ARCHITECTURE OF AMBIGUITY: STATE–CRIMINAL FUSION IN CYBER ESPIONAGE OPERATIONS

Date: November 21, 2025

Disclaimer: *This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.*

KEY EVENTS

On November 21, 2025, Alexander Leslie presented *Architecture of Ambiguity: State–Criminal Fusion in Cyber Espionage Operations* at the 2025 West Coast Security Conference. The presentation was followed by a question-and-answer period with audience members and CASIS Vancouver executives. The presentation examined ambiguity as a deliberate instrument of state power in cyberspace, introduced a structured framework for analyzing state-criminal fusion, and applied the model comparatively across multiple state actors.

NATURE OF DISCUSSION

The discussion focused on how states intentionally cultivate ambiguity in cyberspace to obscure attribution, manage escalation risk, and extend operational reach. Mr. Leslie outlined a three-layer analytical framework – direct adoption, intermediary cutouts, and long-term co-option – to explain how relationships between states and criminal cyber actors vary in structure but converge in strategic effect. The presentation emphasized the interaction between technical cyber operations and information warfare, illustrating how operational activity and narrative manipulation reinforce one another to shape perception and constrain operational response.

BACKGROUND

State-fusion in cyberspace refers to the ways governments collaborate with, tolerate, or exploit criminal hackers and front groups to conduct espionage, disruption, or influence operations while limiting direct attribution. Mr. Leslie

argued that these arrangements are not incidental but constitute an intentional "architecture of ambiguity" that blurs the boundary between criminality and state-directed cyber activity, complicating detection and attribution.

The first layer of the framework, direct adoption, describes how states operate within existing criminal ecosystems by leveraging commodity malware, hijacked botnets, and illicit infrastructure. Operating within these environments allows state activity to resemble ordinary criminal traffic, lowering costs and increasing deniability. Russia-linked examples were cited to demonstrate how criminal infrastructure can enable persistent, low-cost operations over extended periods.

The second layer, cutouts and false flags, involves the use of front entities, intermediaries, and fabricated personas to serve as "plausibility buffers". This layer aligns with concepts of perception management and reflexive control, exploiting attribution delays and competing narratives to shape analytical and public interpretations. Examples included Russian-linked groups employing pseudo-activist branding and coordinated leak-and-claim channels during the early stages of the full-scale invasion of Ukraine.

The third layer, co-option and integration, reflects deeper institutional fusion between state services and criminal actors. This is carried out through semi-official relationships, protection, and coercive leverage. Framed as "mafia-state" logic applied to cyberspace, this model permits criminals to operate with relative impunity so long as targets remain external. The state, in turn, retains leverage through selective enforcement and latent coercion.

To contextualize these dynamics, Mr. Leslie introduced several analytical frameworks. The mafia-state model captures mutually reinforcing relationships between political elites, security services, and criminal networks. Cyber privateering describes the quasi-sanctioned use of cyber actors to pursue state-aligned objectives. The principal-agent dilemma highlights the challenges states face in managing and mitigating the risks associated with employing proxy actors. Collectively, these concepts illustrate how states seek both operational control and the appearance of non-control to reduce retaliation risk.

The framework was applied comparatively to demonstrate how different states organize state-criminal relationships to achieve similar strategic outcomes. In Russia, ambiguity was depicted as a deliberate and embedded operational posture

within criminal ecosystems. In China, ambiguity was framed as more structured, relying on corporate front companies, contractors, and research institutions. In Iran, ambiguity was linked to ideological mobilization, with cyber groups operating under activist-style branding while pursuing politically aligned objectives. In North Korea, the state itself was characterized as the primary criminal actor, integrating espionage and cyber theft under centralized control to generate revenue and strategic leverage.

Question and Answer

Can you speak at all to Russia's efforts to groom Western LLMs and what unique challenges do influence operations like this pose to western security?

Russia is attempting to use Western LLMs to foster influence operations by injecting them with conspiracy theories, propaganda, and disinformation. This presents a challenge to western security as LLMs are becoming increasingly part of our everyday lives, not only in terms of individual day-to-day activity but also as part of software supply chains. However, this issue is not just limited to Russia. Recent behaviour from OpenAI was attributed to Iranian threat actor activity, and Chinese actors have used various LLMs to automate cyber-attacks at an unprecedented rate.

What role do you see private intelligence firms playing in the intelligence community moving forward? Do you see an increase in private-public fusion to leverage the full potential of emerging technologies?

Proprietary technology increasingly underpins national critical infrastructure and defensive cyber systems. Crucial insight into commercial networks, exploited vulnerabilities, and malware activity often sits with private-sector vendors rather than governments. Without sustained cooperation, governments risk blind spots as cyber capabilities continue to advance. Reflecting this shift, allied countries are increasing funding for cyber capabilities and strengthening public-private partnerships, recognizing that much of the expertise, infrastructure, and technical insight now resides in the private sector.

KEY POINTS OF DISCUSSION

- Ambiguity is a deliberately engineered feature of contemporary cyber operations. It enables states to outsource operational risk while retaining strategic benefit and plausible deniability.
- A three-layer framework – direct adoption, intermediary cutouts, and co-option/integration – provides a structured method for analyzing how states leverage existing malware, illicit infrastructure, and criminal actors to expand their cyber capability.
- Comparative analysis of Russia, China, Iran, and North Korea demonstrates structural variation in state-criminal fusion models, with convergence around the strategic objective of attribution uncertainty and constrained retaliation.

FURTHER READING

Leslie, A. (2024, May 6). Agents of Chaos: Hacktivism Spreads Fear, Disinformation, and Propaganda. RSAC Conference.

Leslie, A. (2025, April 28). The Travels of "Marko Polo": Navigating a Global Infostealer Scam Empire. RSAC Conference.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/