Beyond Attribution: Indictments As Cyber Statecraft

How the United States Uses Law and Public-Private Collaboration to Raise the Cost of State-Linked Cyber Operations

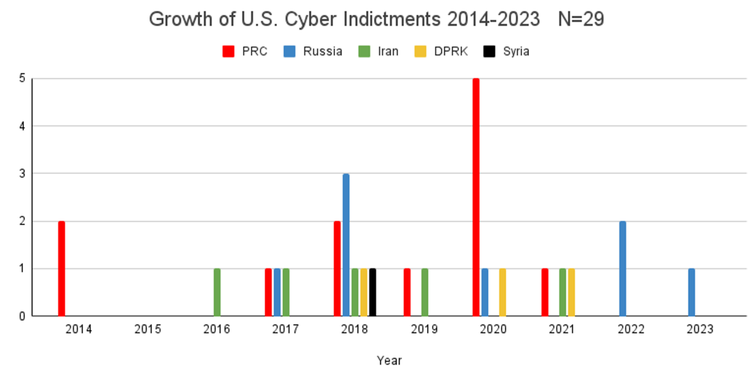
Problem Statement and Goals

Since the early 2010s, the United States has increasingly used criminal indictments as a tool of cyber statecraft. Yet why they emerged, how they have evolved, and what enables them remain understudied.

This study identifies:

- Critical junctures in the evolution of cyber indictment strategy
- Key drivers shaping case selection and timing
- The evolving role of private cyber threat intelligence firms

Why it matters: Understanding how indictments are made reveals how U.S. cyber power is exercised—and how public-private collaboration enables deterrence, accountability, and norms in cyberspace.



The rise in cyber indictments reflects more than increased enforcement. It tracks the maturation of attribution, evidence-sharing, and public disclosure—capabilities largely developed in the private sector and later operationalized by government.

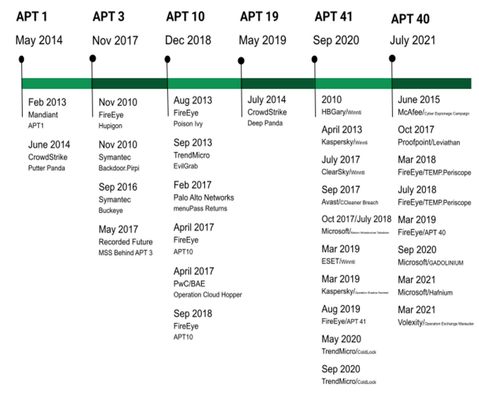
Approach

The analysis reconstructs the indictments process between 2014–2023 through:

- **Process tracing** of cyber indictment cases from initial intrusion to government action
- **Comparative case analysis** across China, Russia, North Korea, and Iran
- **Triangulation** of interviews, legal documents, and technical disclosures to identify causal drivers and critical junctures

Sources: interviews with U.S. officials, prosecutors, and threat intelligence analysts; Department of Justice indictments and other legal filings; technical threat reports and public attributions; and related sanctions, advisories, and diplomatic actions.

Case Overview: Indictments of China-linked hackers were not discrete events but part of a broader ecosystem. They are the culmination of long-running public–private investigative processes. Private threat intelligence firms publicly attributed cyber operations months, if not years, before indictments were unsealed. These early disclosures established technical baselines, sustained attribution confidence, and contributed to how cases were later framed in court.



Results

U.S. cyber indictments have evolved from episodic legal responses into a durable instrument of cyber statecraft, sustained through public–private collaboration.

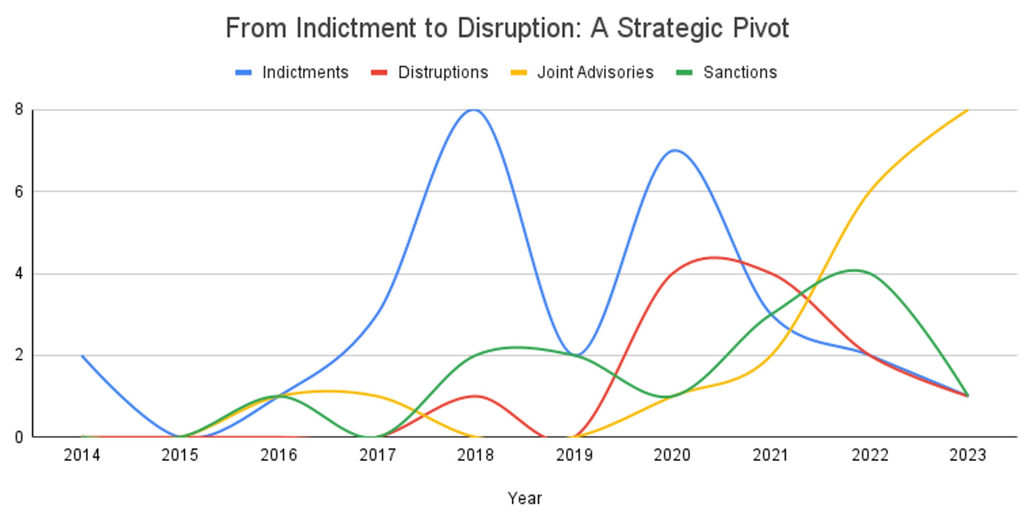
- **Deterrence as signaling**: Indictments function as strategic signals for norms of responsible state behavior—even when arrest is improbable. Their value is in exposure and persistence, not prosecution alone.
- **Transparency as operational advantage**: Public attribution creates evidentiary baselines and aligns narratives across government, allies, and industry. Transparency strengthens cyber statecraft.
- **Power enabled by partnership**: U.S. cyber statecraft increasingly leverages commercial threat intelligence to operationalize attribution and impose cost. This partnership supports, rather than replace, state authority.
- **Integration into a layered response**: Indictments now operate within a stacked toolkit, paired with sanctions, forfeitures, disruptions, and diplomatic actions, to accumulate pressure over time—a strategic pivot.

Cyber indictments now operate as infrastructure for U.S. cyber statecraft, reinforcing deterrence, alliance coordination, and norms of responsible state behavior within a public-private ecosystem.

The persistence of cyber indictments along with the growth of other tools of statecraft reflect a strategic pivot. It highlights the United States calibration of tools for maximum impact.

As attribution matured and public–private workflows improved, indictments shifted from stand-alone responses to routine instruments of signaling and pressure.

Bottomline: Indictments operate within a broader cyber policy ecosystem that includes private cyber threat intelligence (CTI) industry.



Simin Kargar
Johns Hopkins University School of Advanced International Studies

Cyber Indictments Are Co-produced: Private Attribution Enables Public Punishment.

Abstract

Since the early 2010s, the United States has set itself apart by deploying a broad and visible toolkit of statecraft—criminal indictments, sanctions, diplomatic actions, asset seizures, and technical disclosures—to impose costs on its adversaries and signal red lines in cyberspace. This research traces how the U.S. has responded to state-backed cyber operations from China, Russia, Iran, and North Korea since 2014.

Indictments remain a centerpiece, but their evolution tells a larger story. Over the past decade, they have expanded in scope and sophistication while also giving way to non-prosecution tools such as forfeiture actions and infrastructure disruption. These measures reflect a new kind of cyber statecraft that is flexible, layered, and designed to meet the challenges of attribution, enforcement, and deterrence in an increasingly contested digital domain.

The research underscores one central finding: U.S. cyber strategy leverages a public-private partnership unlike any other in national security. Private cyber threat intelligence firms provide early technical insight, attribution assessment, and evidentiary continuity that support government action. In many major cases, private cyber attribution precedes U.S. indictments, establishing the evidentiary and narrative foundations for prosecution. Over time, this dynamic collaboration has outgrown traditional contracting and now enables strategy itself.

The analysis also highlights the deeper forces at play: geopolitics, economic security, and the politics of disclosure that drive the design and impact of U.S. cyber policy. Drawing on case studies, interviews, and primary documents, this work shows how collaboration between government and industry has redefined U.S. cyber statecraft over the past decade, with implications for deterrence, alliance management, and the emerging norms of responsible state behavior in cyberspace.

Simin Kargar
Johns Hopkins University School of Advanced International Studies