dynamic countermeasures" aim to force attackers to discontinue their attacks or reduce attack effectiveness by increasing the operational cost. These technologies work by depleting the attackers' resources, raising the complexity of the attacks, and reinforcing the defense by targeting attack sources and infrastructure and by implementing intelligent countermeasures.

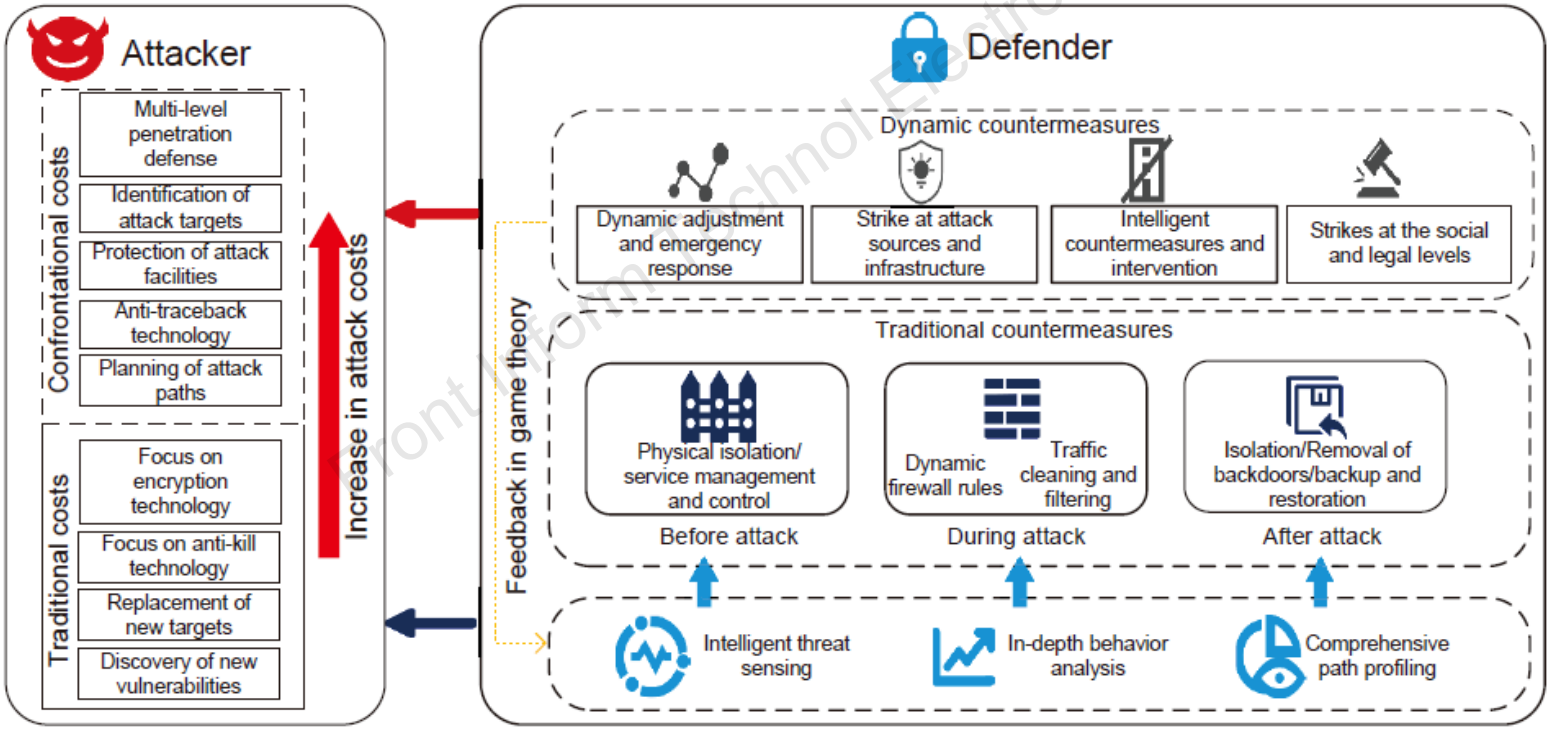

Fig. 6 Countermeasure technology based on active cybersecurity with game theory

Challenges

- **Incomplete collection of information elements**

Complex networks consist of numerous nodes, intricate connections, massive traffic volumes, and variable traffic flows. The inherent flexibility and openness of network topological structures impede comprehensive monitoring of node status and identification of potential risk entry points.

- **Complex calculations of massive data**

Network attack–defense interactions generate extensive datasets from diverse sources, including device monitoring data, security system logs, and network traffic information. These data exhibit multi-dimensional characteristics, heterogeneous structures, and inherent noise, with volumes that exceed traditional data-processing capabilities.

- **Complex emergency response coordination**

Cybersecurity responsibility lies with various network operators, including network service providers, enterprise network management departments, and critical infrastructure operators. As network assets expand, attacks may originate from numerous unexpected nodes or routes.

Xiaosong Zhang received his M.S. and Ph.D. degrees in Information Security from the University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2011, respectively. He is currently a Professor in School of Computer Science and Engineering and the Institute for Cyber Security, University of Electronic Science and Technology of China. His research interests include software vulnerability analysis, program analysis, network security, and data security.